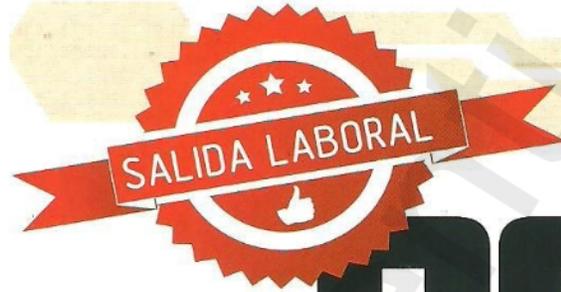


PC DE ESCRITORIO Y PORTÁTILES | TABLETS | CELULARES ¡Y MUCHO MÁS!

# USERS

ARGENTINA \$18,40.- // MÉXICO \$49.-



CURSO VISUAL  
Y PRÁCTICO

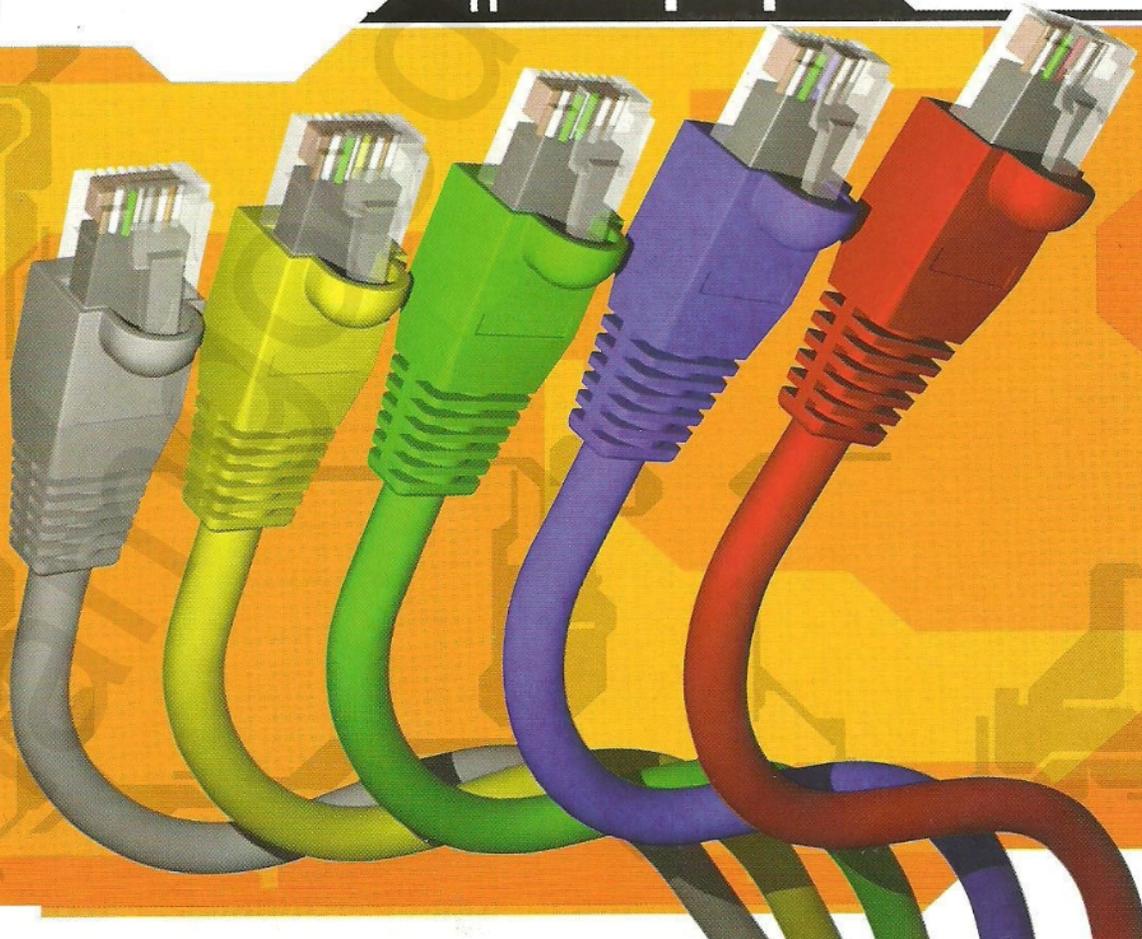
# Técnico PC

MANTENIMIENTO Y REPARACIÓN

## FUNDAMENTOS DE REDES

# 20

EN ESTE FASCÍCULO CONOCEREMOS LOS CONCEPTOS RELACIONADOS CON LAS REDES CABLEADAS, Y REALIZAREMOS LA CONFIGURACIÓN Y SOLUCIÓN DE PROBLEMAS.



# En esta clase veremos...

FUNCIONAMIENTO DE LAS REDES CABLEADAS Y LA FORMA EN QUE DEBEMOS CONFIGURAR LOS DISPOSITIVOS CONECTADOS. TAMBIÉN APRENDEREMOS A CONFIGURAR UN ROUTER HOGAREÑO Y RESOLVEREMOS PROBLEMAS DE CONECTIVIDAD.

En la entrega anterior conocimos todo lo relacionado con el hardware stressing, aprendimos a realizar este tipo de pruebas de rendimiento en diversos componentes de la computadora e interpretamos los resultados obtenidos. Por otra parte, conocimos aplicaciones especialmente diseñadas para efectuar poderosas pruebas de rendimiento. También monitorizamos el rendimiento de los dispositivos sometidos al stressing mientras se llevan a cabo las pruebas.

En esta oportunidad conoceremos todos los conceptos relacionados con las redes cableadas, y veremos el alcance del modelo OSI, las normas Ethernet y el protocolo TCP/IP. Analizaremos los distintos tipos de redes existentes y describiremos los dispositivos que encontraremos en una red cableada. También aprenderemos a armar un cable UTP, configuraremos un router hogareño y solucionaremos los problemas de conectividad más comunes.

08

EL MODELO OSI

10

EL PROTOCOLO TCP/IP

11

TIPOS DE REDES

18

CONFIGURAR UN ROUTER HOGAREÑO



# Introducción a las redes informáticas

HOY EN DÍA, CASI TODOS LOS DISPOSITIVOS ELECTRÓNICOS PERTENECEN A UNA INMENSA RED INTERCOMUNICADA LLAMADA INTERNET, PERO ¿QUÉ ES Y QUÉ INVOLUCRA? EN ESTA CLASE CONOCEREMOS LOS DISTINTOS ESQUEMAS DE REDES QUE ENCONTRAMOS Y SUS CARACTERÍSTICAS.



Desde la creación de la computadora y el manejo de la información de modo electrónico, se han requerido medios para transmitir datos entre dispositivos, sistemas y equipos de manera rápida, eficaz y a largas distancias. Para lograr este cometido, se fueron creando diferentes esquemas de interconexión que permitían tanto enviar como recibir esta información mediante lo que se denominó **red informática**. Una red informática es un enlace a través del cual dos o más dispositivos se comunican mediante medios físicos o inalámbricos con el fin de intercambiar datos, ya sea para hacer funcionar otros dispositivos o para almacenar información. En la actualidad, los fi-

nes de las redes son extremadamente variados. Con la difusión que fueron alcanzando las redes, surgieron tecnologías de intercambio masivo. En un principio, estas se limitaban a redes reducidas entre gobiernos y universidades dentro de una misma localidad, pero luego fueron ampliándose a provincias, estados, países y continentes. Esta red masiva dio nacimiento a Internet, como la conocemos hoy en día.

## CONECTIVIDAD Y ACCESO

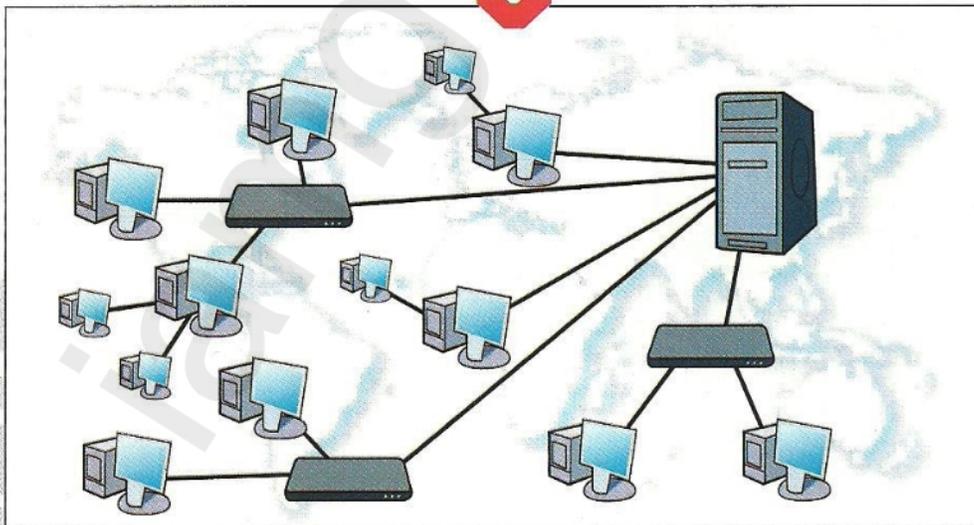
El aumento de usuarios domésticos, empresariales y comerciales llevó a las redes informáticas a ser más masivas y complejas, porque lo que se buscaba era aumentar la conectividad y el acceso a dispositivos comunes; gracias a esta necesidad, surgió la red local que se instala en el mismo domicilio. Actualmente, es común encontrarnos con una red doméstica en numerosos hogares.

## ESQUEMAS

Existen diversos esquemas de interconexión que fueron normalizándose con el paso de los años, con los cuales se optimizaron parámetros de funcionamiento hasta llegar a la más común y más difundida mundialmente. El esquema principal cuenta con un proveedor de información, dispositivos interconectados mediante cables o medios inalámbricos y un concentrador. La relación que se maneja entre ellos, el modo y medio por el cual se intercambia la información definen a una red.

**LAS REDES NOS PERMITEN ACCEDER A LOS DISPOSITIVOS CONECTADOS DESDE CUALQUIER LUGAR, DE MANERA INSTANTÁNEA, Y CONTROLARLOS.**

**Red WAN.** Esquema de las redes de mayores dimensiones o WAN (Wide Area Network, red de área extensa).



Si revisamos en cada casa, encontraremos una combinación muy habitual que consta de una entrada de Internet (a través de un proveedor), que va a un router o módem (el encargado de procesar esta información y redirigir los paquetes de datos a otras computadoras); y a partir del router, se conecta una o más computadoras, destino final de la información.

En una empresa, comercio u otro emprendimiento, existen más ramificaciones de la misma red, que se diferencia, entonces, por el número de terminales, routers y servidores principales. Pero el esquema básico siempre se mantiene en el mismo orden.

**Interfaz de red.** Los equipos informáticos precisan una interfaz de red para compartir contenidos.



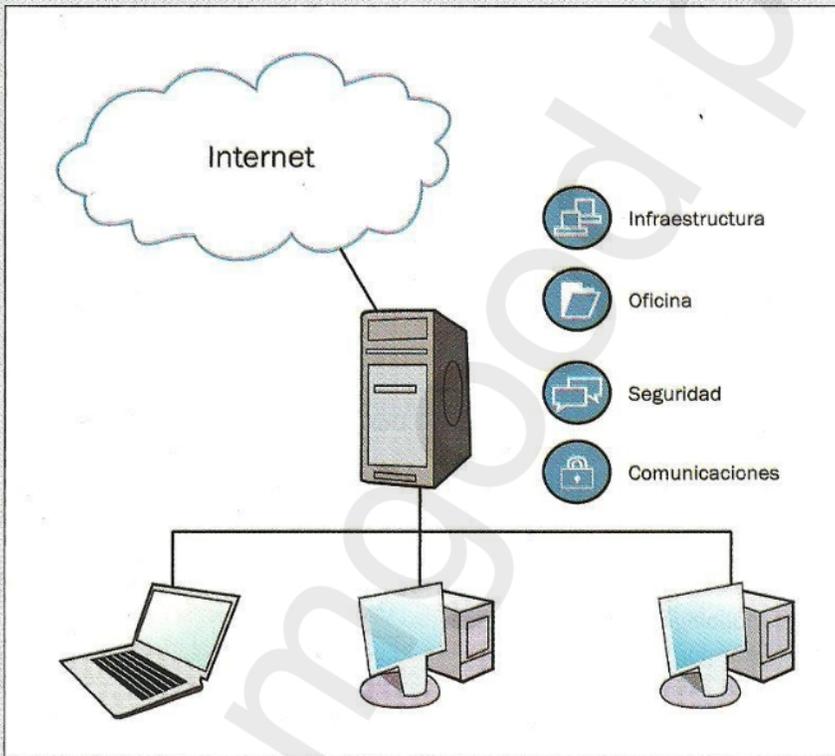
## ACCESO A DATOS

Dentro de la red, lo que buscamos es acceder a datos en otras terminales con un fin específico. En una red doméstica establecemos un vínculo para utilizar diferentes dispositivos; por ejemplo, usar una impresora instalada en otra computadora. Una de las finalidades más requeridas en las redes es compartir archivos en carpetas que se alojan en una computadora diferente de la nuestra, como un servidor que maneja toda la información, documentos, fotos, videos y música, sin necesidad de tenerla guardada directamente en nuestro equipo.

Otro objetivo es distribuir Internet en la red mediante una configuración adecuada. Con que un solo dispositivo tenga acceso a Internet, podremos distribuir dicha conexión a todos los dispositivos conectados. Algunos usos más profesio-

nales nos permiten manejar dos o más equipos de la red al mismo tiempo para realizar trabajos cooperativos. Y para usos relacionados con el ocio, la red nos permitirá jugar con otras personas en varias computadoras conectadas y, también, de forma remota.

El ámbito comercial o en una pyme, la red permite brindar acceso de modo más restringido, al definir usuarios y permisos para limitar el uso de cada terminal a un fin determinado; por ejemplo, un empleado podrá manejar un programa pero no contará con acceso a Internet. Hoy en día, es posible sincronizar información con Internet y manejarnos en redes mucho más amplias, para acceder a ella desde nuestro hogar o desde un bar.



## PROYECCIONES

Las redes informáticas nos permiten estar conectados a un grupo desde distancias antes no imaginadas, acceder a la información sin espera y comunicarnos al instante con otras personas. Los usos de las redes modernas abarcan funciones que todavía no están del todo desarrolladas, y van más allá de programar tareas, acceder remotamente a equipos y controlarlos. El futuro está por venir.



**Red local.** Configuración básica de una LAN (Local Area Network, red de área local).

## REDES INALÁMBRICAS

Las redes inalámbricas admiten la conexión de un sinnúmero de dispositivos, además de computadoras, tales como teléfonos, electrodomésticos, periféricos,

y otros. La idea de una red local inalámbrica es aumentar el número de dispositivos que pueden conectarse y acceder a ellos desde cualquier localización.

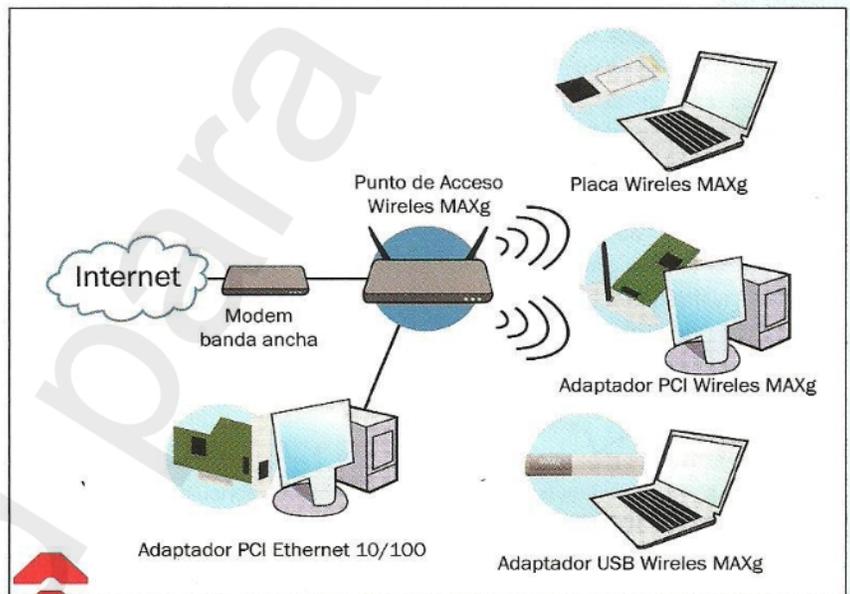
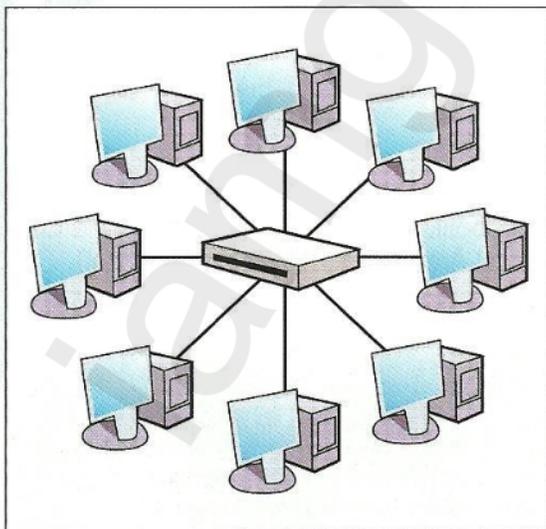
# Topologías cableadas e inalámbricas

LAS TOPOLOGÍAS DE LAS REDES VIENEN DADAS POR LAS COMPUTADORAS Y LA FORMA EN LA CUAL ESTAS SE CONECTAN. UNA TOPOLOGÍA SE DEFINE COMO LA APARIENCIA QUE TOMAN LAS CONEXIONES.

Dentro de la morfología de las conexiones, pueden existir muchos esquemas de conexión, es decir, distintas formas por las cuales las computadoras se conectan, de modo que la información fluya con más agilidad y se eviten diferentes cuellos de botella, nodos o determinados dispositivos. Con el paso de los años, se ha optimizado el flujo de información, se aumentó la velocidad de transferencia, y se economizaron los métodos y medios de conexión. Para entender mejor este proceso, vamos a describir algunas de las topologías que encontramos.

## TOPOLOGÍA DE BUS O LINEAL

Esta topología se basa, principalmente, en terminales y dispositivos conectados a una sola línea (bus) con un terminador en cada extremo. Todos los nodos de la red están conectados a este cable coaxial y Ethernet tipo 10Base2. El funcionamiento implica que, básicamente,



**Tecnología de infraestructura.** En este tipo de arquitectura de red se combinan conexiones tanto Ethernet como inalámbricas.

un paquete es enviado y presentado ante todas las computadoras, las cuales analizan la dirección para determinar si les corresponde a ellas o no.

### Ventajas

- ❑ Es la topología más fácil de armar y configurar por usuarios hogareños.
- ❑ Requiere menos cableado, por lo que es más económica que otras.



### Topología en estrella.

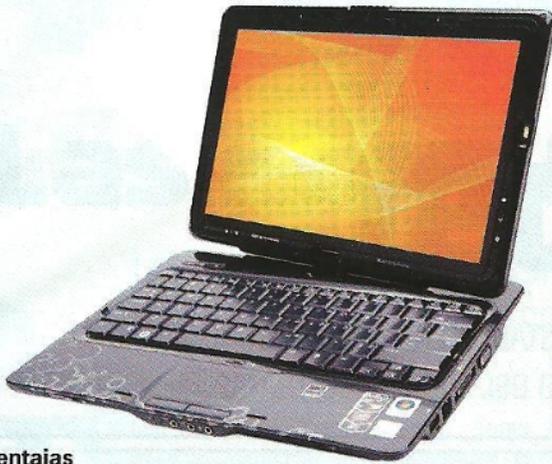
La más difundida y aplicada en redes hogareñas y corporativas de tamaño medio.

### Desventajas

- ❑ Las computadoras no regeneran la señal, por lo que hay ruidos y pérdida de fidelidad con la distancia.
- ❑ Depende de todas las estaciones; un usuario desconectado corta la red.

## TOPOLOGÍA EN ESTRELLA

La topología en estrella es una de las más comunes que podemos encontrar (denominadas redes LAN). En este caso, varias computadoras se interconectan mediante un concentrador (también llamado hub). El funcionamiento del hub se basa en repetir y potenciar la señal recibida desde algún terminal y redireccionarla hasta su destino. Detecta errores y los corrige.



**Ad-hoc.**  
Tecnología inalámbrica basada en conexiones punto a punto, común para interconectar notebooks.

**Ventajas**

- ❑ Si un terminal pierde conexión o esta finaliza, la red no se inutiliza, sino que sigue funcionando normalmente, sin alteraciones.
- ❑ No se pierde la conexión al aumentar o retirar dispositivos.

**Desventajas**

- ❑ Requiere mayor cableado.
- ❑ Cada computadora precisa un cable independiente hacia el hub.
- ❑ El punto crítico del sistema es el hub: si este se apaga, la red queda directamente fuera de servicio.

**TOPOLOGÍA EN ANILLO**

Los dos terminales están interconectados entre sí (a diferencia de la lineal), por lo que el último sistema es el comienzo del primero; así, cada computadora está conectada a otras dos, y la señal viaja en círculos. Utiliza un solo cable coaxial entre todos los equipos, porque la información viaja en un solo sentido. Cada computadora se comporta como un repetidor y regenerador de señal y, virtualmente, el trayecto recorrido es menor.

**Ventajas**

- ❑ Los problemas que surjan son fáciles de detectar y resolver.
- ❑ El cableado sigue siendo menor en comparación con la topología en estrella.
- ❑ La información sufre menos ruidos.

**Desventajas**

- ❑ La incorporación de una nueva computadora implica romper el anillo y la red.
- ❑ El soporte técnico requiere desactivar la red para solucionar conflictos.

**TOPOLOGÍA MESH**

Esta topología presenta una característica por la cual todas las computadoras están interconectadas entre sí. Esto hace que la red se sature rápidamente, porque el envío de información a otra máquina provoca un efecto en cadena de embotellamiento de la información.

**Ventajas**

- ❑ Todas las computadoras están interconectadas, sin intermediarios.

**Desventajas**

- ❑ Las conexiones son costosas y se requiere demasiada cantidad de cable.
- ❑ Cada dispositivo debe tener tantas placas de red como computadoras haya.

**TOPOLOGÍA AD-HOC**

La conexión es inalámbrica de tipo punto a punto, ya que se realiza de un dispositivo a otros sin medios físicos, sino a través de señales de radio entre ellos. Para que la conexión sea fiable, los equipos deben estar dentro de determinado rango; a medida que

**REDES MIXTAS**

Si bien hemos mencionado las configuraciones o topologías básicas, para seleccionar la mejor red, es importante saber distinguir su capacidad o tolerancia máxima en cuanto a computadoras disponibles, tasa de transferencia de información y distancia entre equipos. Esto nos llevará a elegir entre un tipo u otro de topología e, incluso, una combinación adecuada de ellas. Además, el presupuesto disponible es un factor determinante al decidir la topología más conveniente.

se alejan, se pierde la fidelidad de la información y la señal; esta distancia depende de la potencia del equipo.

**Ventajas**

- ❑ No se requieren medios físicos para la interconexión.
- ❑ Dentro del rango de trabajo proporciona movilidad y versatilidad.

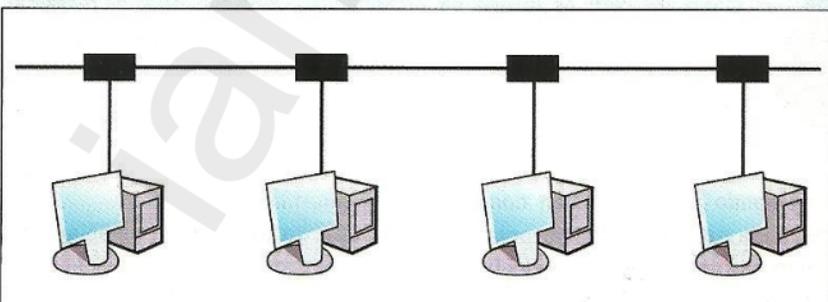
**Desventajas**

- ❑ Rango muy limitado de trabajo.
- ❑ Velocidad de trabajo reducida e inferior a las de las redes físicas.

**LAS REDES CABLEADAS POSEEN MAYOR TASA DE TRANSFERENCIA DE DATOS QUE LAS INALÁMBRICAS.**

**TOPOLOGÍA DE INFRAESTRUCTURA**

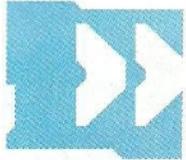
Esta arquitectura requiere de un elemento que coordine y sirva como punto base de información, una estación central inalámbrica. Si todos los elementos trabajan bajo el mismo SSID, todos tendrán acceso.



**Topología en bus.** Topología básica en línea, una de las primeras en ser implementadas.

# El modelo OSI

PARA DEFINIR EL MODO Y EL MEDIO POR EL CUAL SE ESTABLECEN LAS INTERCONEXIONES, SE UTILIZA UN MODELO DE COMUNICACIÓN DENOMINADO OSI. ¿DE QUÉ SE TRATA?



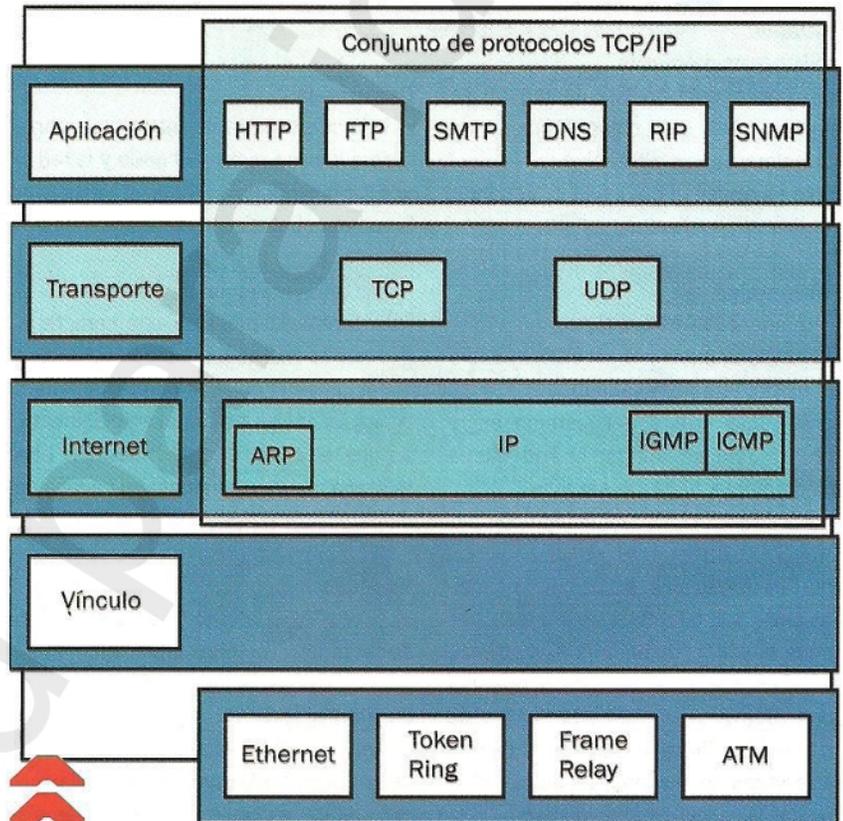
Para resolver cómo se comunican las computadoras, se definió un modelo de interconexión entre dispositivos abiertos (*Open System Intercommunication*); es decir, un modelo que determina cómo se lee con el fin de que todos los receptores entiendan el mensaje y haya compatibilidad entre ellos; en otras palabras: el modelo fija las reglas, el lenguaje y las normas que se deben llevar a cabo para establecer una comunicación.

## NIVELES

Esta norma está compuesta por siete niveles o capas que definen las diferentes etapas por las que pasa la información durante la transferencia entre dispositivos. Si bien esta base ha evolucionado mediante diversos protocolos y normas, el modelo OSI es un esquema de referencia que permite entender su funcionamiento.

## CAPAS

❑ **Capa física:** define el medio físico (sea este cableado, placas, routers) por el cual se llevan a cabo las comunicaciones dentro de una red y la forma en que esta se realiza.



**Protocolos asociados.** A cada capa se le asocian diferentes protocolos comúnmente utilizados por las aplicaciones.

❑ **Capa de enlace de datos:** asegura que la transferencia de datos sea fiable, para que la información llegue sin errores. Con este fin, se incluye en los paquetes de datos información adicional que permita identificar paridad y congruencia de datos.

❑ **Capa de red:** es la que se encarga de identificar el enrutamiento entre varias redes. Lo que busca esta capa es garantizar que la información que circula en la red llegue al destino aun cuando estas no estén conectadas. Esta capa es utilizada, principalmente, por los routers, que identifican al emisor y buscan al destinatario.

❑ **Capa de transporte:** se encarga de transportar la información desde el origen hasta el destino, sin importar el tipo de red física que se utilice.

❑ **Capa de sesión:** se dedica a mantener y controlar el enlace entre dos terminales que estén intercambiando información. Debe ser capaz de restaurar la sesión si esta es interrumpida.

❑ **Capa de presentación:** presenta los paquetes de información de manera legible y entendible al terminal de destino. Trata la semántica y la sintaxis de la información.

❑ **Capa de aplicación:** establece los protocolos que usarán las aplicaciones y los servicios de las diferentes capas.



**Router.** Los routers están definidos en la capa de red del modelo OSI.

# Las normas Ethernet

LAS NORMAS ETHERNET FUERON CREADAS PARA ESTANDARIZAR EL FUNCIONAMIENTO DE LAS REDES. EN ESTA SECCIÓN CONOCEREMOS SUS CARACTERÍSTICAS Y FUNCIONAMIENTO.

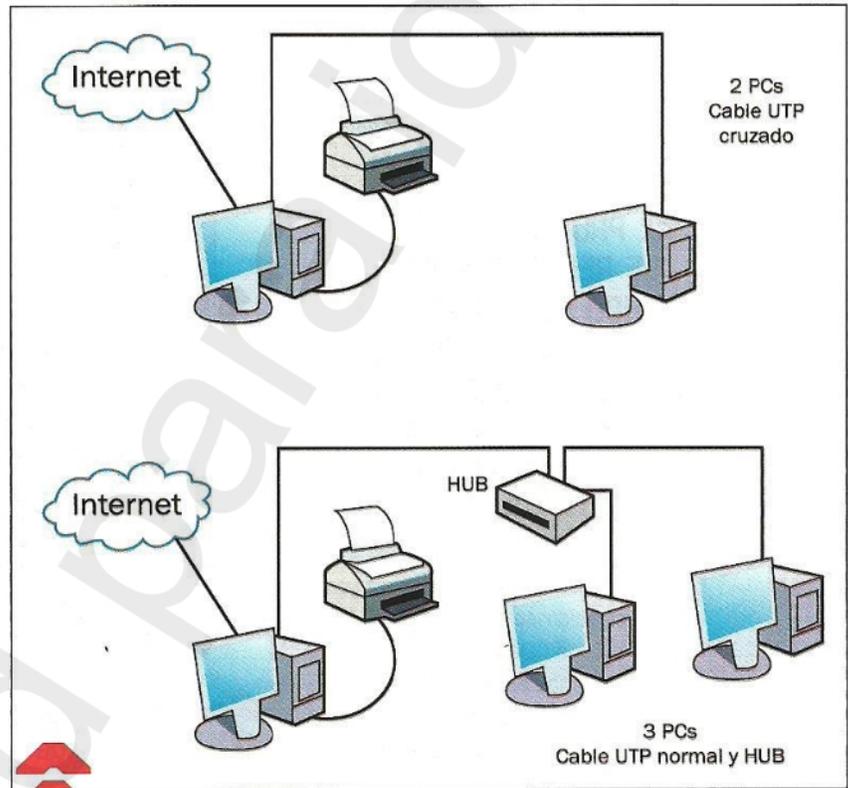
Las normas Ethernet tienen como objetivo identificar los paquetes y la información, y hacer que esta llegue a destino sin errores. Así fueron implementadas las normas del modelo IEEE 802 (*Institute of Electrical and Electronic Engineer*, comité 802), que se basa en protocolos para recibir y enviar información, en tramas o paquetes de datos, bajo una identificación específica.

**AL CONECTAR DOS EQUIPOS EN RED DEBEMOS SEGUIR LAS NORMAS ETHERNET, BASADAS EN PROTOCOLOS PARA ENVIAR Y RECIBIR PAQUETES DE DATOS.**

Estas normas se han aplicado a lo largo de los años, modificando la velocidad de transferencia desde 1 Mbit/s hasta 10 Gbit/s, y utilizando medios físicos desde cables coaxiales, cables con 8 hilos conductores (cable UTP con 4 pares trenzados), hasta fibra óptica. Los puertos terminales son placas de red que están preparadas para funcionar con ellos, y que derivan en concentradores o switches que se distribuyen a toda la red.

## CABLEADOS

Para cumplir con los estándares definidos, se establecieron distintos medios o cableados que recibieron diversas denominaciones (hablamos de tecnologías actuales sin hacer hincapié en otras pasadas de la misma norma):



**Modelo Ethernet.** Modelo básico de configuración de una red bajo el modelo Ethernet, con dos configuraciones y un switch.

❑ **10BaseT** (capacidad de transmisión - banda base - distancia máxima o medio físico): surge debido a que las versiones anteriores (5, 10, etc.) presentaban muchas complicaciones para localizar las fallas en el cableado. La velocidad de transferencia era de 10 Mbit/s, y fue rápidamente reemplazada por modelos más eficientes. El cableado máximo llega hasta 100 metros y 150 en par trenzado categoría 5 (CAT5).

❑ **100BaseTX**: utiliza cable de par trenzado UTP de 8 hilos, pero solo emplea 4: 2 para recepción y 2 para envío de datos. El resto se usa, opcionalmente, para telefonía y video. El ancho de banda permitido es de 25 MHz

y 100 Mbps. La longitud máxima del cableado es de 100 metros.

❑ **1000BaseT**: se diferencia, principalmente, por el uso de los 4 pares de hilos de cables, lo cual optimiza su funcionamiento porque aprovecha al máximo el cableado. Llega a transferir hasta 1 Gbit/s. Se mantiene el uso del cable CAT5.

❑ **1000BaseTX**: se destina a redes de alta velocidad con servidores más exigentes; la tasa de transferencia es de 1Gbit/s. La diferencia con los anteriores es que requiere cableado categoría 6, más costoso de actualizar, por lo que aún se prefiere la norma 1000BaseT, que usa cables categoría 5.

# El protocolo TCP/IP

CONOCEREMOS EL PROTOCOLO MÁS USADO PARA LA CONEXIÓN Y TRANSMISIÓN DE DATOS ENTRE COMPUTADORAS Y DISPOSITIVOS MÓVILES. ESTABLECE, ADEMÁS, LA BASE DE INTERNET.



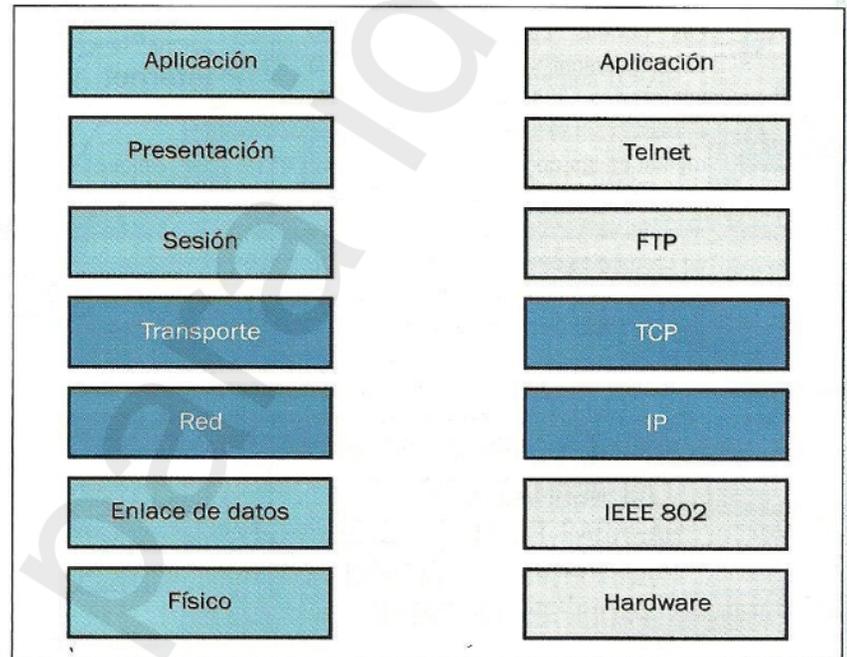
Un protocolo es una regla ordenada y consensuada de pasos o formalidades que se deben seguir con el fin de establecer una comunicación comprensible entre las partes implicadas en ella.

**EL PROTOCOLO TCP/IP SE REMONTA A 1972, CUANDO EL DEPARTAMENTO DE DEFENSA DE LOS EE.UU. LO UTILIZÓ PARA ENLAZAR SU PROPIA RED DE COMPUTADORAS.**

## COMUNICACIÓN

En Internet, el protocolo establecido para la comunicación se denomina Protocolo de Control de Transmisión (TCP, por sus siglas en inglés) e IP (Protocolo de Internet), y sirve para enlazar, dentro del contexto de red, a todos aquellos dispositivos que requieran transmitir o recibir datos. Es decir que lo que hace posible la comunicación en Internet y en las redes de área local de equipos de escritorio, portátiles, tablets, teléfonos móviles y todo hardware capaz de establecer una conexión, es este lenguaje común.

El protocolo TCP/IP hace posible que un servidor que funciona bajo el sistema ope-



**OSI Y TCP/IP.** Correspondencia funcional entre el modelo de niveles OSI y las capas protocolares TCP/IP.

rativo Linux reconozca un computadora Windows en la red, y que esta pueda comunicarse con otra bajo el S.O. de Apple. Toda red, tanto cableada como wireless, sigue los pasos establecidos por el protocolo TCP/IP y, mediante él, es posible la navegación web, el envío de

correo electrónico y la implementación de otros protocolos, como FTP (transferencia de archivos) y Telnet (acceso remoto a otros dispositivos).

## DATOS TRANSMITIDOS

El protocolo TCP es el encargado de controlar la fiabilidad de los datos transmitidos. Se ocupa de resguardar el orden, identificar los errores, y establecer el puerto y las aplicaciones que le darán curso en su destino.

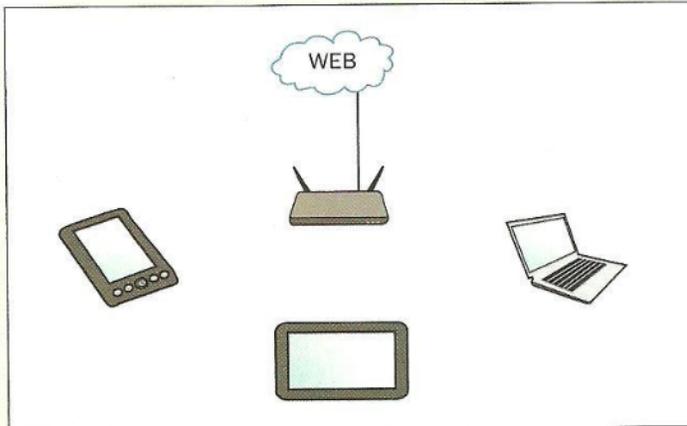
El protocolo IP da una dirección única y distintiva a un dispositivo conectado a la red, de tal modo que la transmisión de flujo de datos (a cargo del TCP) tenga un destino preciso. Esta dirección tiene tres números separados por un punto (por ejemplo: 74.125.45.99) y se resuelve en la interfaz de usuario por medio de un nombre de dominio conocido como DNS (por ejemplo: [www.google.com](http://www.google.com)).

## TCP/IP Y EL MODELO OSI

Desde los años 80 del siglo pasado, el desarrollo de tecnologías fue variando, y cada fabricante estableció pautas propias de conexión para sus dispositivos. Por eso, y con el fin de enlazar las diferentes redes, fue necesario implementar un estándar de comunicación, conocido como modelo OSI, que instaura un modelo de interconexión de sistemas abiertos (*Open System Interconnection*). Este estándar establece siete niveles de comunicación: nivel físico, de enlace de datos, de red, de transporte, de sesión, de presentación y de aplicación. El protocolo IP actúa en el nivel de red, y el TCP, en el nivel de transporte.

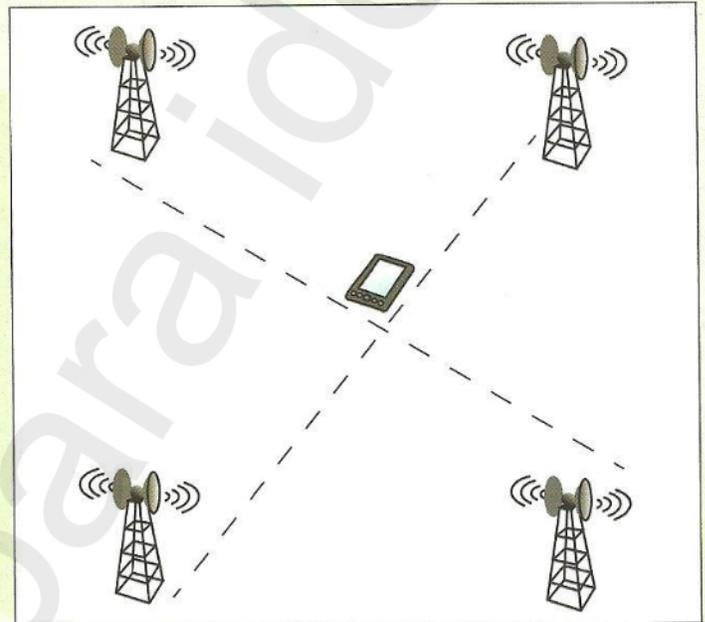
# Tipos de redes

INDEPENDIEMENTE DE SU TOPOLOGÍA, LAS REDES ADQUIEREN UNA CARACTERÍSTICA PROPIA SEGÚN SU EXTENSIÓN Y SU FUNCIONALIDAD. AQUÍ DISTINGUIREMOS LAS REDES PRINCIPALES.



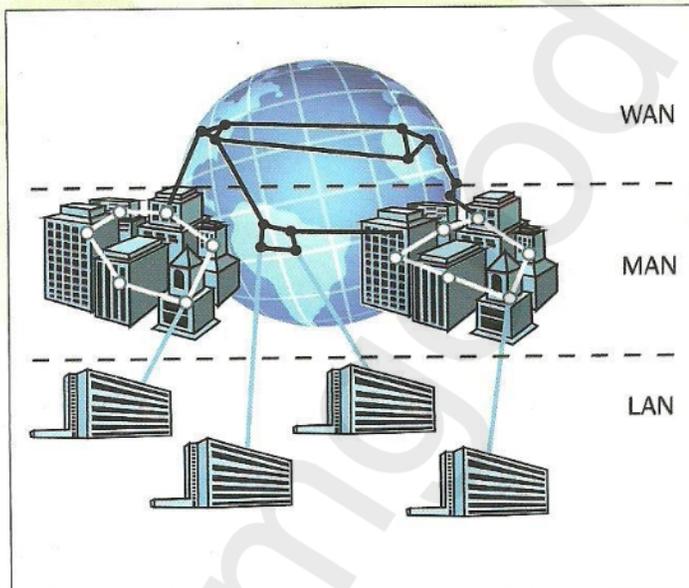
## PAN

(*Personal Area Network*): identifica a las redes delimitadas por el uso personal. Su carácter es tanto más específico cuanto más se extienden los dispositivos móviles inalámbricos de uso individual; por ejemplo, puede ser entre dos dispositivos Bluetooth.



## GAN

(*Generic Access Network*): permite el desplazamiento de equipos móviles, basados en voz o IP, y funciona por alternancia entre las redes LAN o WAN encargadas de mantenerlos con conexión.



## WAN, MAN y LAN

- ✘ **WAN** (*Wide Area Network*): es una red de área amplia, que llega a extenderse por kilómetros. El prototipo de WAN es una ciudad, provincia o país; su entorno de conexión es extenso, y abarca a todos los dispositivos y redes conectados a esa red.
- ✘ **MAN** (*Metropolitan Area Network*): red que abarca un área de hasta 50 km, cuya extensión permite el enlace de varios edificios o LANs dentro de un área corporativa o metropolitana específica.
- ✘ **LAN** (*Local Area Network*): es una red que enlaza hardware y software en un entorno próximo, de no más de 200 metros. Generalmente, conecta a estaciones de trabajo con un servidor y todos los recursos compartidos entre los usuarios de esa red.

## UN SIGLO DE REDES

Aunque nos parezca de ciencia ficción, lo cierto es que las redes actuales son el resultado del desarrollo de tecnologías que llevan más de cien años. Para darnos una idea, podemos mencionar que el cable de par trenzado,

tan habitual en las redes actuales, es un invento de Alexander Graham Bell que se remonta a 1881; mientras que la primera transmisión inalámbrica de ondas electromagnéticas estuvo a cargo de Nikola Tesla, en 1891.

# Transmisión de datos en una red

Una red cableada moderna, ya sea hogareña o de oficina, está conformada no solo por computadoras de escritorio, sino también por equipos portátiles, impresoras y dispositivos de interconexión.

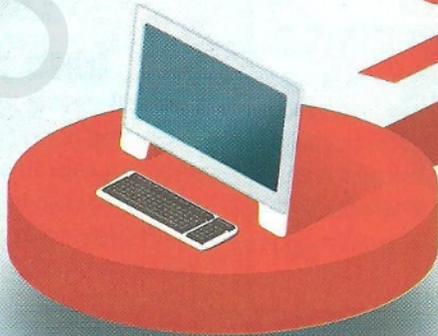
Para que una comunicación de red pueda ser satisfactoria, esta se realiza de manera fragmentada, en pequeñas cápsulas de información llamadas tramas y paquetes.

192.168.1.27

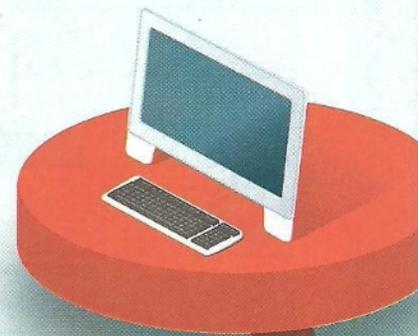


**1** El equipo de origen emite un paquete de red hacia otro en la misma red. Tal como en el correo postal, cada paquete tiene una dirección de origen y una de destino.

**PC de origen**  
192.168.1.23



192.168.1.2



**2** El switch recibe el paquete de red y es capaz de interpretar la dirección de destino, gracias a las tablas que vinculan direcciones IP con direcciones físicas.

**SWITCH**



**5** El switch interpreta el aviso de confirmación y lo envía a la dirección correspondiente, de forma inversa que en el paso 3. Si el equipo de origen no recibe esta notificación, considera que el paquete se perdió y vuelve a enviar el paquete original.

## El contenido de los paquetes de red

Los paquetes de red no contienen pura y exclusivamente la información propiamente dicha que se desea transmitir. Justamente para que pueda ser transmitida, se adosa, además, a cada paquete de datos, información sobre el origen y el destino (Direcciones MAC, IP y puertos) y un número de orden correlativo, en lo que se conoce como cabecera. Además, se agrega un mecanismo de verificación de errores (CRC, comprobación de redundancia cíclica).



A TRAVÉS DE LA SIGUIENTE REPRESENTACIÓN GRÁFICA, SE EXPLICA EL COMPLEJO MECANISMO MEDIANTE EL CUAL UN SIMPLE PAQUETE DE RED ES ENVIADO DE UN DISPOSITIVO A OTRO.

**PC de destino**  
**192.168.1.4**

3 Una vez interpretado el paquete, el switch envía en forma directa el paquete de red hacia el puerto al que está conectado el equipo o dispositivo de destino.

**192.168.1.5**

4 El equipo de destino recibe el paquete y envía una señal de confirmación de recepción (llamada ACK) al equipo que originó el mensaje.

**192.168.1.8**

CRC

**Qué es el overhead**

El overhead es toda aquella información adicional a los datos en sí; comprende direcciones físicas (MAC), direcciones IP, puertos y CRC.

En conexiones cableadas de corta distancia, como las redes locales, el overhead ocupa una mínima parte de cada paquete, pero en otro tipo de conexiones, como las inalámbricas o las cableadas de larga distancia, el porcentaje de overhead puede ocupar un gran porcentaje de la transmisión: un mal, pero necesario.

Direcciones MAC

Direcciones IP

Puertos

Comprobación

# Dispositivos para redes cableadas

SEGÚN SU DISPOSICIÓN O TOPOLOGÍA, LAS REDES CABLEADAS INCORPORAN EN SU FUNCIONAMIENTO DISPOSITIVOS DE DIFERENTES TECNOLOGÍAS, QUE DESCRIBIMOS A CONTINUACIÓN.

En los últimos años, las conexiones inalámbricas han tenido una gran expansión debido a su comodidad. No obstante, la red cableada no ha desaparecido ni retrocedido significativamente frente a la wireless; tanto es así, que podríamos afirmar que cualquier red inalámbrica tiene como base una interconexión de dispositivos cableados. Las tecnologías actuales permiten considerar que las redes cableadas son insustituibles en cualquier red LAN de amplia distribución y volumen. La red cableada es sólida; esto quiere decir que es mucho más complejo interferir o capturar datos desde un dispositivo externo a la red; es fiable, porque la tecnología de interconexión ofrece una variedad de cables como el coaxial, el de par trenzado o UTP y el de fibra óptica, destinado a conexiones más veloces,

seguro y con posibilidad de cubrir grandes extensiones; además es flexible, y se puede expandir o ampliar gracias a los recursos de software y hardware que intervienen en su estructura.

Según su topología, las redes cableadas incorporan los dispositivos que describimos a continuación.

**LAS TECNOLOGÍAS ACTUALES PERMITEN CONSIDERAR QUE LAS REDES CABLEADAS SON INSUSTITUIBLES EN CUALQUIER RED LAN DE AMPLIA DISTRIBUCIÓN Y VOLUMEN.**

## TARJETA DE RED

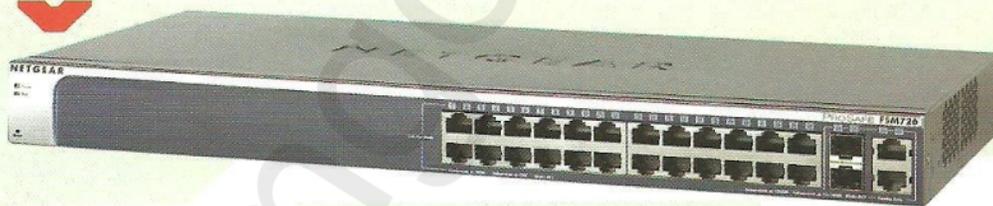
Se trata de una placa PCB de circuito impreso de inserción interna o externa a la computadora. Dependiendo del

bus de datos de la tarjeta, contamos con plataformas de expansión PCI, PCI-Express, USB o ExpressCard, entre otras. Su interfaz consta de un puerto Ethernet o de fibra óptica y un indicador lumínico de actividad. Funciona a una velocidad de entre 10 y 1000 mbps. Posee un número único que la identifica, conocido como dirección MAC, y que es incorporada al momento de su fabricación. Entre sus recursos podemos mencionar la inclusión de una memoria ROM, que permite el inicio y el acceso remoto a un equipo.

## SWITCH

Es un dispositivo puente que permite la interconexión entre nodos por medio del almacenamiento automático de una tabla de direcciones MAC. Un switch (o conmutador) puede conectar redes LAN posibilitando un tráfico seguro y ágil, ya que los datos son administrados por la dirección MAC que enlaza el nodo de origen con el de destino. Este recurso disminuye las colisiones de datos, la velocidad de ancho de banda y la simultaneidad de transmisiones entre computadoras. En switches denominados "inteligentes", incluso es posible configurar la segmentación de la red de modo de separar grupos de dispositivos en redes virtuales o VLAN.

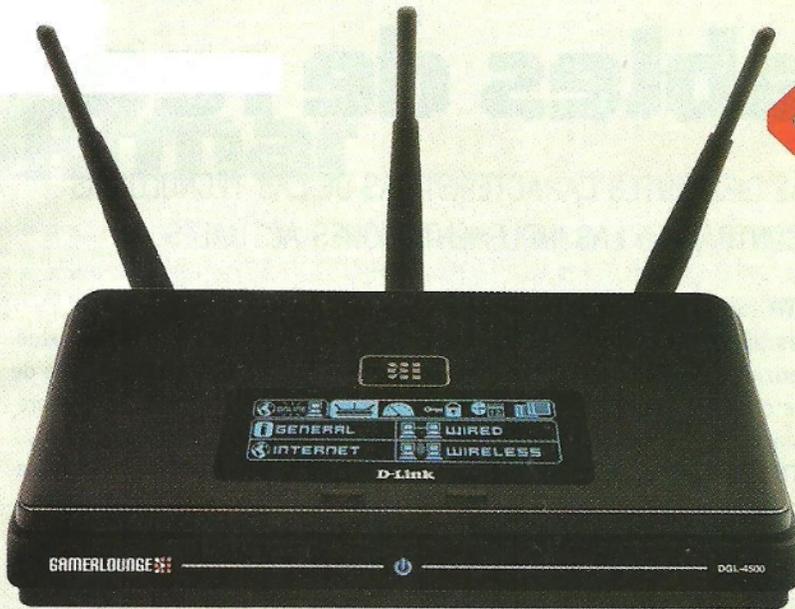
**Switch.** Su tabla de direcciones MAC permite una óptima transmisión de datos entre origen y destino.



## FIBRA ÓPTICA PARA INTERNET

A mediados del siglo XIX, un joven multimillonario inglés llamado Cyrus W. Field estaba obsesionado con unir telegráficamente Europa con América a través de un cable submarino transoceánico. En el año 1857 cumplió su propósito al lograr la comunicación entre dos barcos: el suyo y otro en la costa americana.

Este es el antecedente para la inmensa maraña submarina de cables intercontinentales que hoy día posibilita, mediante la fibra óptica, las comunicaciones telefónicas y de Internet en todo el mundo. Como sabemos, las redes cableadas garantizan la transmisión de datos en grandes volúmenes y a óptima velocidad.



**Router.** Muy difundido hoy, es el dispositivo que hace posible las extensiones de WAN por medio de wireless o Ethernet.

### REPETIDOR

Es un dispositivo que recibe una señal media o baja y la retransmite ampliada. Bajo estas características, podemos considerar al access point como un repetidor. Por lo general, este dispositivo recibe una señal de medios inalámbricos o cableados, y la retransmite para el acceso de otros dispositivos inalámbricos.

### GATEWAY

Por último, mencionamos el gateway, que es un dispositivo nodo dentro de la red local, que sirve para enlazar con otra red de protocolo diferente. Podemos considerar como gateway a un módem, router o computadora dentro de una red local, que enlaza a un nodo host con otro nodo servidor de red externa. El ejemplo más habitual de este tipo de dispositivos es la conexión de una red hogareña a Internet.

### ROUTER

Es un dispositivo que funciona a niveles de direcciones IP y que permite transferencias de datos de manera inteligente. Posibilita la interconexión de varias subredes y trabaja en área extensa o WAN. A diferencia del switch, que almacena una tabla de direcciones MAC, el router diseña la tabla de origen y destino, trazando posibles rutas. Recibe los datos en la capa física de entrada, los lee, los comprime en algunos casos y selecciona la mejor ruta para la transmisión. Mantiene los datos, gestiona las tablas y los mecanismos de red dentro del dispositivo, e incorpora entre sus recursos a los switches, hubs y otros routers. Es un dispositivo absolutamente configurable, y entre sus funcionalidades está la de incorporar un firewall, y abastecer simultáneamente redes LAN y WLAN.

### HUB

Es un dispositivo que ha caído en desuso. Permite la conexión de varias computadoras en una topología en estrella, y retransmite los datos recibidos ampliando y limpiándolos de errores. La transmisión de datos no es simultánea, sino alternada, es decir que termina de recibir y transmitir un paquete de datos y, luego, continúa con el siguiente.



**Hub.** Obsoleto, pero útil en pequeñas redes hogareñas o en espacios de trabajo reducidos.

## ¿TE RESULTA ÚTIL?

Lo que estás leyendo es el fruto del **trabajo de cientos de personas** que ponen todo de sí para lograr un **mejor producto**. Utilizar versiones "pirata" desalienta la inversión y da lugar a publicaciones de **menor calidad**.

**NO ATENTES CONTRA LA LECTURA. NO ATENTES CONTRA TI. COMPRA SOLO PRODUCTOS ORIGINALES.**

Nuestras publicaciones se comercializan en kioscos o puestos de voceadores; librerías; locales cerrados; supermercados e internet ([usershop.redusers.com](http://usershop.redusers.com)). Si tienes alguna duda, comentario o quieres saber más, puedes contactarnos por medio de [usershop@redusers.com](mailto:usershop@redusers.com)

# Tipos de cables de red

EN ESTA SECCIÓN DESCRIBIREMOS LAS DIFERENTES CARACTERÍSTICAS DE LAS TECNOLOGÍAS DE CABLE DE RED QUE PODEMOS ENCONTRAR EN LAS IMPLEMENTACIONES ACTUALES.

Los cables de par trenzado son filamentos de cobre entrelazados. Esta transposición permite equilibrar el nivel de interferencias de otros conductores de corriente electromagnética adyacentes.

## PAR TRENZADO

Entre los tipos de par trenzado encontramos los siguientes:

❑ **UTP** (*Unshielded Twisted Pair*): son cables de fácil manejo y aplicación. Su uso es habitual en redes locales. No tienen blindaje (de allí su nombre) y, por lo tanto, son más susceptibles a los errores por interferencias.

❑ **STP** (*Shielded Twisted Pair*): estos cables presentan un blindaje, y se caracterizan porque cada par está aislado de otro por una malla que disminuye considerablemente la interferencia.

❑ **FTP** (*Foiled Twisted Pair*): el blindaje de estos cables no es por pares o por grupos de filamentos como los anteriores, sino global, es decir que abarca todo el conjunto de pares trenzados.

**EL TIPO DE CABLE POR EMPLEAR EN UNA RED DEPENDE DE LA EVALUACIÓN DE COSTO, VELOCIDAD Y SEGURIDAD REQUERIDAS EN ELLA.**

## OTROS CABLES

No podemos dejar de mencionar otros cables de características diferentes que aún juegan un papel importante en la estructura de una red cableada. Entre ellos encontramos al coaxial. Este cable tiene un núcleo central de cobre por donde viaja la señal eléctrica. Está aislado por un elemento denominado dieléctrico, el cual, a su vez, está cubierto por una malla o blindaje que funciona como cuerpo de retorno de datos. Finalmente, el conjunto es protegido por una malla plástica.

El cable coaxial se utiliza habitualmente para la transmisión de las señales televisivas por cable. Algunos proveedores de Internet lo usan para lo que denominamos conexión de cablemódem.

## FIBRA ÓPTICA

Para las conexiones de redes extensas, es más habitual emplear cable de fibra óptica, cuya estructura es parecida a la del coaxial. El núcleo, en vez de ser de cobre, tiene uno o más filamentos de vidrio o material plástico. Este cable emplea una señal lumínica en lugar de una eléctrica, y los datos son transmitidos por impulsos de luz. Las señales lumínicas son concentradas; no desaparecen hasta que llegan a destino. No es posible "pinchar" un cable de fibra óptica para robar información, ya que, al hacerlo, se interrumpe la transmisión de los haces de luz en ese punto.

## Cable coaxial.

Menos implementado que el par trenzado o el óptico, pero útil en algunos dispositivos.



### Cables de par trenzado.

La opción entre cable blindado o UTP está determinada por el presupuesto y la seguridad.



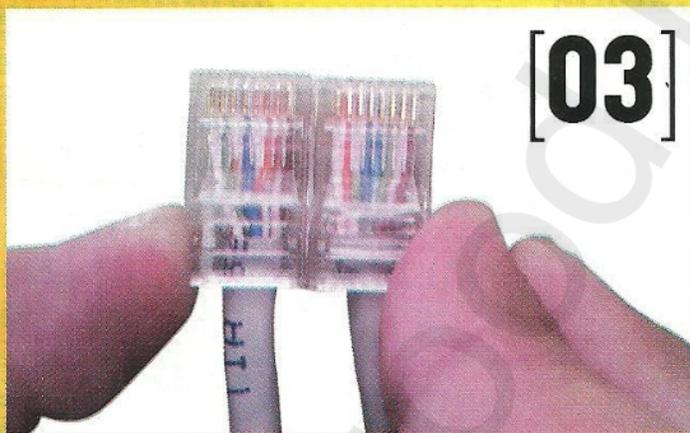
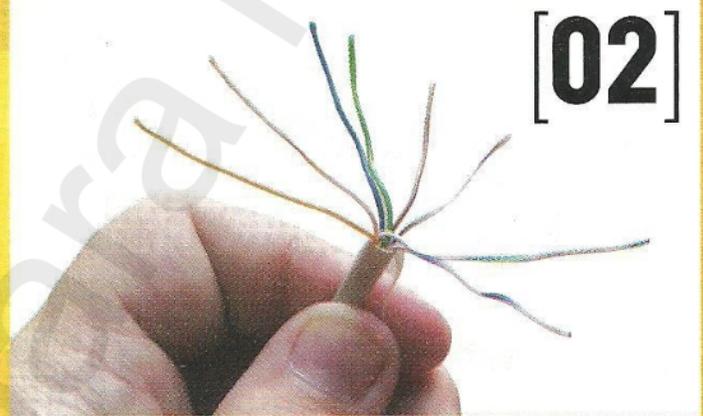
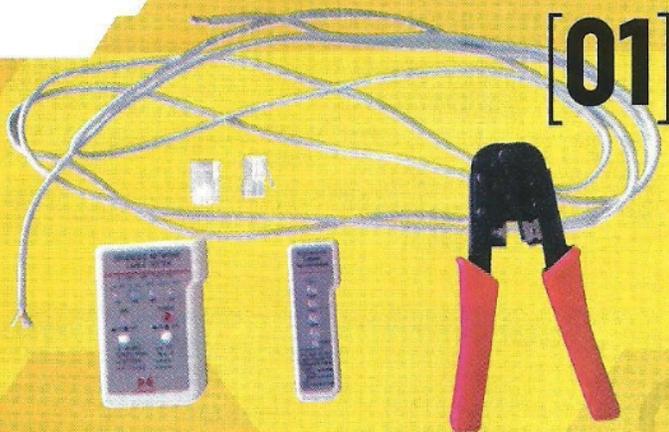
## COMPATIBILIDAD ELECTROMAGNÉTICA

El fenómeno de la diafonía se produce en un entorno de trabajo donde se emiten señales electromagnéticas; se trata de la perturbación de un circuito electromagnético a otro. Un circuito electromagnético perturba por atenuación cuando sus datos son inteligibles en el circuito perturbado;

y lo perturba por ruido cuando se captan señales no inteligibles. El blindaje que presentan algunos cables de par trenzado tenía como propósito salvaguardar los datos de la diafonía; sin embargo, el cable de par trenzado UTP ha brindado buena respuesta de compatibilidad.

# Armar un cable UTP

LOS CABLES DE RED CON LOS QUE DAMOS CONECTIVIDAD A NUESTROS EQUIPOS PUEDEN ROMPERSE POR VARIOS MOTIVOS. ES POR ESO QUE, SI CONTAMOS CON LAS HERRAMIENTAS Y CON LOS ELEMENTOS NECESARIOS, PODREMOS ARMAR DE NUEVO ESTOS CABLES SIN NECESIDAD DE RECURRIR A UN TÉCNICO ESPECIALIZADO. VEAMOS CÓMO REALIZAR ESTA TAREA CON ÉXITO.



[01]

Primero los ingredientes: pinza crimpadora (1), tester de red (1), fichas RJ-45 (2) y cable UTP categoría 5 (cantidad necesaria). Como vemos en la imagen, con estos elementos vamos a preparar un cable de red para reemplazar al que se haya dañado.

[02]

Con la pinza crimpadora cortamos y retiramos unos 2 cm de vaina protectora que recubre los 4 pares del cable UTP; los separamos y los acomodamos de acuerdo con la norma que estamos necesitando (T568A o T568B). Luego, repetimos este mismo procedimiento pero con el otro extremo del cable.

[03]

Una vez ordenados los pares, los colocamos en orden en la ficha RJ-45, como se aprecia en la imagen del ejemplo. Para continuar, colocamos la ficha con el cable insertado en la ranura correspondiente de la crimpadora, de esta manera realizamos el cierre de la ficha y la consiguiente fijación del cable.

[04]

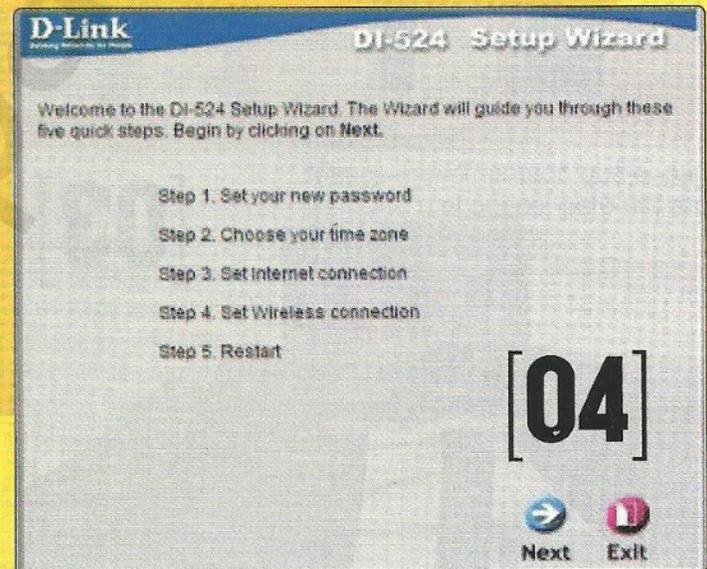
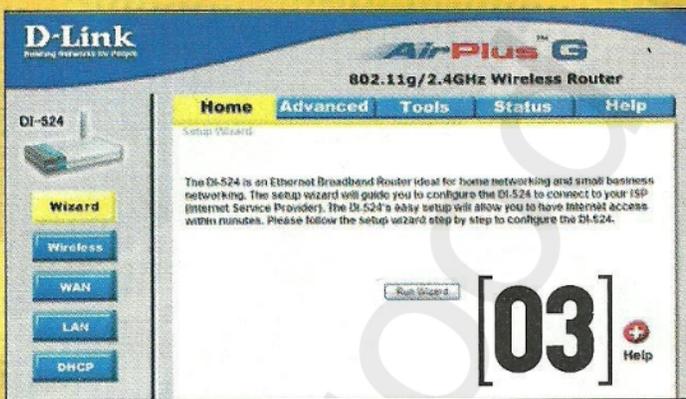
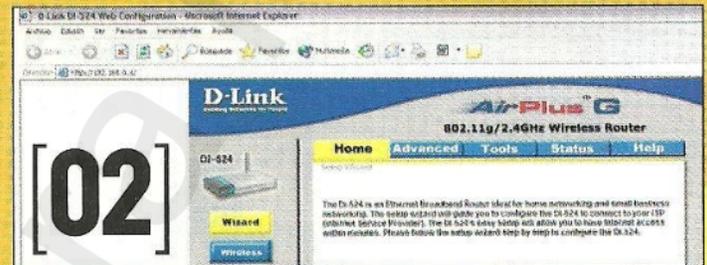
Es importante ordenar correctamente los cables según la norma que deseamos utilizar, solo después de esto utilizaremos la herramienta de corte que vemos en la imagen llamada crimpadora, para emparejar los cables. Repetimos este procedimiento hasta que queden todos los cables iguales.

# Configurar un router hogareño

EN ALGÚN MOMENTO DE NUESTRA CONEXIÓN A INTERNET TENDREMOS LA NECESIDAD DE CONFIGURAR NUESTRA PROPIA RED, UNA TAREA QUE PUEDE SER TAN COMPLICADA O SIMPLE COMO QUERAMOS. AQUÍ VEREMOS CÓMO HACERLO SENCILLO TOMANDO COMO EJEMPLO ESTE MODELO DE D-LINK.



[01]



[01]

La configuración es similar en la mayoría de los dispositivos, por lo que tomaremos como ejemplo el modelo D-Link DI-524. Conectamos la antena y el cable de corriente. A la entrada WAN se conecta un cable de red proveniente del módem (sea cablemódem o módem ADSL).

[02]

Para la primera configuración, conectamos un cable de red a uno de los puertos Ethernet del router, y este, a la placa de red de la PC. Abrimos el navegador e ingresamos la IP del router (figura en el manual; pero suele ser la misma para casi todos los modelos).

[03]

Se nos pedirá usuario y contraseña, que encontramos en el manual, ya que en este punto, los datos pueden variar de un fabricante a otro. Una vez hecho esto, accedemos a la interfaz web del dispositivo, en donde corremos el asistente de configuración para poner la red WiFi en funcionamiento.

[04]

En el primer paso, se nos solicitará cambiar la contraseña de acceso al router, procedimiento más que recomendable para mantener cierto grado de seguridad en la red. Luego, debemos seleccionar la zona horaria. Completados estos pasos iniciales, comenzaremos a configurar nuestra red.

# SIEMPRE ES ACONSEJABLE CAMBIAR LA CONTRASEÑA DE ACCESO AL ROUTER.

**D-Link** **DI-524 Setup Wizard**

Select Internet Connection Type (WAN)

Select the connection type to connect to your ISP. Click Next to continue.

Dynamic IP Address Choose this option to obtain an IP address automatically from your ISP. (For most Cable modem users)  
 Static IP Address Choose this option to set static IP information provided to you by your ISP.  
 PPP over Ethernet Choose this option if your ISP uses PPPoE. (For most DSL users)  
 Others PPTP, BigPond Cable, L2TP and Telia.

[05]

Back Cancel Next Exit

**D-Link** **DI-524 Setup Wizard**

Set Wireless connection

Enter in the SSID name and Channel number to be used for the Wireless Access Point. Click Next to continue.

Network ID (SSID)   
 Channel  WEP Encryption   
 WEP Key   
 Input 10 HEX characters (HEX is 0-9, A-F, or a-f)

[06]

Back Cancel Next Exit

**Home** **Advanced** **Tools** **Status** **Help**

Wireless Settings

These are the wireless settings for the AP (Access Point) portion.

Wireless  Enabled  Disabled

Network ID (SSID)

Channel

Security

Preshare Key

[07]

Apply Cancel Help

**Home** **Advanced** **Tools** **Status** **Help**

Special Application

Special Application is used to run applications that require multiple connections.

Enabled  Disabled

Name

Trigger Port

Trigger Type

Public Ports

Public Type

[08]

Apply Cancel Help

Special Application List

Name	Trigger	Public Port
Battle.net	6112	6112

[05]

En un cablemódem o módem ADSL, al configurar la conexión a Internet, debemos seleccionar la IP dinámica. Esto significa que nuestro ISP será el que asigne la IP pública mediante la cual tendremos salida a Internet. Esta IP nada tiene que ver con las direcciones privadas.

[06]

Ahora debemos configurar los parámetros de WiFi. Completamos el campo SSID con el nombre mediante el cual el sistema operativo verá la red; el canal de transmisión no hace falta cambiarlo; y en encriptación no modificamos nada, ya que lo configuraremos luego.

[07]

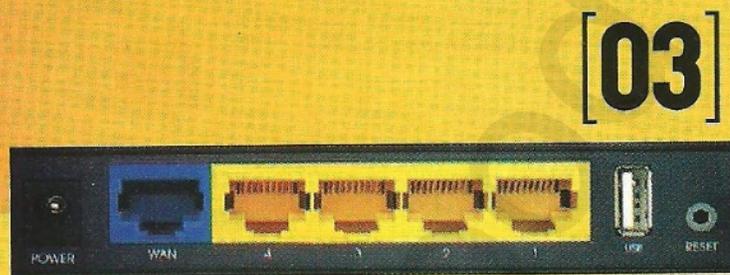
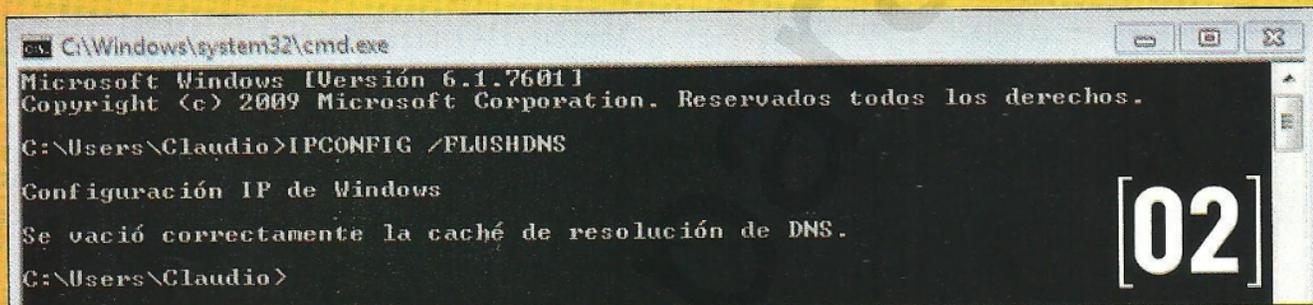
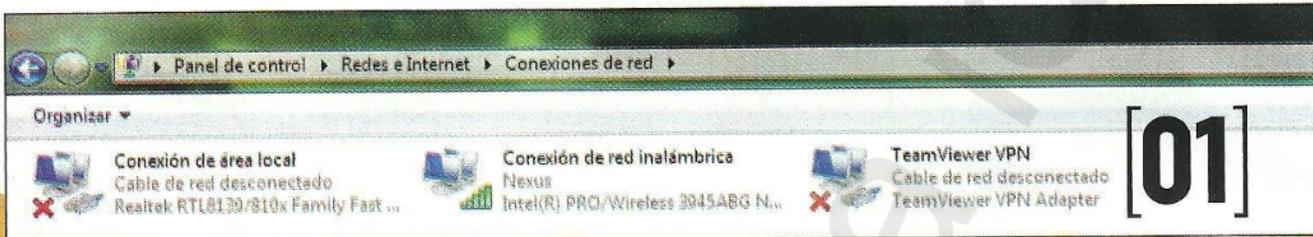
En la sección Wireless vamos a cambiar el tipo de seguridad. Disponemos de varias opciones, aunque la que nos brindará el mayor grado de resguardo es WPA2. Luego de seleccionar el método de cifrado de la señal que deseemos, definimos la contraseña que nos permitirá conectarnos.

[08]

Si queremos evitar que se "cuelguen" de nuestro WiFi, en el menú Wireless, dentro del apartado Advanced, podemos determinar que el router no transmita el SSID. Así, la red no será visible para Windows, y tendremos que configurar nuestro acceso para conectarnos a redes que no transmitan SSID.

# Solución de problemas de conectividad

SON MUCHAS LAS CAUSAS QUE PUEDEN PROVOCAR QUE SE INTERRUMPA NUESTRO ACCESO A LA RED, ALGUNAS MÁS SIMPLES DE RESOLVER Y OTRAS MÁS COMPLEJAS. VEAMOS ALGUNOS DE LOS PROBLEMAS CON LOS QUE PODEMOS ENCONTRARNOS Y QUE PUEDEN EVITAR QUE DISFRUTEMOS DE NUESTRA CONEXIÓN A INTERNET; APRENDAMOS A SOLUCIONARLOS.



[01]

En primer lugar, en caso de que Windows nos indique que la conectividad es limitada o nula, podemos intentar deshabilitar la placa de red y, luego, habilitarla otra vez. Para realizar esta tarea, solo debemos dirigirnos al **Centro de redes y conectividad** del sistema operativo.

[02]

Si el paso anterior no soluciona el problema de conectividad, podemos ingresar en el modo consola (Inicio/Símbolo de Sistema) y ejecutar el comando `IPCONFIG /RELEASE` para liberar la conexión, `IPCONFIG /RENEW` para crear una nueva, o `IPCONFIG /FLUSHDNS` para borrar la caché de DNS y generar otra (en caso de que se hubiera dañado).

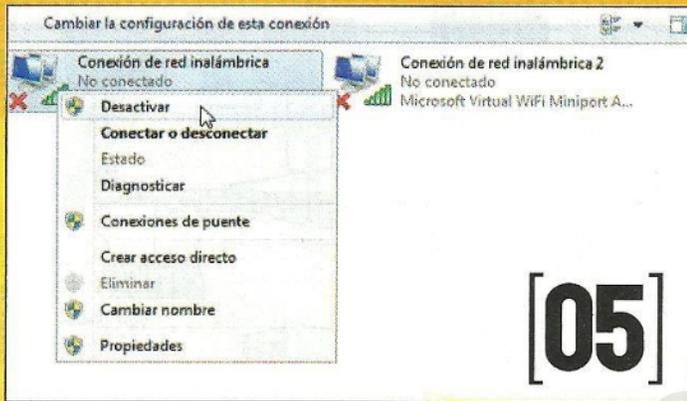
[03]

Si continuamos con el problema de conectividad, podemos apagar el módem/router, ya que puede ocurrir que este se haya colgado y haya que reiniciar las configuraciones. En todo caso, y si lo creemos necesario, podemos resetear su configuración con el botón destinado a tal fin, para descartar fallas.

[04]

Por el lado del hardware, podemos reemplazar el cable de teléfono o el cable de red (anteriormente vimos cómo armar un cable de red UTP para reemplazo). Otra alternativa posible, antes de cambiarlo, es probar su funcionamiento con un tester de red. Con esta simple prueba podemos descartar de inmediato si la falla se debe al cable de red o no.

ES POSIBLE QUE AL INSTALAR UN NUEVO SOFTWARE COMIENCE A FALLAR LA CONEXIÓN. EN ESOS CASOS HAY QUE COMPROBAR SI CAMBIÓ LA CONFIGURACIÓN.



```
C:\Users\Phantom>netstat
```

Conexiones activas

Proto	Dirección local	Dirección remota	Estado
TCP	127.0.0.1:49405	Phantom:49406	ESTABLISHED
TCP	127.0.0.1:49406	Phantom:49405	ESTABLISHED
TCP	192.168.1.5:55620	yx-in-f94:https	ESTABLISHED
TCP	192.168.1.5:55621	mia04s04-in-f0:https	ESTABLISHED
TCP	192.168.1.5:55622	mia05s01-in-f2:https	ESTABLISHED
TCP	192.168.1.5:55624	mia05s01-in-f5:https	ESTABLISHED
TCP	192.168.1.5:55822	LB140:http	TIME_WAIT
TCP	192.168.1.5:55844	209.17.88.139:http	TIME_WAIT
TCP	192.168.1.5:55875	mail:http	TIME_WAIT
TCP	192.168.1.5:55876	mail:http	TIME_WAIT
TCP	192.168.1.5:55877	mail:http	TIME_WAIT
TCP	192.168.1.5:55878	mail:http	TIME_WAIT
TCP	192.168.1.5:55879	mail:http	TIME_WAIT

[07]

[05]

[06]

[07]

En caso de que estemos intentando conectarnos por WiFi, podemos hacerlo por Ethernet (y viceversa), para descartar o confirmar una posible falla en la placa de red (ya sea wireless o cableada), y proceder a su reemplazo. Podemos activar y desactivar las tarjetas desde el Centro de redes y recursos compartidos de Windows.

Si tenemos un modem ADSL conectado a un router o switch, debemos probar el modem directamente en la PC, para descartar o confirmar la funcionalidad del router o switch. En la imagen vemos un modelo que sólo acepta una conexión de salida, sea router o PC. Si a pesar de todo, no logramos utilizar la conexión, no tendremos más remedio que comunicarnos con el servicio técnico de nuestro ISP, ya que la falla puede estar en el DSLAM de la central telefónica.

Puede suceder que la velocidad de navegación sea lenta; en este caso, lo que debemos hacer es cerrar todos los programas que usen la conexión y acceder a la consola (Inicio/Símbolo de Sistema), donde ejecutamos el comando netstat -a. La cantidad de conexiones y los protocolos de ellas nos dirán si estamos infectados con un virus o un malware/spyware.

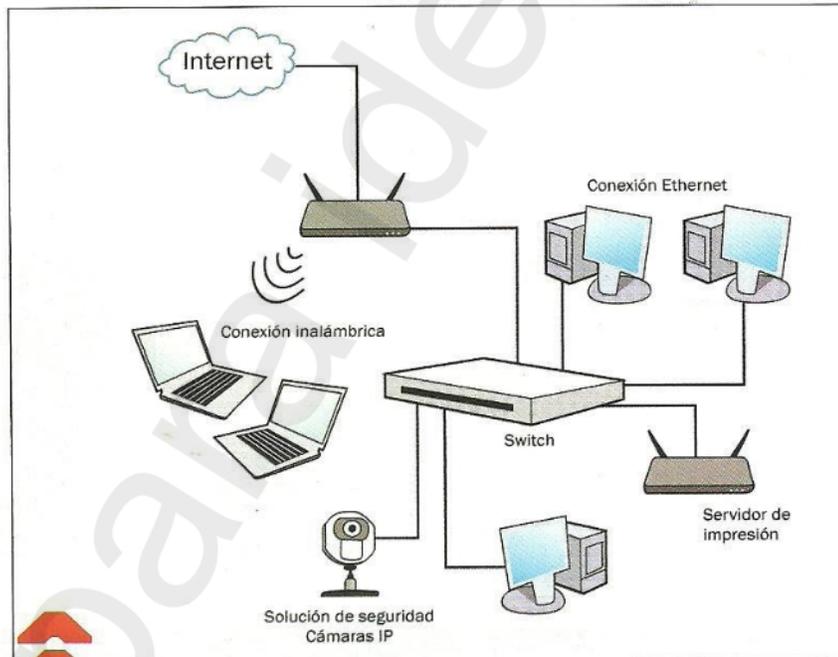
# Organizar y presupuestar una red hogareña

PARA ORGANIZAR UNA RED DEBEMOS SEGUIR ALGUNOS CONSEJOS QUE COMENTAMOS.

Al enfrentarnos a la tarea de crear una red de computadoras, lo primero que necesitamos, es identificar cada uno de los equipos y dispositivos que conformarán la red de datos. Por otra parte, también precisamos conocer las ubicaciones en las cuales estará cada dispositivo; de esta forma, podremos determinar qué tipo de hardware se requiere, por ejemplo, computadoras, notebooks, router y switch, entre otros. En este punto es una buena idea generar un listado detallado de cada uno de los equipos y dispositivos que integrarán la red. Este listado nos permitirá efectuar las cotizaciones correspondientes antes de adquirir lo que necesitamos.

## CABLES Y ACCESORIOS

Una vez que logremos identificar los equipos que se conectarán y los dispositivos a instalar, deberíamos realizar un croquis con las distancias que debe recorrer el cableado y la señal WiFi.



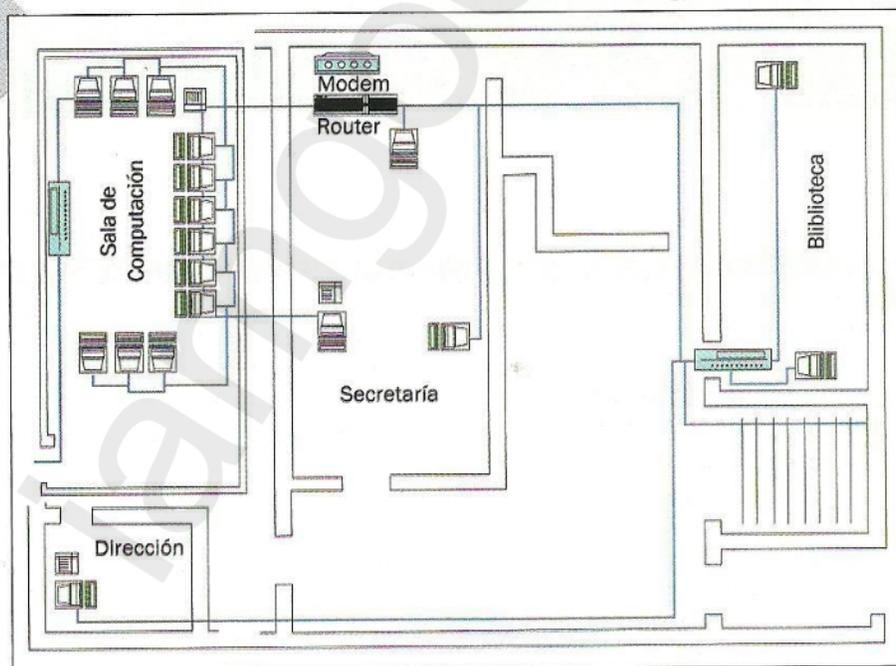
**Diagrama.** Un esquema como este nos permite generar un listado con los dispositivos de conexión que necesitamos para nuestra red.

Así podremos calcular los repetidores que puedan hacer falta y la cantidad de cable necesario para nuestra red. Una vez realizado esto, agregamos estos elementos al listado de materiales.

A la hora de calcular el metraje de cableado es conveniente agregar entre un 10 y un 20 por ciento de longitud por cualquier imprevisto que pueda surgir, como toparnos con una viga de hierro u hormigón que pueda bloquearnos el recorrido planeado originalmente. También debemos tener en cuenta los accesorios, por ejemplo: fichas RJ-45, cablecanal, codos, tapas, uniones, tarjetas de red y de WiFi, entre otros.

## PARA FINALIZAR

Una vez que listemos los elementos necesarios y hayamos decidido la organización de la red plasmándola en un croquis, podemos calcular los costos totales de su implementación.



**Croquis.** Establecemos la ubicación de los equipos, y calculamos la cantidad de cable y accesorios necesarios.