Introducción a las redes

Desde la creación de la computadora y el manejo de la información en forma electrónica 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. Esta red 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 fines de las redes son extremadamente variados y, con la difusión que fueron alcanzando, surgieron tecnologías de intercambio masivo. En un principio, estas se limitaban a redes reducidas, compartidas 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.

> UNA RED PERMITE COMUNICAR DISPOSITIVOS DE MANERA FÍSICA O INALÁMBRICA

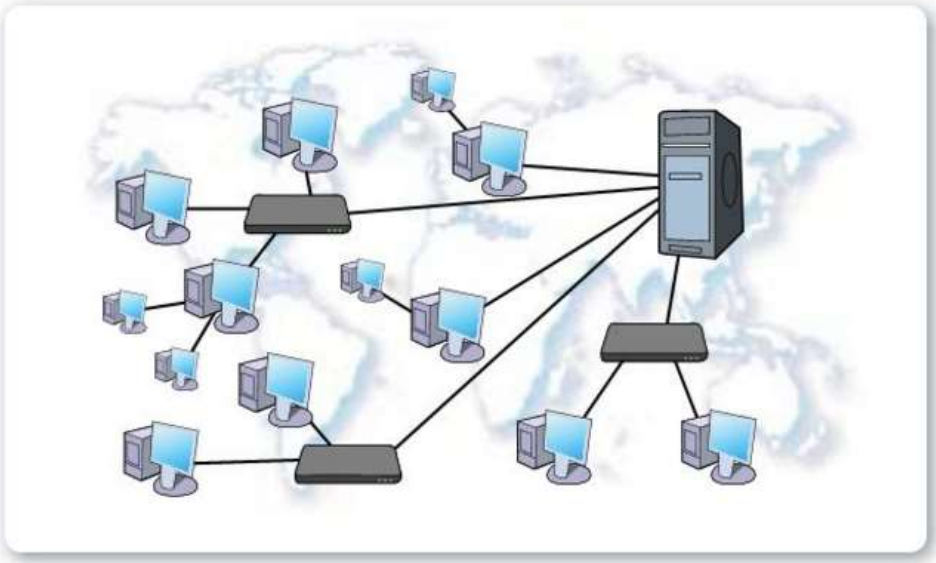


Figura 1. Esquema de las redes de mayores dimensiones o WAN (Wide Area Network, Red de Área Extensa).

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 al más común y más difundido 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 el medio por el cual se intercambia la información definen a una red.

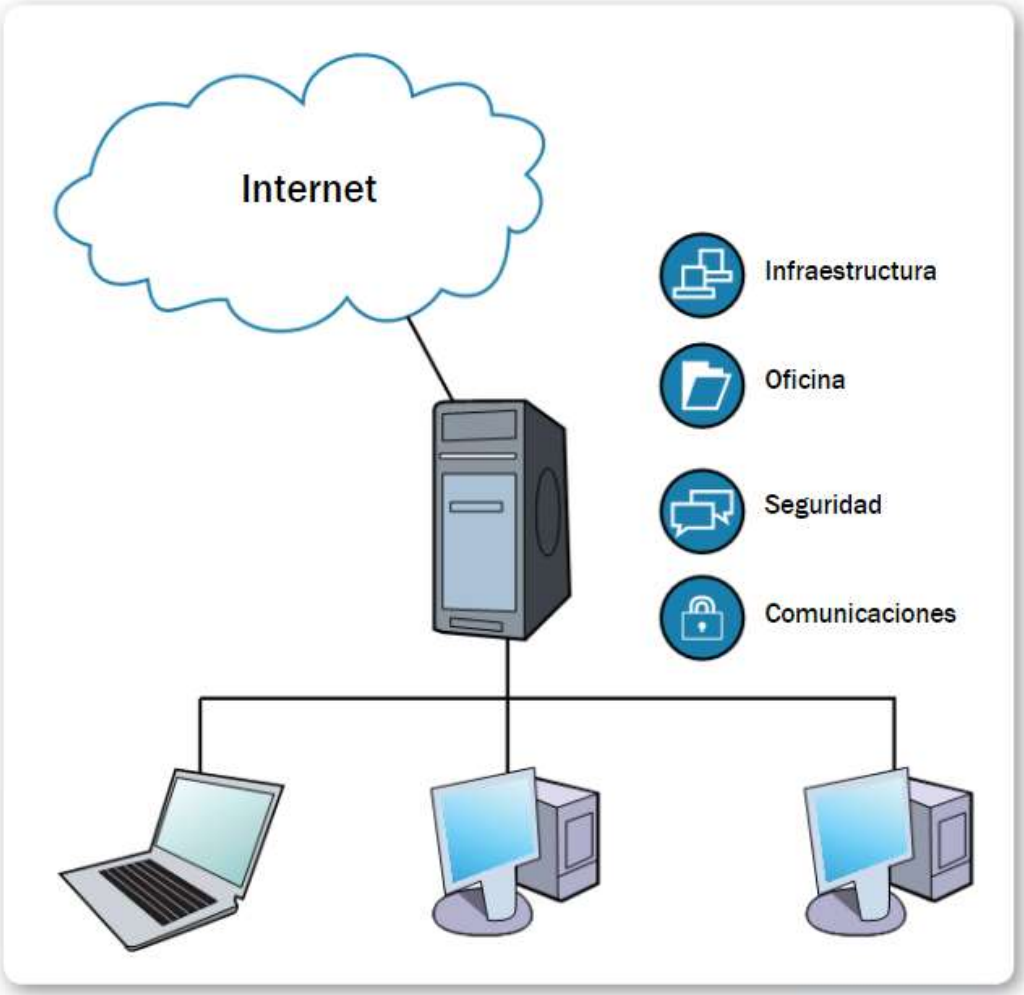


Figura 2. Configuración básica de una LAN(Local Area Network, Red de Área Local).

Si revisamos en cada casa u oficina encontraremos una combinación muy habitual, que consta de una entrada de internet (a través de un proveedor de acceso) 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 a 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.

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 nuestra computadora.

> GRACIAS A UNA RED PODEMOS DISTRIBUIR INTERNET ENTRE VARIOS DISPOSITIVOS

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

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 incrementar 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.



Figura 3. Mediante un switch podemos configurar la red para que todos los equipos accedan a internet.

En 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 según un fin determinado; por ejemplo, un empleado podrá manejar un programa pero no contará con acceso a internet. Debemos considerar que hoy en día es posible sincronizar información a través de internet y manejarnos en redes mucho más amplias, para acceder a ellas desde nuestro hogar o desde un bar.

IoT, conectando objetos: proyecciones

En la actualidad, las redes informáticas nos permiten estar conectados a un equipo ubicado a distancias antes no imaginadas, acceder a la información sin espera y comunicarnos al instante con otras personas. Cada vez se hace más presente el uso de un concepto que se utiliza en las redes, los chips con sensores y los beneficios de la nube: el IoT (Internet de las Cosas). Esta iniciativa, es la que permitirá conectar e interactuar con diversos objetos, electrodomesticos y equipos vestibles con los usuarios.

Por eso, más allá de programar tareas, acceder remotamente a equipos y controlarlos, podemos decir que el futuro de las redes recién comienza a escribirse.



Figura 4. Los equipos informáticos deben contar con una interfaz de red para compartir contenidos.

Topologías

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 cuellos de botella, nodos o el uso de determinados dispositivos. Con los años se ha optimizado el flujo de información y se economizaron los métodos y medios de conexión.

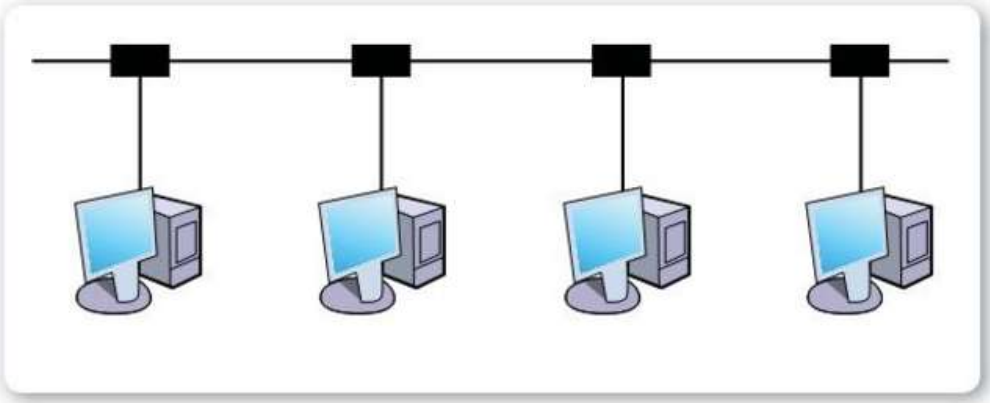


Figura 5. Topología básica en línea.

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 de este tipo de conexión implica que, básicamente, un paquete es enviado y presentado ante todas las computadoras, las cuales se encargarán de analizar la dirección que se encuentra en el paquete para determinar si les corresponde a ellas o no.

> LA TOPOLOGÍA DE BUS POSEE LOS DISPOSITIVOS CONECTADOS A UNA ÚNICA LÍNEA

Ventajas

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

Desventajas

- Las computadoras no regeneran la señal, por lo que hay ruidos y pérdida de fidelidad con la distancia.
- Esta topología es dependiente de todas las estaciones, de modo que un usuario desconectado corta la red.

Topología en estrella

La topología en estrella es una de las más comunes (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 alguna terminal y redireccionarla hasta su destino. Detecta errores y los corrige.

REDES INALÁMBRICAS

Las redes inalámbricas admiten la conexión de un sinfín 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 y acceder a ellos desde cualquier localización.

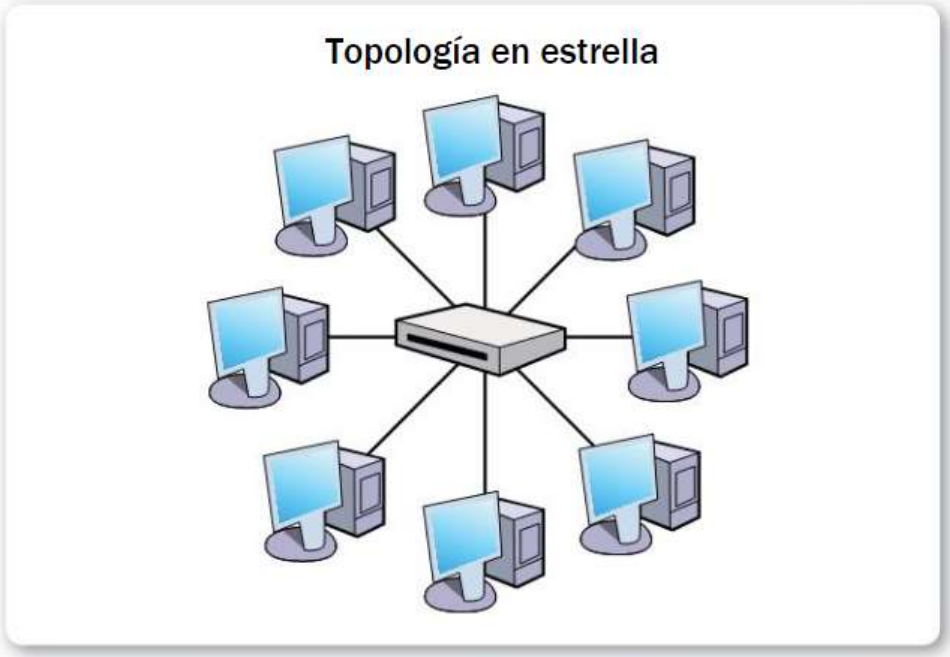


Figura 6. La más difundida y aplicada en redes hogareñas y corporativas de tamaño medio.

Ventajas

- Si una terminal pierde conexión o esta finaliza, la red no se inutiliza, sino que sigue funcionando normalmente.
- No se pierde la conexión al incorporar o retirar dispositivos.

Desventajas

- Esta topología 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 fuera de servicio.

ESTRELLA EXTENDIDA

Esta topología es igual a la topología en estrella excepto en que, a diferencia de esta, en la estrella extendida cada nodo puede ser el nodo principal de las demás máquinas. De esta manera, se pueden formar varias estrellas que se conectan entre sí por los nodos principales, entregándonos la posibilidad de escalar la red en forma sencilla, uniendo simplemente diferentes redes que se encuentran implementadas con la topología de estrella.

Topología en anillo

En esta configuración, las 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.

> EN LA TOPOLOGÍA ANILLO, LOS PROBLEMAS SON FÁCILES DE DETECTAR Y RESOLVER

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 y es más fiable.

Desventajas

- La incorporación de una nueva computadora implica romper el anillo y la red, teniendo que redefinir su implementación.
- El soporte técnico para este tipo de conexión requiere desactivar la red para solucionar conflictos.

Topología mesh

En este caso, 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 de la red se encuentran interconectadas directamente, sin intermediarios.

Desventajas

- Las conexiones son costosas y se requiere demasiado cable.
- Cada dispositivo conectado a la red debe tener tantas placas de red como computadoras encontremos conectadas.



Figura 7. Equipos como los routers son comunes para conectar dispositivos móviles.

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 se alejan, se pierde la fidelidad de la información y la señal.

Ventajas

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

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 elegir la más conveniente.

Desventajas

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

Topología de infraestructura

Esta arquitectura requiere de un elemento que coordine y sirva como punto base de información: una estación central inalámbrica. Si los elementos están bajo el mismo SSID (nombre de red), tendrán acceso.

Ventajas

- Pueden interconectarse redes Ethernet y redes inalámbricas.
- El elemento central (access point o router) coordina la información con más eficiencia.
- Pueden usarse repetidores cableados o inalámbricos de la red.

Desventajas

- El equipamiento físico es más costoso.

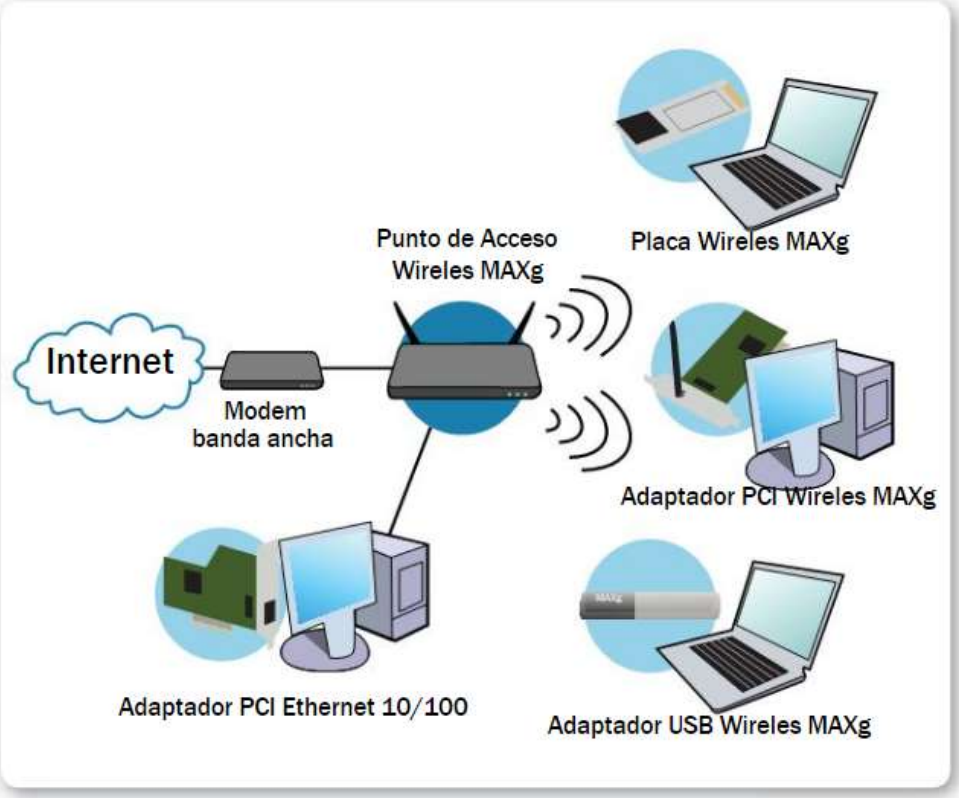


Figura 8. Infraestructura que combina conexiones Ethernet e inalámbricas.

El modelo OSI

Para resolver cómo se comunican las computadoras, se definió un modelo de interconexión entre dispositivos abiertos (Open System Intercommunication); es decir, un modelo que determine cómo se lee, con el fin de que todos los receptores entiendan el mensaje y haya compatibilidad entre ellos. En otras palabras: el modelo define 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.

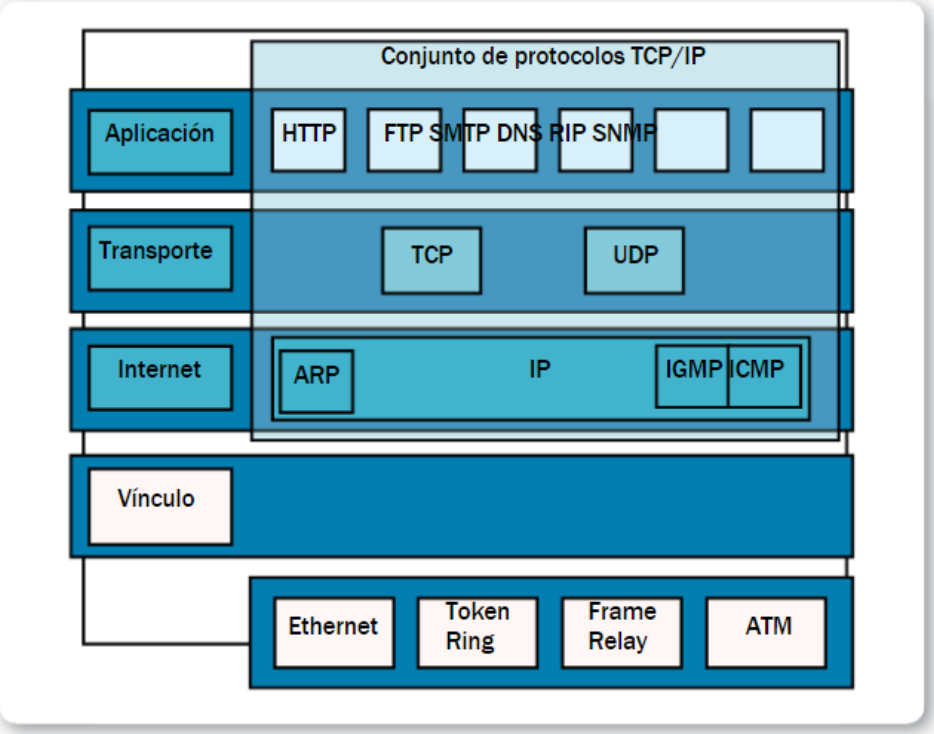


Figura 9. A cada capa se le asocian diferentes protocolos comúnmente utilizados por las aplicaciones.

Capas

- Capa física : define el medio físico (cableado, placas, routers) por el cual se llevan a cabo las comunicaciones dentro de una red y la forma en que esta se realiza.
- 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 permite identificar paridad y congruencia de datos.
- Capa de red : identifica el enrutamiento entre varias redes. Lo que busca esta capa es garantizar que la información 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 : esta capa se encarga de realizar el transporte de 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 es interrumpida.
- Capa de presentación : su función es presentar los paquetes de información de manera legible y entendible a la 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. Debemos considerar que cada aplicación requiere diferentes protocolos que, luego, serán usados por distintas capas.

> EN LA CAPA FÍSICA SE DEFINE EL MEDIO FÍSICO POR EL CUAL SE REALIZARÁ LA COMUNICACIÓN

CAPA 8

Debemos tener en cuenta que el modelo OSI contempla el modo en que se maneja la información, el uso y el destino, pero no se refiere al operador. En la cultura popular se denomina capa 8 al factor humano, que puede inferir de manera directa produciendo errores o, incluso, acelerando el proceso. No es parte del estándar pero, sin duda, es un factor determinante.



Figura 10. Los routers están definidos en la capa de red del modelo OSI.

Las normas Ethernet

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.

> LAS NORMAS INCREMENTARON LA VELOCIDAD DE TRANSFERENCIA A TRAVÉS DE LOS AÑOS

Consideremos que 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 y cables con 8 hilos conductores (cable UTP con cuatro pares trenzados) hasta fibra óptica. También recordemos que los puertos terminales son placas o interfaces de red que se encuentran preparadas para funcionar con ellos, y que derivan en concentradores o switches que se distribuyen a toda la red de datos.

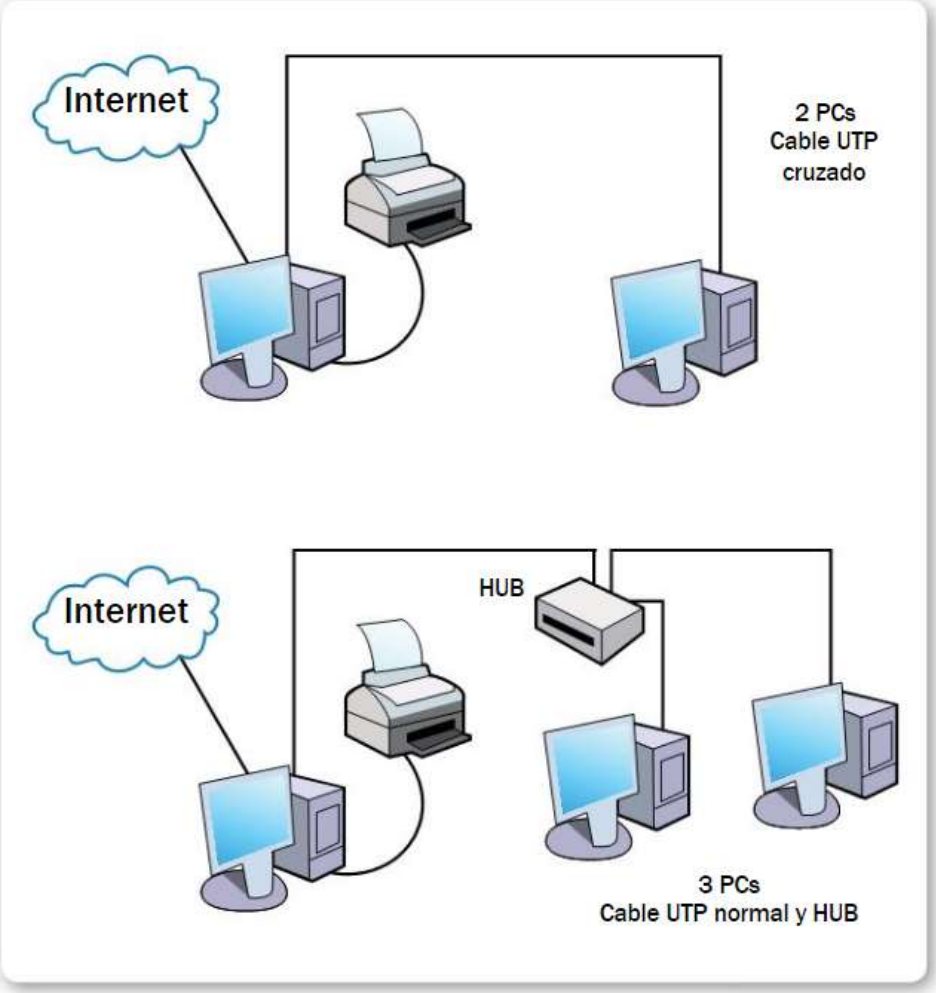


Figura 11. Forma básica de configuración de una red bajo el modelo Ethernet, con dos configuraciones y un switch.

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):

- 10BaseT (capacidad de transmisión - banda base - distancia máxima o medio físico): surge debido a que las versiones anteriores presentaban 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 ocho hilos pero solo emplea cuatro: dos para recepción y dos para envío de datos. El resto se usa, opcionalmente, para telefonía y video. Recordemos que el ancho de banda permitido es de 25 MHz y 100 Mbps. Por otra parte, la longitud máxima del cableado es de 100 metros.
- 1000BaseT : se diferencia, principalmente, por el uso de los cuatro 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 cuya exigencia es más amplia; la tasa de transferencia es de 1Gbit/s. La principal diferencia con los modelos anteriores es que requiere cableado categoría 6, más costoso de actualizar, por lo que se sigue prefiriendo la norma 1000BaseT que usa cables categoría 5.

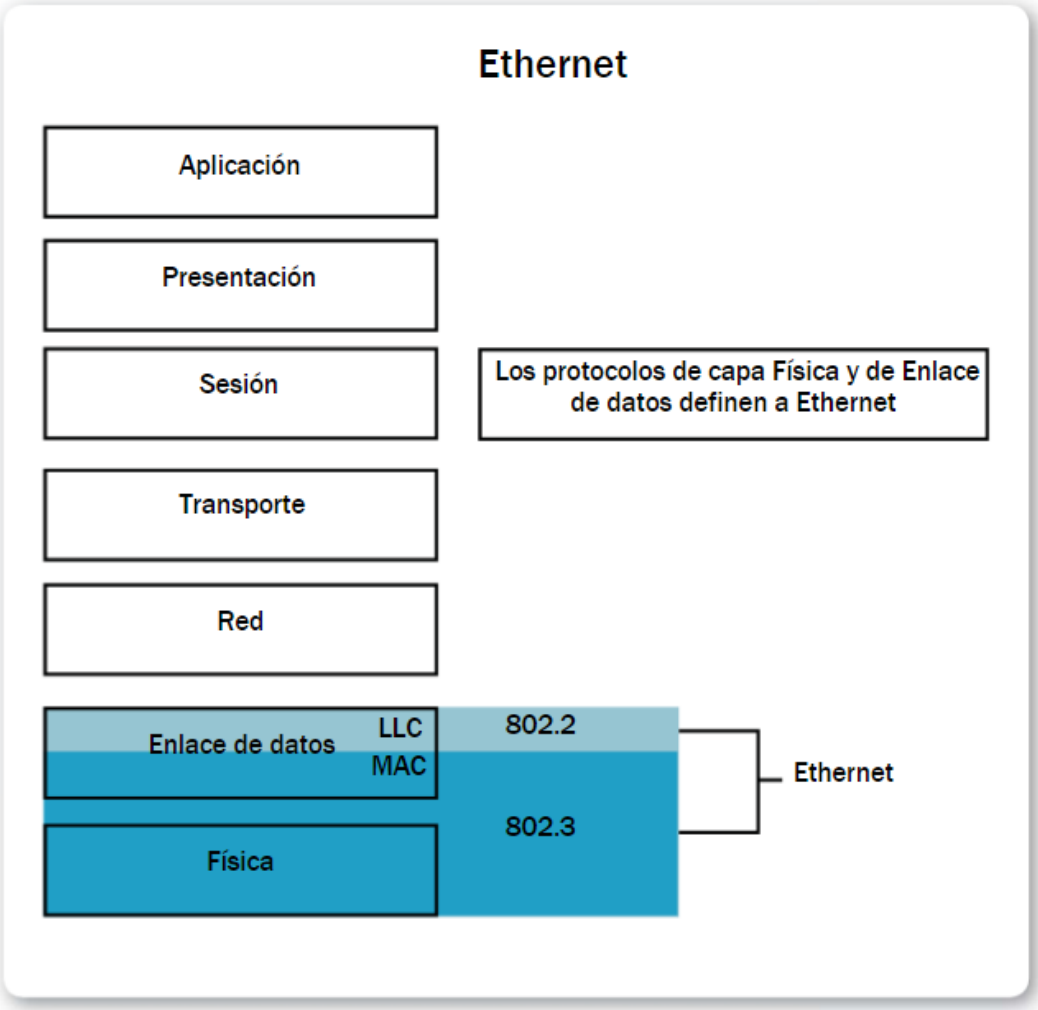


Figura 12. Esquema que abarca la norma 802.3 y la capa física de Ethernet.

El protocolo TCP/IP

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.

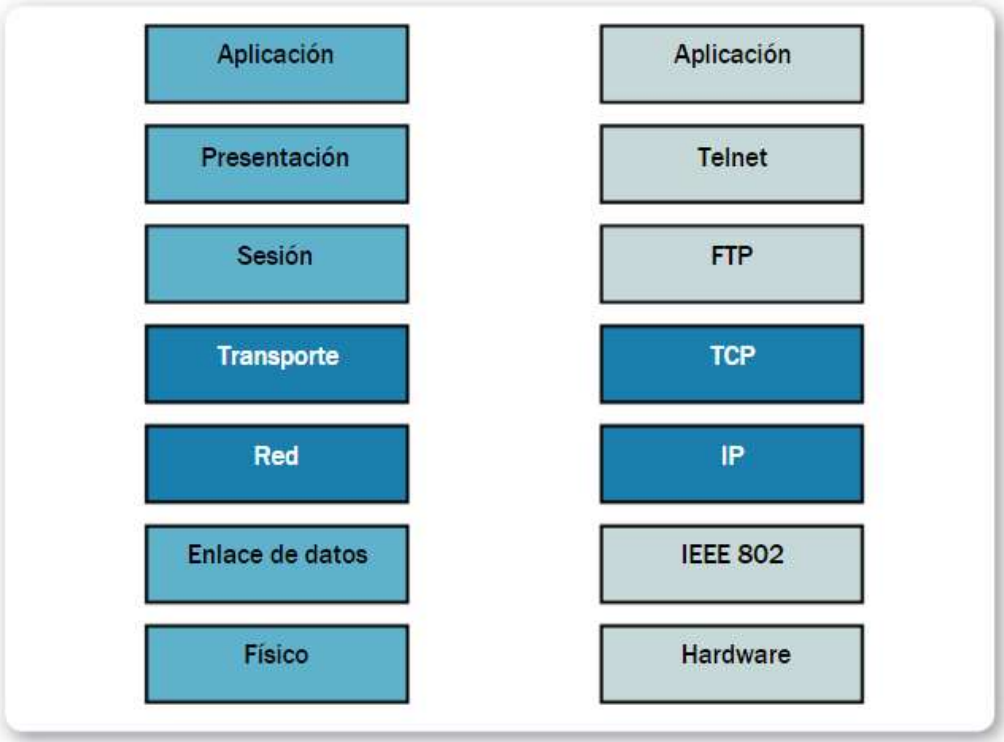


Figura 13. Correspondencia funcional entre el modelo de niveles OSI y las capas protocolares TCP/IP.

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 independientemente de su soporte, tipo y sistema operativo. 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, que establece pautas precisas y pasos ordenados de comunicación, y que tiene vigencia internacional.

EL PROTOCOLO TCP/IP PERMITE QUE VARIOS SISTEMAS COEXISTAN EN LA RED

Para ser más precisos, el protocolo TCP/IP hace posible que un servidor que funciona bajo el sistema operativo Linux reconozca una computadora Windows en la red y que esta, a su vez, pueda comunicarse con otra bajo el SO de Apple sin que se produzcan conflictos en el reconocimiento. 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

Es importante definir que el protocolo TCP es el encargado de controlar la fiabilidad de los datos transmitidos. Recordemos que la conexión dentro de la red se realiza a través de datos transmitidos en flujos ordenados que tienen un principio y un final. Este protocolo se ocupa de resguardar el orden, identificar los errores, y establecer el puerto y las aplicaciones que le darán curso en su destino.



Figura 14. La mayoría de los dispositivos, como las impresoras de red, utilizan el protocolo TCP/IP para comunicarse.

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 cuatro 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).

Dispositivos para redes cableadas

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, ya 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.

FUTURO DE ETHERNET

En la actualidad se han alcanzado velocidades máximas de transferencias de 10 Gbps, pero se están desarrollando tecnologías de varios Gigabits con velocidades de 40, 100 y 160 Gbps. Sin embargo, su implementación dependerá del costo y de la evolución tecnológica. En caso de ser factible, surgirán nuevas modificaciones a la norma, y los medios físicos serán aún más versátiles.



Figura 15. El router posibilita las extensiones de WAN por medio de wireless o Ethernet.

Tarjeta de red

La tarjeta o interfaz de red es 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 también ExpressCard, entre otras opciones. 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, que es incorporado 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.

DIRECCION MAC

Cada tarjeta o interfaz de red tiene un número de identificación único de 48 bits en hexadecimal, llamado dirección MAC. Estas direcciones de hardware únicas son administradas por el Institute of Electronic and Electrical Engineers (IEEE). Los tres primeros octetos del número son conocidos como OUI y se encargan de identificar a proveedores específicos.



Figura 16. En redes cableadas, hay un puerto Ethernet para conectar por medio de fichas RJ-45 al motherboard.

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, el aumento 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 tal de separar grupos de dispositivos en redes virtuales o VLAN.

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

PARA CREAR NUESTRA RED, CONFIGURAREMOS CORRECTAMENTE EL ROUTER

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.

Es necesario saber que configurar nuestra propia red puede ser tan complicado o simple como queramos. Para realizar esta tarea, lo primero que debemos hacer es configurar correctamente nuestro router hogareño.

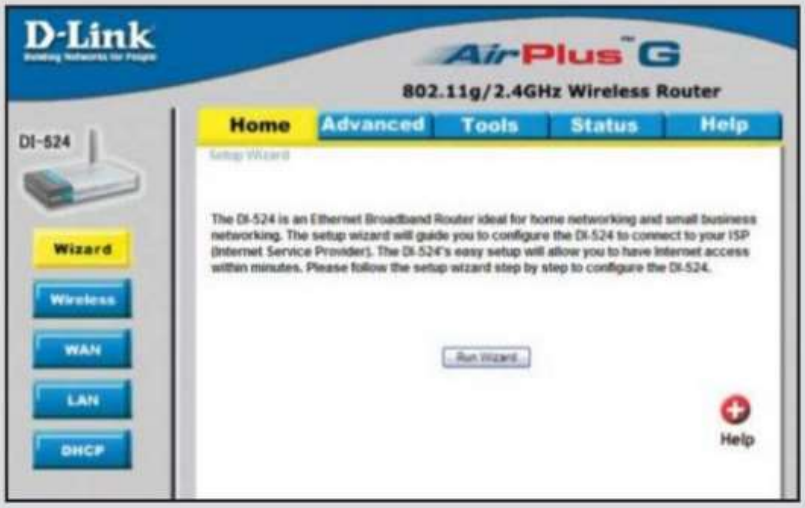
Veamos la manera adecuada de hacerlo, tomando como ejemplo un modelo de la empresa D-Link:

PAP: CONFIGURAR UN ROUTER HOGAREÑO

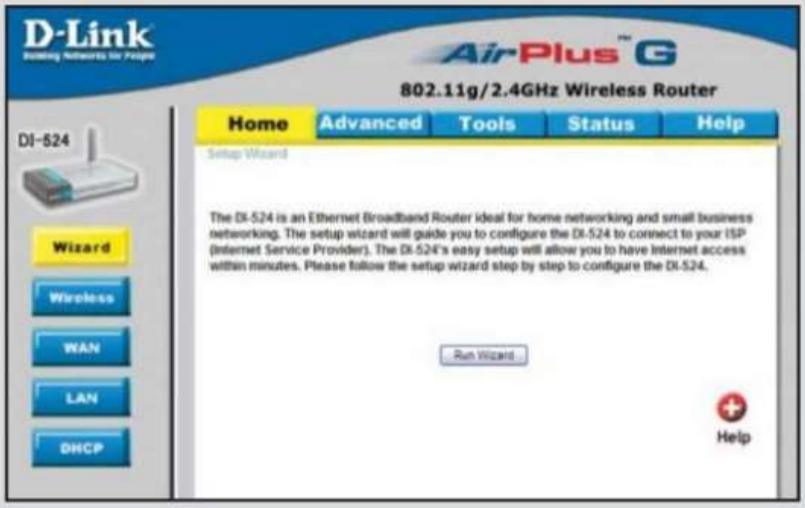
01 Básicamente, los asistentes de configuración son similares en la mayoría de los dispositivos, por lo que se tomará como ejemplo el modelo D-Link DI-524 . Empiece por conectar la antena y el cable de corriente (a la entrada WAN se conecta un cable de red que proviene del módem, ya sea cablemódem o ADSL).



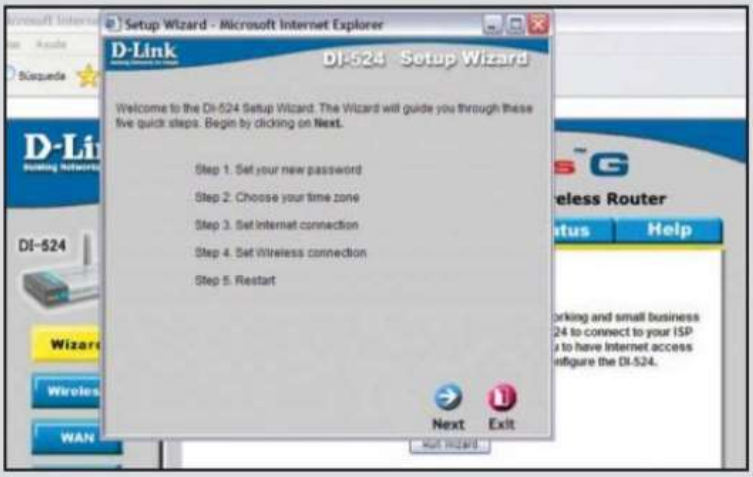
02 Para la primera configuración, conecte un cable de red a uno de los puertos Ethernet del router, y este a la placa de red de la PC. Abra el navegador e ingrese la dirección IP del router, tal como se observa en la imagen.



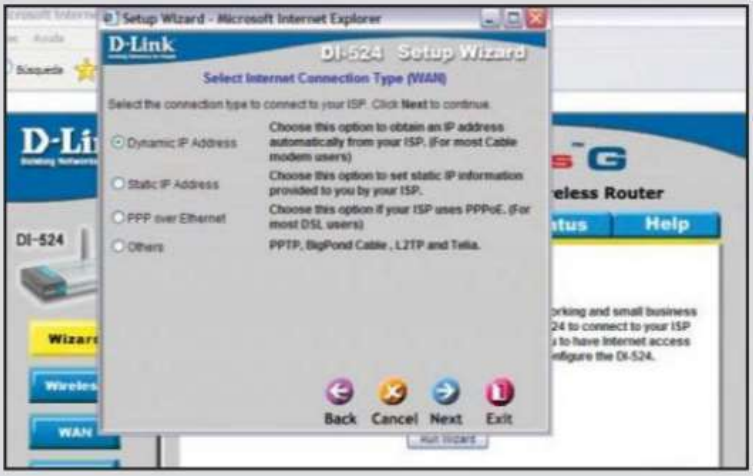
03 Se le pedirá usuario y contraseña, que encontrará en el manual (en este punto, los datos pueden variar de un fabricante a otro). Una vez hecho esto, corra el asistente para poner la red WiFi en funcionamiento.



04 En el primer paso se le solicitará cambiar la contraseña de acceso al router, procedimiento más que recomendable para mantener cierto grado de seguridad en la red. Luego debe seleccionar la zona horaria.



05 Si se encuentra frente a un cablemódem o módem ADSL, al configurar la conexión a internet debe seleccionar la opción que recibe la IP dinámica (que nada tiene que ver con las direcciones privadas).



06 Ahora debe configurar los parámetros de WiFi. Complete el campo SSID con el nombre mediante el cual el sistema operativo verá la red; no hace falta cambiar el canal de transmisión ni modificar nada en Encriptación.



07 En la sección Wireless deberá cambiar el tipo de seguridad. La opción que brindará el mayor grado de resguardo es WPA2(AES), que cuenta con un algoritmo de cifrado de 128 bits.



Para terminar, si queremos asegurarnos de que nadie pueda "colgarse" de nuestra conexión WiFi, en el menú Wireless dentro del apartado Advanced o Avanzado, podemos determinar que el router no transmita el SSID. De este modo, la red no será visible para Microsoft Windows, y tendremos que configurar nuestro acceso para conectarnos a redes que no transmitan SSID.

Hub

Es un dispositivo que ha caído en desuso desde hace años. Permite la conexión de varias PCs 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. Los hubs cuentan con conexiones que van desde los 4 a los 32 puertos, pero tengamos en cuenta que, al no disponer de una tabla de direcciones, a mayor cantidad de computadoras conectadas al hub, mayores son las posibilidades de colisiones de datos.

EN LA ACTUALIDAD LOS HUBS HAN SIDO REEMPLAZADOS POR SWITCHS O ROUTERS

Repetidor

Básicamente, es un dispositivo que recibe una señal media o baja y la retransmite ampliada. 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.

CONCENTRADORES

Hace algún tiempo los concentradores sufrieron el problema de que, como simples repetidores, solo podían soportar una única velocidad. Pero, mientras que las PC con ranuras de expansión pueden ser fácilmente actualizadas a Fast Ethernet con una nueva tarjeta de red, máquinas con menos mecanismos de expansión comunes, como impresoras, pueden ser costosas o imposibles de actualizar.

Gateway

El gateway es un dispositivo nodo que puede encontrarse dentro de la red local, y sirve para enlazar con otra red que presenta un 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. Mencionaremos como el ejemplo más habitual la conexión de una red hogareña a internet, tarea que puede ser realizada sin complicaciones mediante el uso de un gateway.

> EL GATEWAY PERMITE REALIZAR LA CONEXIÓN DE REDES CON PROTOCOLOS DIFERENTES



Figura 17. El hub es obsoleto, pero útil en pequeñas redes hogareñas o en espacios de trabajo reducidos.

FIBRA ÓPTICA PARA INTERNET

A mediados del siglo XIX, el joven multimillonario inglés 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.

Cables de red

Los cables de par trenzado son filamentos de cobre entrelazados. Debemos considerar que esta transposición en los filamentos de cobre permite equilibrar el nivel de interferencias de otros conductores de corriente electromagnética adyacentes.

Par trenzado

Entre los tipos de par trenzado existentes encontramos los que mencionamos a continuación:

- 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 sino global, es decir que abarca todo el conjunto de pares trenzados.

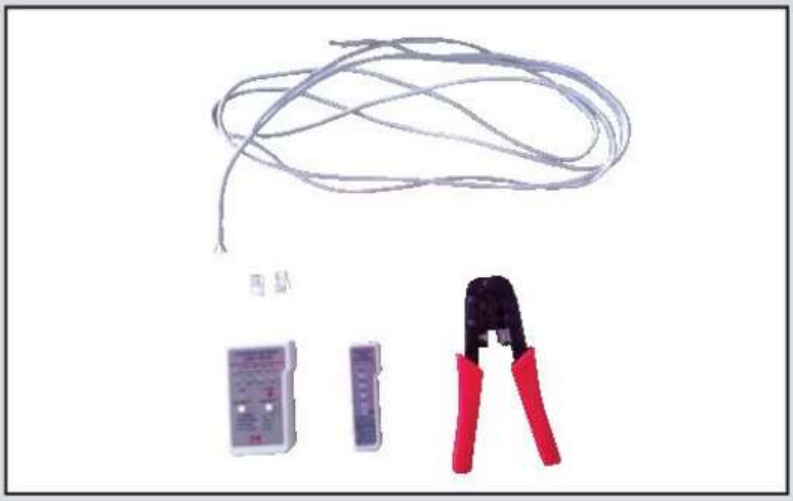
Es importante tener en cuenta que los cables de red con los que damos conectividad a nuestros equipos pueden romperse por varios motivos. Por esta razón, debemos saber cómo crear cables nuevos. En el siguiente Paso a paso veremos cómo podemos reemplazarlos.

HISTORIA DEL CABLE UTP

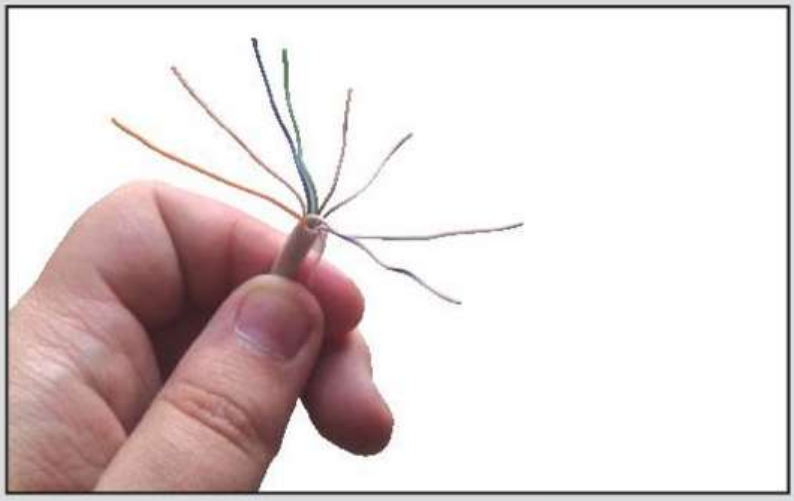
Es importante saber que, en la historia de las telecomunicaciones, el cable UTP ha tenido un rol fundamental. Este tipo de cable es el más común y se originó como la solución para realizar la conexión de teléfonos, terminales y ordenadores sobre el mismo cableado, ya que está habilitado para comunicación de datos permitiendo frecuencias con más altas transmisiones. Con anterioridad, en Europa, los sistemas de telefonía empleaban cables de pares no trenzados para poder comunicarse.

PAP: CREAR UN CABLE DE RED

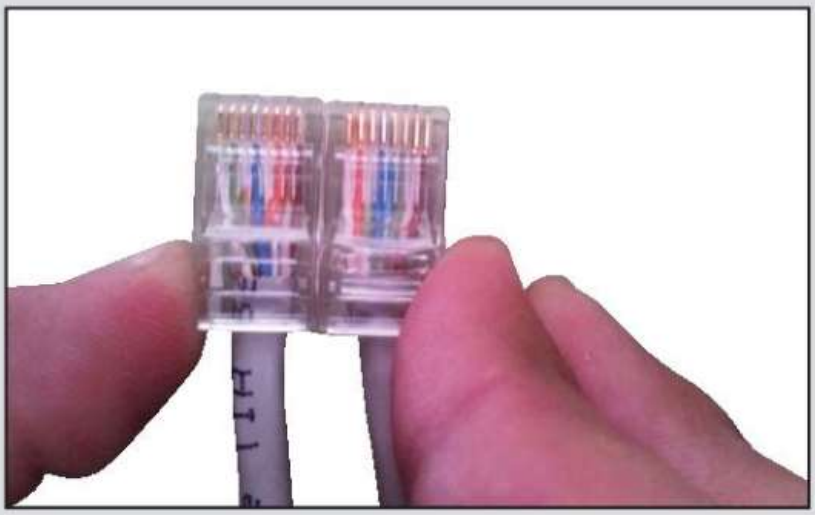
01 Primero, tenga a mano los elementos necesarios: pinza crimpeadora, tester de red, fichas RJ-45 y cable UTP categoría 5 (cantidad necesaria).



02 Con la pinza crimpeadora, corte y retire unos 2 cm de vaina protectora que recubren los 4 pares del cable UTP; sepárelos y acomódelos de acuerdo a la norma que necesita (T568A o T568B).



03 Una vez ordenados los pares, colóquelos en orden en la ficha RJ-45. Para continuar, coloque la ficha con el cable insertado en la ranura correspondiente de la crimpeadora, para realizar el cierre de la ficha y la consiguiente fijación del cable.



Aclaración importante: en la actualidad, el hardware de red tiene la capacidad de identificar el tipo de norma requerida; por lo tanto, no es necesaria la diferencia entre patch cord y cross over. No todos tienen dicha capacidad, por lo que no debemos asumirla directamente.

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

PAR TRENZADO

Los cables de par trenzado fueron inventados por Alexander Graham Bell en el año 1881. En el año 1900, el conjunto de la red estadounidense de la línea telefónica era de par trenzado o hilo abierto, con la transposición a la protección contra interferencias.

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 realizar la transmisión de las señales televisivas por cable. También algunos proveedores de internet lo usan para lo que denominamos conexión de cablemódem .

> EL CABLE COAXIAL ES USADO POR PROVEEDORES DE TELEVISIÓN E INTERNET

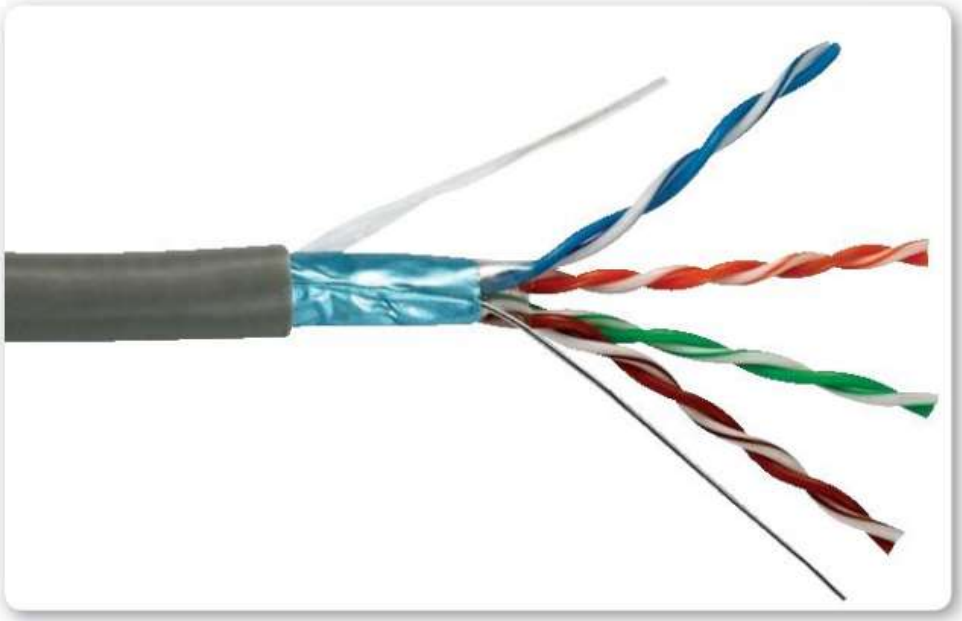


Figura 18. La elección de cable blindado o de UTP está determinada por el presupuesto y la seguridad.

COMPATIBILIDAD ELECTROMAGNÉTICA

Entre los problemas que buscan solucionar los diferentes tipos de cable se encuentra el de la diafonía . Este fenómeno se produce naturalmente 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 perturba por ruido cuando se captan señales no inteligibles.

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. Su alta fiabilidad hace que se lo emplee en la transmisión de grandes cantidades de datos, a grandes distancias.



Figura 19. El coaxial es menos implementado que el par trenzado o el óptico, pero útil en algunos dispositivos.

CODIFICACIÓN DE SEÑALES

Es interesante tener en cuenta que el uso de la luz para la codificación de señales no es una tecnología nueva: ya los antiguos griegos se encargaban de utilizar espejos para transmitir información, de modo rudimentario, usando luz solar. En el año 1792, Claude Chappe diseñó un sistema de telegrafía óptica que, mediante el uso de un código, torres y espejos distribuidos a lo largo de los 200 km que separan Lille y París, conseguía transmitir un mensaje en tan solo 16 minutos.

Redes inalámbricas y normas 802.11

En el inicio de las redes informáticas, cuando solo existía una cantidad limitada de computadoras en lugares privilegiados del mundo, las conexiones se realizaban mediante extensiones de cable de proporciones impensadas. Hoy por hoy, la tecnología nos permite reducir las conexiones cableadas, y se están disminuyendo las distancias, quitando elementos físicos e incrementando la conectividad.



Figura 20. Los rack son elementos usados para establecer redes cableadas con servidores en determinados sectores.

Evolución

La evolución de las redes se inició a partir de que el usuario común tuvo acceso a ellas y generó la necesidad de una mayor disponibilidad de conectividad. Cuando el grupo de personas con acceso a la red no tenía las dimensiones actuales, los requerimientos eran cubiertos con redes de menor velocidad y tamaño, que contaban con un dispositivo (de, en promedio, cuatro a ocho puertos) que se conectaba mediante un cable de red hasta el terminal (computadora, generalmente), y

problema solucionado. Al extenderse este grupo, es normal encontrar por domicilio más de 8 dispositivos (si consideramos que hoy en día la conectividad llega a electrodomésticos, televisores, celulares e impresoras) y, a su vez, cada una de ellas ya no pertenece a un lugar fijo por un período prolongado de tiempo. Así, depender de un cable fijo generó limitaciones, principalmente de espacios y conexiones. Para enfrentar este nuevo inconveniente, hubo que investigar otras alternativas que permitieran la intercomunicación rompiendo las limitaciones. Prevalecieron entonces dos tipos de conectividad: las tecnologías Bluetooth y WiFi (marca de la WiFi Alliance que adopta, prueba y certifica que los equipos cumplen los estándares 802.11).



Figura 21. Router potenciado para realizar conexiones inalámbricas estables.

Estándar

El estándar WiFi permitió distinguir algunas características entre una red cableada y una inalámbrica.

Red cableada

- Requiere grandes cantidades de cable para interconectar un gran número de computadoras.
- Permite longitudes máximas de cableado de hasta 100 metros.

- Requiere interfaces de red instaladas en todas las placas madre de las computadoras.
- El número máximo de computadoras conectadas a la misma red está limitado a la cantidad máxima de puertos de los routers y switches.
- La velocidad de transferencia depende del adaptador, pero puede ir de 100 Mb/s a 1000 Mb/s.

Red inalámbrica

- No requiere cables de ningún tipo para conectarse a la red.
- El alcance es variable y depende, fundamentalmente, de tres factores: la potencia del Access Point (o router WiFi) para trasmitir la señal, la distancia implicada y la cantidad de objetos interpuestos entre este y el dispositivo que se desea conectar.
- Algunos dispositivos vienen incorporados con interfaces inalámbricas, pero, de no contar con una, se puede adquirir un adaptador WiFi.
- Cada router tiene una capacidad muy alta de conexiones simultáneas (este número está limitado por el modelo y la cantidad máxima de direcciones IP asignables).
- La velocidad de conexión depende de la intensidad de la señal, pudiendo ser de 8 Mbps a 600 Mbps como máximo.

Tecnologías

Cada tipo de red inalámbrica se maneja con estándares de funcionamiento 802.11 que definen la tecnología para establecer las comunicaciones. Esta norma especifica el funcionamiento de las redes WLAN y, a lo largo del tiempo, se ha modificado identificándose con letras desde la "a" hasta la "w". Las siguientes son las más importantes:



MEJORAR LA CONECTIVIDAD

Algunos proveedores de internet ofrecen la tecnología WiMAX, que funciona de manera inalámbrica mediante microondas y retransmisión por ondas de radio, y trabaja bajo el estándar 802.16. La principal ventaja es que no requiere cableado para funcionar. Paralelamente, el cableado se optimiza mediante fibra óptica, lo que mejora la velocidad y la calidad de la información. En el futuro, las tecnologías cableada e inalámbrica seguirán coexistiendo, pero con importantes mejoras.

- a: la primera revisión de la norma 802.11 que establece protocolos; funciona en 5 GHz y tiene una velocidad máxima de 5 Mb/s. Posee 12 canales: 8 para red inalámbrica y 4 para conexiones fijas.
- b: al ser una revisión, mejora determinadas particularidades. Incrementa la velocidad a 11 Mb/s. Cambia a la banda de 2,4 GHz.
- g: como cambio del estándar 802.11b, mejora la velocidad teórica a 54 Mb/s y es compatible con la norma "b", a diferencia de la "a", que no lo es con ninguna. Una singularidad clave es que, con equipos adecuados, alcanza una distancia de hasta 50 km.
- n: implica una mejora importante porque la velocidad real puede llegar hasta los 600 Mb/s y se incrementa el alcance. A su vez, se la diseñó para funcionar en dos bandas de frecuencia, la de 2,4 GHz y la de 5 GHz, haciéndola compatible con todas las versiones anteriores.

Debemos tener en cuenta que ambas redes, cableadas e inalámbricas coexisten y coexistirán en el futuro, debido a que presentan utilidad, son necesarias y la tecnología lo sigue permitiendo.

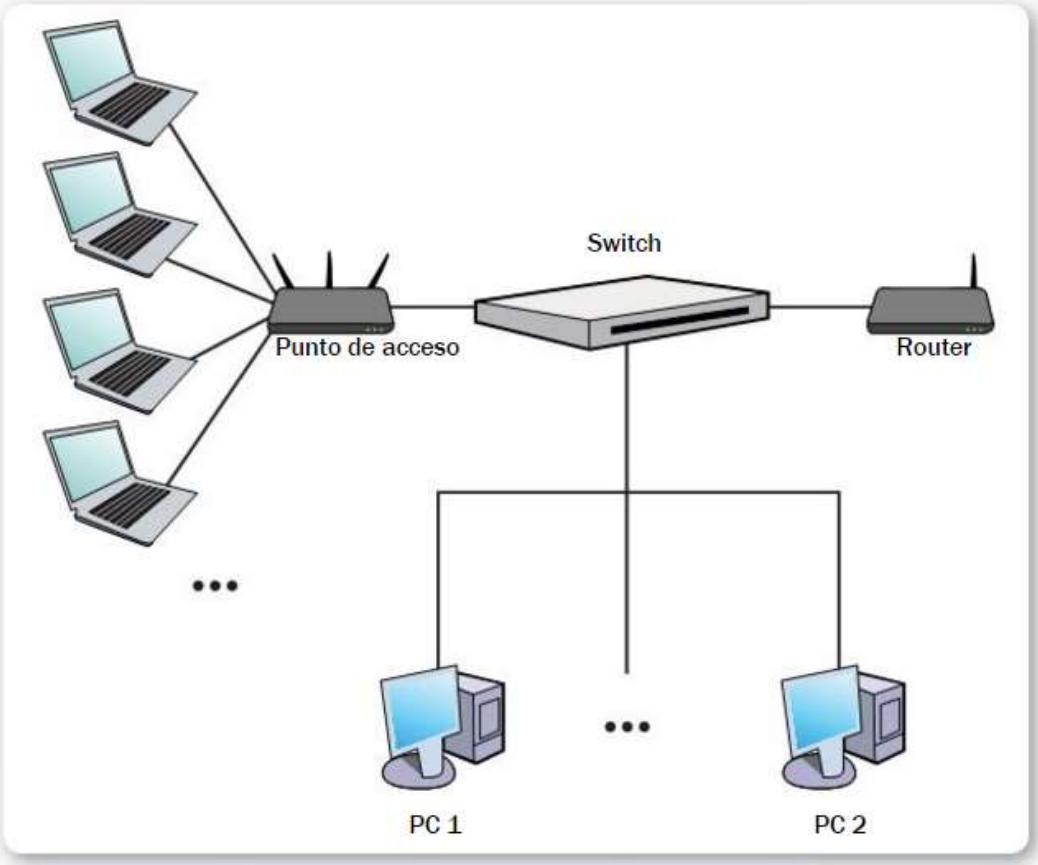


Figura 22. Esquema de red cableada e inalámbrica funcionando mediante routers y switches.

Configuración de routers WiFi

Con nuestro router inalámbrico podremos liberarnos de los muchos cables que rodean las inmediaciones de muebles, plantas, dormitorios y pasillos. Sin embargo, puede que saquemos todos los cables y cada computadora tenga su adaptador pero, al querer ingresar a la red, nos encontremos con un nombre extraño que hace alusión al flamante router. Nos conectamos sin introducir ninguna clave, intentamos navegar y vemos que no es posible hacerlo.

> LA CONFIGURACIÓN DE UN ROUTER WIFI NOS PERMITE LIBERAR LA RED DE MUCHOS CABLES



Figura 23. Router con cuatro puertos de red (amarillo), uno WAN (azul) y dos de línea (verde).

En una ráfaga de preguntas recurrimos a la caja y no entendemos si estamos leyendo las instrucciones en coreano o en español.

Lo mejor, en este punto, será sentarnos frente a la computadora que acabamos de conectar, tomar la guía que presentamos a continuación y

Para comenzar

Antes de empezar, les recordamos que la guía está pensada de la manera más genérica posible, para tratar de abarcar la mayor cantidad de modelos disponibles en el mercado (que de por sí son numerosos), ya que cada fabricante los ha diseñado a su gusto y capacidades. Esto no quiere decir que no haya opciones comunes a todos.

Comencemos con las generalidades. Todo router wireless cuenta con puertos traseros que, mínimamente, son cuatro y están pensados para configurar el dispositivo de manera externa. Para evitarnos problemas de conexión, conectamos el cable de red que acompaña al dispositivo a la computadora y esperamos a que esta lo reconozca. Cuando nos informe que está conectada, abriremos el navegador web.



Figura 24. Al ingresar desde un explorador, se nos solicita nombre de usuario y clave.

Por defecto y de fábrica, los routers están preparados para ser configurados mediante estos exploradores con una interfaz basada en una página web, y todos se comportan de la misma manera. Para ingresar, utilizamos una dirección común a todos los routers: escribimos en la barra de direcciones 192.168.1.1 (o 192.168.0.1).

EL PRIMER ROUTER

El primer dispositivo que ofrecía la misma funcionalidad que lo que hoy conocemos como router era el Interface Message Processor o IMP. Se trataba de dispositivos que formaban la ARPANET, la primera red de conmutación de paquetes que funcionó a gran escala.



Figura 25. La página de inicio tiene detalles básicos y menús del router.

Datos iniciales

Al ingresar a esta dirección, un cartel de bienvenida nos pedirá que introduzcamos un nombre de usuario y una contraseña (cada fabricante los asigna según crea conveniente, y varían con cada modelo); en general, es alguna de estas posibles combinaciones:

- Usuario: admin, admin123, admin1234, guest, (vacío).
- Pass: admin, admin123, 1234, guest, (vacío).

Combinaciones

Hay que intentar con todas las combinaciones posibles de las indicadas antes; si aun así no funciona, es probable que el fabricante haya indicado la combinación correcta en el manual de usuario, en la caja o, incluso, en la etiqueta que se encuentra a un lado del router.

La primera página nos dará un resumen de la configuración inicial, el estado de la conexión y estadísticas. Normalmente el menú de configuración está redactado en inglés, pero tratemos de guiarnos con un diccionario en mano por si algún término se hace difícil de entender. A la derecha veremos una columna con información referida al ítem que seleccionamos, y que puede guiarnos en la configuración.

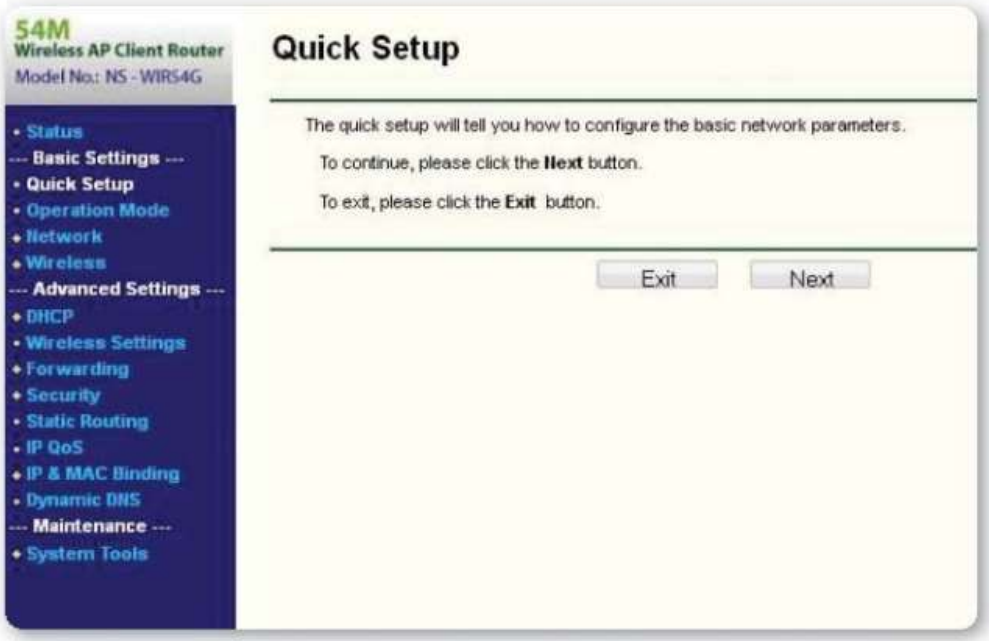


Figura 26. Esta sección que nos guiará paso a paso en la configuración básica.

En el menú de la izquierda o en la parte superior (dependiendo del modelo de router que tengamos) podremos diferenciar algunas secciones; entre ellas, la más relevante es Status . Status/Estado . Observamos información importante sobre el estado de la conexión, configuración WAN, LAN, wireless, tráfico (información enviada y recibida), etcétera. Recordemos que estos son los datos más importantes a la hora de configurar un router WiFi.

Divisiones generales

Encontraremos una serie de divisiones importantes en el menú de configuración del dispositivo. Las conoceremos a continuación:

Configuración rápida/Quick Setup : sirve para ajustar los detalles esenciales del router. Entre los comandos más comunes hay

ENCAMINADOR INALÁMBRICO

A pesar de que tradicionalmente los encaminadores solían tratar con redes fijas (Ethernet, ADSL, RDSI), en los últimos tiempos han comenzado a aparecer encaminadores que permiten realizar una interfaz entre redes fijas y móviles (Wi-Fi, GPRS, Edge, UMTS, Fritz!Box, WiMAX).

algunos parámetros que detallaremos más adelante. Configurando adecuadamente esta sección, lo más seguro es que podamos acceder a internet en las computadoras de la red; sin embargo, es mejor familiarizarnos con la configuración manual.

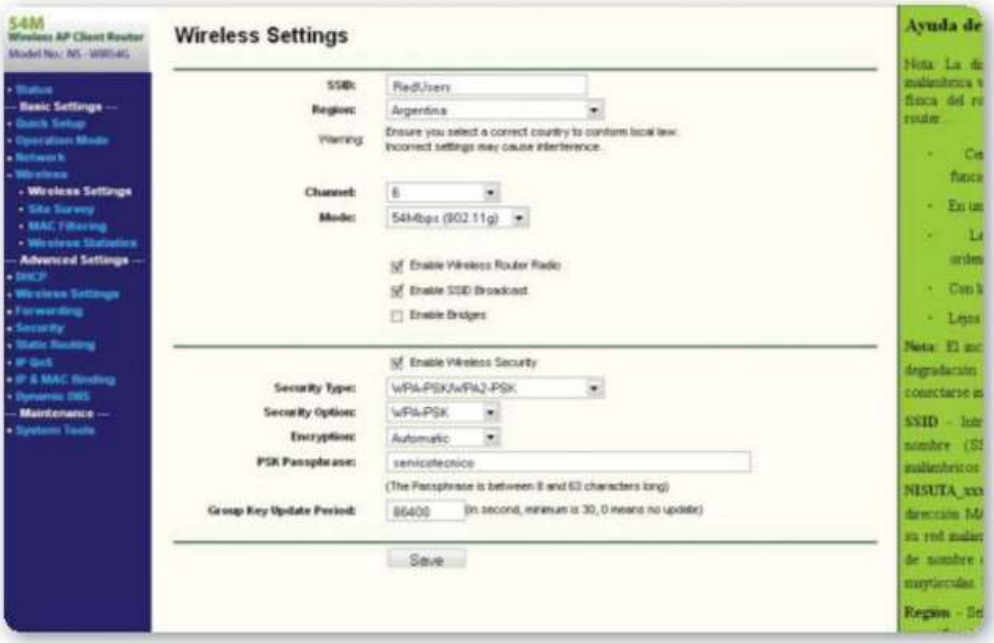


Figura 27. Configuración óptima de seguridad inalámbrica.

LAN

Este valor es el que utilizamos para ingresar a la configuración del router (que generalmente es 192.168.0.1); si modificamos este número, para volver a ingresar debemos hacerlo por esa dirección. En algunos menús se permite configurar la máscara de subred, que cubre la red bajo el rango permitido. También se indica la dirección MAC, que es la dirección física y única del router. En la mayoría de los dispositivos encontramos una opción que se designa como Clonar MAC/ Clone MAC, que sirve en caso de que el proveedor tenga asignada la MAC del router. Para que los demás dispositivos tengan acceso, debe estar declarada aquí.

WAN

Red de Área Extensa, es la interfaz por la cual ingresa la conexión a internet; nos permitirá conectar el router a internet y distribuir su acceso a los demás dispositivos. Antes de configurar esta sección, revisamos la parte trasera del router y confirmamos que el cable por el cual ingresa internet (desde el módem) esté conectado al puerto

indicado como WAN. Confirmada la conexión, procedemos a configurar las opciones que mencionamos y describimos a continuación:

- IP dinámica / Dynamic IP : utilizada en conexiones a internet por cablemódem. La IP es proporcionada por el proveedor de internet que hemos contratado; el router automáticamente configura las direcciones y redirecciona la información hacia las computadoras conectadas a él. Podremos configurar parámetros como el Nombre de Host / Host Name (determinados proveedores requieren que las conexiones entrantes estén identificadas con este nombre para poder acceder), Tamaño de MTU / MTU Size (tamaño máximo de los paquetes enviados y recibidos; si el proveedor de internet no requiere algún tamaño específico, no se debe modificar) y Servidores DNS/ DNS Servers (esta dirección se debe especificar solo si el proveedor la proporciona).
- IP Estática / Static IP : dentro de esta gama de configuraciones deberemos conocer la dirección IP del proveedor, la máscara de subred, la puerta de enlace para ingresar en la red y los servidores de DNS. Si alguno de esos valores es mal ingresado, no contaremos con acceso ni a la red ni a internet.
- PPPoE : los proveedores de internet (por ejemplo, telefónicas locales) requieren nombre de usuario y contraseñas predeterminadas para cada línea, por lo que debemos contratar el servicio y será la empresa la que proporcione esos datos. Hay que configurar el tiempo durante el cual el router permanecerá conectado a internet: Conexión a pedido / Connect On Demand , cada vez que necesitamos internet se conecta automáticamente y, después de cierto tiempo, se desconecta; se utiliza esta configuración para Internet limitada al consumo. Conectar Automáticamente / Connect Automatically : se conecta cada vez que encendemos el router.



FUNCIONAMIENTO DEL ROUTER

El funcionamiento de un router, como se deduce de su nombre, consiste en enviar los paquetes de red por el camino o ruta más adecuada en cada momento. Para realizarlo almacena los paquetes recibidos y procesa la información de origen y destino que poseen.

Conectar manualmente / Connect Manually : se conecta accediendo a esta sección de la configuración o desde el Menú de Estado). Consideremos que debemos elegir esta opción si contamos con una conexión a internet mediante módem ADSL.

- Existen otros modos de configuración pero son menos usados e, incluso, algunos dependen de normativas nacionales, como L2TP (tecnología de redes compatible con las redes privadas virtuales, permite a los usuarios remotos tener acceso seguro a redes empresariales a través de internet) y PPTP (similar a L2TP pero con tecnologías de cifrado diferentes).

> EL MODO DE CONFIGURACIÓN L2TP DEPENDE DE NORMATIVAS NACIONALES

Wireless

En este apartado es posible permitir que todos los dispositivos inalámbricos puedan conectarse en forma adecuada, tanto a la red que estamos configurando como, también, a internet.

El mayor problema que tendremos en esta sección es el orden que dan los fabricantes a las opciones, así que daremos una guía que no debe seguir un orden predeterminado.

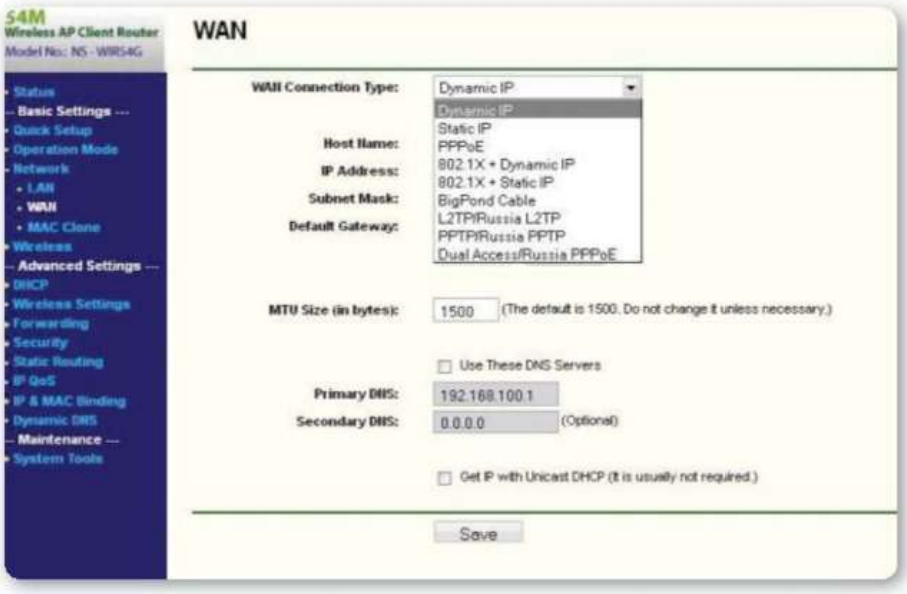


Figura 28. Esta configuración depende del proveedor de internet y el medio que utilice.

SSDI

En este apartado podemos asignar el nombre que mostrará la señal de WiFi para identificar nuestra red.

Región

País en el cual se encuentra la red, para apegarse a la normativas de radiofrecuencia y canales habilitados. Recordemos que este parámetro puede provocar interferencia si no lo configuramos bien.

Modo

Dependiendo del tipo de router que tengamos, podemos modificar el modo de trabajo: Access Point, Repetidor, Repetidor universal o puente.

Opciones

Habilitar la Señal del Router / Enable Wireless Router Radio (para impedir o permitir que se conecten computadoras de modo inalámbrico) y Habilitar transmisión del SSID / Enable SSID Broadcast (si la deshabilitamos, la red seguirá funcionando pero estará en modo "invisible" y cada dispositivo deberá conectarse manualmente).

Seguridad

La configuración de seguridad permite establecer permisos para que solo determinados usuarios tengan acceso a la red y, así, se proteja la información. Para habilitar esta opción, debemos configurar el tipo de seguridad que necesitamos.

Tipo de seguridad/Security Type

En esta sección seleccionamos el tipo de seguridad que se nos permite, entre las siguientes alternativas:

UN SIGLO DE REDES

Las redes actuales son el resultado de un desarrollo de tecnologías que lleva más de cien años. Para darnos una idea, podemos mencionar que el primer indicio de redes de comunicación fue de tecnología telefónica y también telegráfica. Durante el año 1940 se transmitieron datos desde la Universidad de Darmouth , en Nuevo Hampshire , a la ciudad de Nueva York .

- WEP : primer sistema de cifrado que prevaleció en redes wireless, hoy débil y obsoleto. Podemos configurar Opciones de Seguridad (Sistema Abierto / Open System , encriptación de una clave en formato hexadecimal o ASCII de 64 o 128 bits que depende de lo que soporte el dispositivo); Clave Compartida / Shared Key (requiere que el cliente y el punto de acceso tengan la misma clave WEP para realizar la autenticación); Formato de la Clave (puede ser Hexadecimal o ASCII); y desde una hasta cuatro claves diferentes con una encriptación que puede ser más o menos compleja.
- WPA/WPA2 : sistema de cifrado más seguro, basado en seguridad WPA o WPA2 con contraseña precompartida. Se pueden asignar encriptaciones o hashing de clave que mejoran la encriptación de los paquetes de datos. Encontramos TKIP y AES (la segunda es la codificación autorizada estándar más fuerte). Asignamos la dirección IP del servidor que encripta, el puerto y su contraseña.
- WPA-PSK/WPA2-PSK : similar a la anterior, solo que en vez de asignar un servidor usamos una frase o clave de entre 8 y 63 caracteres de longitud. El modo de encriptación es el mismo, pero relativamente más fácil de configurar.

> WPA Y WPA2 SON SISTEMAS DE CIFRADO SEGUROS, BASADOS EN CONTRASEÑA COMPARTIDA

Opciones adicionales

Con estas opciones podremos tener una red funcional conectada a internet; lo que nos queda es controlar quién ingresa, y permitir o no el acceso a la red mediante el Filtro MAC .

Dentro de la configuración encontraremos una opción llamada Site Survey o Wireless Statistics (máquinas conectadas), donde podremos obtener información sobre los dispositivos en red, su dirección MAC y, si lo deseamos, agregarlos al filtro para impedir su acceso total a la red. También podremos asignarles direcciones IP específicas (o nombre de las computadoras en la red) mediante el DHCP.

En sus configuraciones podremos asignar intervalos de direcciones que se darán a las computadoras conectadas; si se supera el límite, no podrán conectarse nuevos equipos.



Figura 29. Cuando terminamos de configurar, corroboramos que la red con seguridad está habilitada.

Juegos y aplicaciones

Algunos juegos o programas de intercambio de información P2P requieren determinados puertos que no estén configurados de fábrica. Lo que necesitamos para asignarlos es ir a NAT, Forwarding o Servidores Virtuales / Virtual Servers.

Lo que nos interesa es asignar una determinada dirección IP, un puerto específico (con valores comprendidos entre 1 y 65535), el protocolo (de subida: UDP; de bajada: TCP) y el uso (si es para HTTP, FTP, POP3, etcétera). Esta configuración se realiza para cada IP, ya que es una redirección individual y la ubicación de los datos depende del modelo.

IMPORTANTE

Siempre tengamos presente que una o más modificaciones implicará que el router tenga que ser reiniciado. Esto significa que no se podrá configurar de manera continua, sino que demorarán en cargarse los controladores de la red. En ocasiones, si realizamos cambios inadecuados y no tenemos manera de ingresar al panel web por ningún medio, es posible volver a los valores de fábrica a través del botón [Reset], ubicado en la parte trasera del router.

El resto de las opciones son más personalizadas para cada equipo y están referenciadas a sus características específicas. Lo importante es tener en claro todos los parámetros necesarios para lograr el funcionamiento óptimo de la red wireless.



Figura 30. En este sistema encontramos más opciones a la hora de conectarnos a una red inalámbrica, por ejemplo, desde el área de notificación.

Optimizar la señal WiFi

En esta sección revisaremos en detalle diversos consejos para que podamos optimizar la señal WiFi entregada por nuestros dispositivos inalámbricos. Sigamos las indicaciones del siguiente Paso a paso .

SISTEMAS WINDOWS

Como sabemos, los sistemas Microsoft Windows nos entregan herramientas sencillas para que podamos conectarnos de un modo fácil y rápido a las redes inalámbricas que se encuentran al alcance de nuestra computadora. Si nos encontramos en Windows 7, podemos desplegar las opciones de conexión haciendo clic en el icono adecuado del área de notificación, y también es posible acceder al Centro de redes y recrusos compartidos dentro del Panel de control

PAP: OPTIMIZAR LA SEÑAL WIFI

01 Si usa una pantalla de material metálico junto a la antena, su cara convexa debe apuntar hacia el entorno donde se encuentran los dispositivos inalámbricos.



02 Puede hacer que cualquier router tome las señales débiles de un router originario y las intensifique. Para esto, configúrelo como Repeater Bridge y desactive la opción [DHCP Server].



03 Las antenas externas que vienen de fábrica en routers WiFi suelen ser extraíbles y tienen una ganancia de hasta 3 dBi (potencia de emisión y recepción de una antena). Si cambia la antena por una de 5 o 9 dBi incrementará el alcance de la señal.



Para terminar, es necesario que consideremos que la señal WiFi se propaga desde la altura en que se encuentra la antena hacia abajo. De esta manera, para tener una mejor prestación, es conveniente que procedamos a ubicar el router a la mayor altura posible. Por ejemplo, en un edifico de varios pisos, se aconseja situarlo en el más alto, y los repetidores, en los pisos inferiores. Por otra parte, también es una buena idea considerar el uso de extensiones para las antenas: así obtendremos más alcance y, por lo tanto, una mayor cobertura.

TCP/IP Y EL MODELO OSI

Desde los años 80 del siglo pasado el desarrollo de tecnologías fue vasto y variado, y cada fabricante estableció pautas propias de conexión para sus dispositivos. Con el fin de enlazar las diferentes redes fue necesario implementar un estándar de comunicación, el modelo OSI, que instaura un modelo de interconexión de sistemas abiertos. Este estándar establece siete niveles de comunicación: nivel físico, de enlace de datos, de red, de transporte, de sesión, de presentación y de aplicación.

Seguridad en redes inalámbricas

Si bien la libertad de conectar nuestras computadoras a una red inalámbrica nos proporciona facilidad y comodidad, la seguridad es un tema que debemos tener en cuenta. Lo primero que vamos a hacer es establecer un nombre de usuario y una contraseña para que solo nosotros podamos realizar modificaciones en el router, así como cambiar los datos de configuración previos.

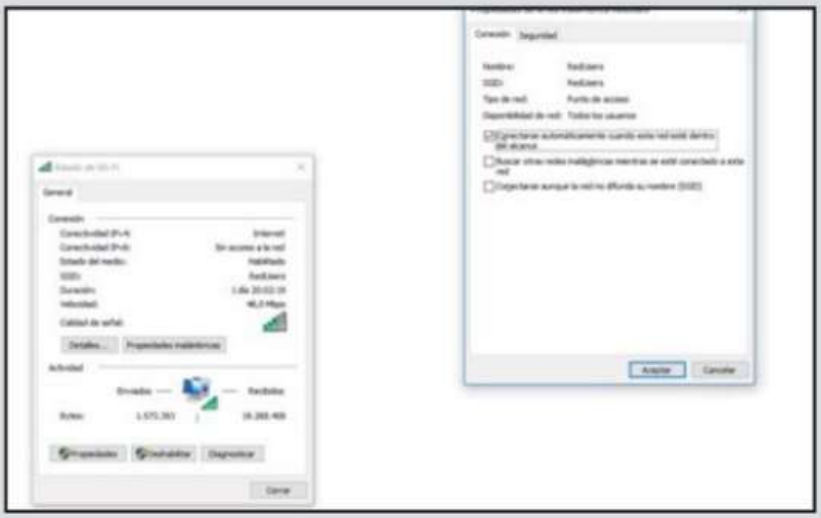
Para realizar estas tareas vamos a Herramientas de Sistema/Contraseña (esto puede variar en diferentes marcas y modelos) y establecemos los parámetros que deseamos aplicar.

PAP: MAXIMIZAR LA SEGURIDAD EN REDES INALÁMBRICAS

01 Debe establecer el mayor parámetro de seguridad que pueda brindar su router –que por lo general es WPA2-PSK–, encriptación automática y una contraseña de entre 8 y 63 caracteres. Trate de establecer una clave con letras, números y símbolos, para incrementar la seguridad al máximo.



02 Para que otras computadoras dentro del rango de alcance no vean la señal del router, proceda a Deshabilitar la transmisión del nombre o SSID, desmarcando Enable SSID Broadcast .



03 Es importante que realice estas configuraciones conectándose al router mediante un cable de red. Para esta tarea debe utilizar alguno de los puertos de red de la parte trasera del dispositivo inalámbrico.



04 Configurando el firewall podrá controlar la información que entra y sale. El origen puede controlarse mediante el filtrado de IP y de MAC. Las reglas de filtrado son: Permitir acceso y Denegar acceso .



05 En Filtro de IP debe asignar las reglas para controlar el acceso de información mediante rangos de direcciones IP (también rangos para direcciones del puerto WAN), que irán entre los valores que especifique.



06 Cada dispositivo con acceso a la red cuenta con un número de MAC específico de fábrica que lo identifica. Mediante el filtro de MAC, podrá permitir o denegar el acceso por esta dirección, pero no podrá establecer rangos porque esta configuración es puntual y precisa para un número determinado de dispositivos.



Recordemos realizar la configuración anotando todos los cambios que vamos efectuando; también es importante que estemos conectados al router mediante cable y, sobre todo, que registremos las contraseñas asignadas en lugar seguro. Si estamos conectados al router de manera inalámbrica mientras realizamos la configuración, lo más probable es que, si no lo hemos configurado en forma adecuada, tengamos problemas de conexión cuando volvamos a intentarlo.

INSTALACIONES DOMICILIARIAS

En general, las instalaciones de red que se efectúan en los domicilios que tienen numerosas habitaciones requieren alargues, antenas potenciadas o repetidores de señal, debido a que obstáculos como paredes o muebles impiden la distribución de señales aceptables. En las empresas este problema se reduce a la incorporación de más dispositivos de mejor calidad y variada ubicación, principalmente, por contar con mayor presupuesto que una red hogareña.

Problemas típicos en redes wireless

Seguridad, ancho de banda y potencia de la señal son los problemas típicos que pueden presentar las redes inalámbricas. Aquí conoceremos algunas soluciones de optimización.

La débil recepción que experimentan algunas placas wireless PCI en equipos de escritorio se soluciona, en muchos casos, incorporando una interfaz WiFi USB, la cual, mediante un cable extensor, puede acomodarse en una posición más despejada. Debemos tener en cuenta que, según la potencia del router emisor, pueden encontrarse dispositivos con antena externa o también sin ella.

PAP: SOLUCIONAR PROBLEMAS EN REDES WIRELESS

01 Los controladores compact-wireless para Linux son drivers genéricos que optimizan la compatibilidad de los controladores de la placa WiFi con su distribución Linux, aumentando la recepción. Instálelos con el compilador make (makeinstall y make load) y reinicie el equipo.



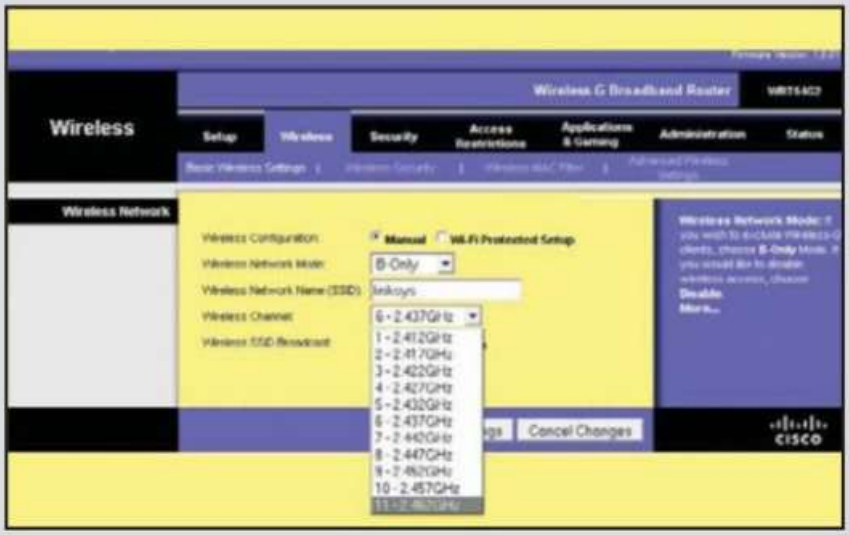
02 En los sistemas operativos de Microsoft puede aumentar el nivel de recepción mediante PowerSaveMode en las propiedades de la placa, en la opción Configuración/Opciones Avanzadas/Maximum .



03 La seguridad es un elemento ineludible en una red WiFi. Para evitar intromisiones, es conveniente encriptar el tráfico de red mediante una clave WAP y bloquear el acceso a la configuración del router cambiando la clave de fábrica.



04 Cambiar el canal de frecuencia en que emite el router es una excelente opción para evitar interferencias. Debe definir el estándar entre 802.11a, 802.11b u 802.11g y especificar por cuál de los canales va a emitir el dispositivo.



05 Muebles metálicos, puertas y ventanas metálicas, horno a microondas y todo aparato emisor o receptor de señales de radio u ondas electromagnéticas afectan la señal. Debe acomodar el router a la mayor distancia posible.



06 Periódicamente, y más aún si su router tiene algunos años, debe hacer actualizaciones del firmware, para reparar errores y potenciar el dispositivo. Por lo general, el software actualizado está disponible en la web del fabricante, desde donde se lo descarga sin costo.



Si bien todos los routers tienen alternativas de configuración parecidas, no debemos dejar de consultar el manual de usuario correspondiente en el momento de establecer cuáles son nuestros requerimientos (hogar o empresa, conexión DNS o cablemódem) y qué parámetros alteraremos en función de eso.

RESUMEN

En este capítulo vimos en detalle la configuración de las redes informáticas, tanto cableadas como inalámbricas. Conocimos temas teóricos como las topologías de red, el modelo OSI y las normas Ethernet, y también revisamos el protocolo TCP/IP. Posteriormente describimos los principales componentes de una red cableada y aprendimos a armar un cable de red y a configurar un router hogareño. Para continuar, analizamos las redes inalámbricas y las normas relacionadas, aprendimos a optimizar una señal WiFi y maximizamos la seguridad en este tipo de redes.

Actividades

TEST DE AUTOEVALUACIÓN

1	¿Cuáles son las ventajas de implementar una red informática?
2	Mencione las topologías de red existentes.
3	¿Qué es el modelo OSI?
4	Describa las normas Ethernet.
5	¿Qué es el protocolo TCP/IP?
6	¿Cuáles con los tipos de cables que encontramos para implementar una red?
7	Describa las normas 802.11.
8	¿Cómo podemos optimizar una señal WiFi?
9	¿De qué modo es posible asegurar una red inalámbrica?
10	¿Qué problemas típicos encontramos en una red inalámbrica?

EJERCICIOS PRÁCTICOS

1	Arme un cable UTP.
2	Realice la configuración de un router hogareño.
3	Optimice la señal WiFi de su red.
4	Maximice la seguridad de su red inalámbrica.
5	Solucione algunos problemas típicos que puedan presentarse en su red inalámbrica.