

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

REDES WiFi

21

EN ESTE FASCÍCULO ANALIZAREMOS LAS REDES INALÁMBRICAS, LOS DISPOSITIVOS ADECUADOS Y LAS TAREAS DE CONFIGURACIÓN RELACIONADAS.



En esta clase veremos...

EL FUNCIONAMIENTO DE LAS REDES CABLEADAS Y LA FORMA EN QUE DEBEMOS CONFIGURAR LOS DISPOSITIVOS CONECTADOS. TAMBIÉN DAREMOS CONSEJOS PARA MEJORAR LA SEGURIDAD.



En la clase anterior conocimos los conceptos relacionados con las redes cableadas, vimos el alcance del modelo OSI, las normas Ethernet y el protocolo TCP/IP. Por otra parte, analizamos los distintos tipos de redes existentes y describimos los dispositivos que encontramos en una red cableada. También aprendimos a armar un cable UTP, configuramos un router hogareño y solucionamos los problemas de conectividad más comunes. En el presente fascículo revisaremos las redes inalámbricas, conoceremos las normas correspondientes y sus ventajas sobre las cableadas. Analizaremos los dispositivos inalámbricos más frecuentes y, también, los accesorios que es necesario tener en cuenta para este tipo de sistema. Aprenderemos a optimizar una red WiFi y a maximizar su seguridad. Finalmente, solucionaremos los problemas más habituales y aprenderemos a instalar una VNC.



06

CONFIGURACIÓN DE ROUTERS WiFi

11

ACCESORIOS INALÁMBRICOS

15

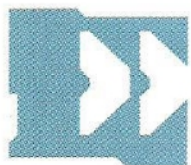
OPTIMIZAR LA SEÑAL WiFi

20

SOPORTE A DISTANCIA: VNC

Redes inalámbricas y normas 802.11

LAS REDES ENTRE DISPOSITIVOS APUNTAN A LA TECNOLOGÍA INALÁMBRICA, AL REEMPLAZO DEL CABLEADO Y A NUEVAS METODOLOGÍAS PARA EL INTERCAMBIO DE LA INFORMACIÓN.



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.

EVOLUCIÓN

La evolución de las redes fue precisa 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. Estas contaban con un dispositivo (en promedio de 4 a

8 puertos) que se conectaba mediante un cable de red hasta el terminal (computadora, generalmente), y problema solucionado. Al extenderse este grupo, donde 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 que, a su vez, cada una de ellas ya no pertenece a un lugar fijo por un período prolongado de tiempo, 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. Prevalcieron 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).

ESTÁNDAR

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

Red cableada

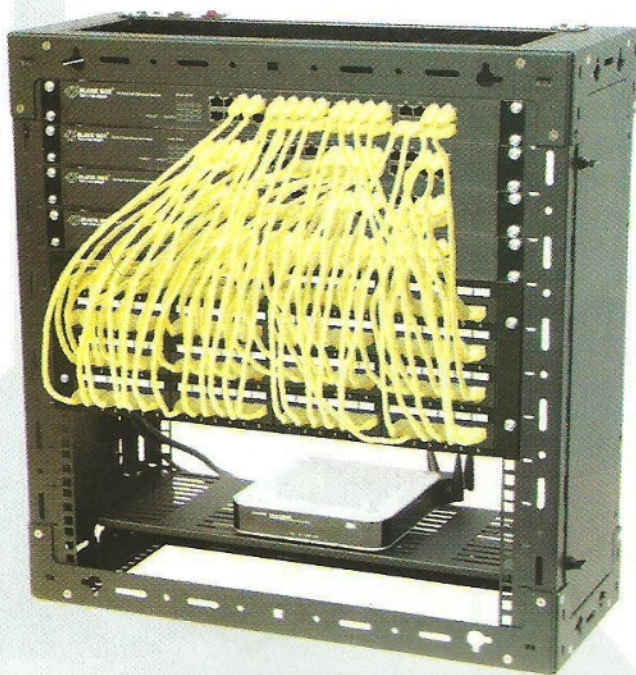
- ❑ Requiere grandes cantidades de cable para interconectar un gran número de computadoras.
- ❑ Permite longitudes máximas de cableado de hasta 100 metros.
- ❑ Requiere interfaces de red que viene instaladas en todas las placas madre de las computadoras.

- ❑ 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.

**PARA MEJORAR
LA VELOCIDAD
DE TRANSFERENCIA,
RECURRIMOS AL CABLEADO;
PARA AUMENTAR LA
MOVILIDAD, RECURRIMOS
A LO INALÁMBRICO.**

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 transmitir la señal, la distancia implicada y la cantidad de objetos interpuestos entre este y el o los dispositivos que se deseen conectar.
- ❑ Algunos dispositivos vienen incorporados con interfaces inalámbricas, pero de no contar con una, es necesario adquirir un adaptador WiFi.
- ❑ Cada router tiene una capacidad muy alta de conexiones simultáneas (sin embargo, 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.



Racks. Estos elementos se usan habitualmente para establecer redes cableadas con servidores en determinados sectores.



Router WiFi.

Router potenciado para realizar conexiones inalámbricas estables.

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 de este tipo de conexión 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, la tecnología cableada y la inalámbrica seguirán coexistiendo, pero sufrirán importantes mejoras.

TECNOLOGÍAS

Cada tipo de red inalámbrica se maneja con estándares de funcionamiento denominados 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, ha sufrido modificaciones que se identifican con las letras desde la "a" hasta la "w", como por ejemplo:

a: la primera revisión de la norma 802.11 que establece protocolos; funciona en la banda de 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.

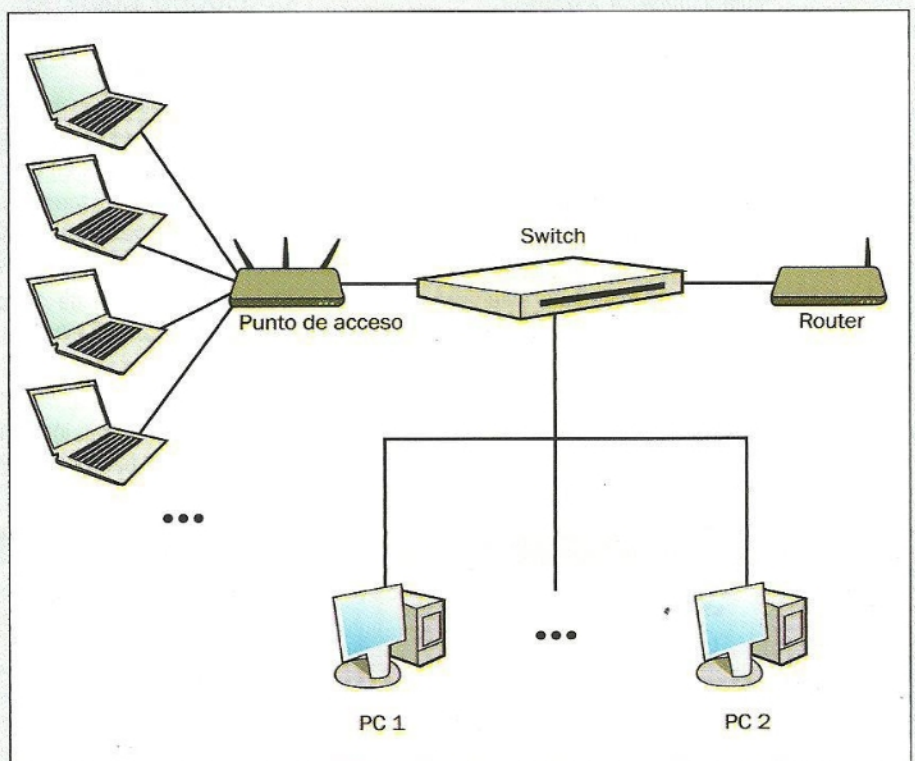
g: como cambio del estándar 802.11b, mejora la velocidad teórica a 54 Mb/s y es compatible con la norma "b", a diferencia de la "a", que no lo es con

ninguna. Una singularidad importante 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 frecuencias, la de 2,4 GHz y la de 5 GHz, haciéndola compatible con todas las versiones anteriores.

Ambas redes coexisten y coexistirán debido a que presentan utilidad, son necesarias y la tecnología lo permite.



Red mixta. Una red cableada e inalámbrica, como todas las de su tipo, funciona mediante routers y switches.

Configuración de routers WiFi

PRIMER PASO LOGRADO: COMPRAMOS NUESTRO ROUTER WIFI, LO INSTALAMOS, PERO AHORA NO TENEMOS ACCESO A LA RED. ¿CÓMO LO CONFIGURAMOS? ¿POR QUÉ ES IMPORTANTE HACERLO CORRECTAMENTE?



Estamos emocionados, por fin tenemos nuestro router inalámbrico y podremos liberarnos de tantos cables que rodean las inmediaciones de muebles, plantas, dormitorios y pasillos. Sacamos todos los cables, cada computadora tiene su adaptador, pero queremos ingresar a la red y nos encontramos con un nombre extraño que hace alusión al flamante router. Nos conectamos sin introducir ninguna clave, intentamos navegar y no es posible hacerlo.

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 es sentarnos frente a la computadora que acabamos de conectar, tomar esta guía y empezar a trabajar.

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.

Empecemos con las generalidades. Todo router wireless cuenta con puertos traseros que, mínimamente, son

cuatro y están pensados para configurar el dispositivo de manera externa. De modo de 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 correctamente, abrimos el navegador web.

UNA CONFIGURACIÓN INADECUADA PODRÍA IMPEDIR EL ACCESO A INTERNET Y A LA RED. POR ESTA RAZÓN, DEBEMOS REALIZAR TODOS LOS PASOS CON MUCHO CUIDADO.

Por defecto y de fábrica, todos 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**).

DATOS INICIALES

Al ingresar a esta dirección, un cartel de bienvenida nos pedirá que introduz-

camos 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).

PROBAR TODAS LAS 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 del router, el estado de la conexión y estadísticas básicas. Normalmente, y por desgracia para algunos, 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 suele haber una columna con información referida al ítem que estamos por utilizar, y que puede guiarnos en el proceso de configuración.



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



Router WiFi. Este router, como muchos modelos que encontramos habitualmente, posee cuatro puertos de red (amarillo), uno WAN (azul) y dos de línea (verde).

En el menú de la izquierda o en la parte superior (dependiendo del modelo), podremos diferenciar algunas secciones que serán las más comunes:

❏ **Status/Estado.** Observamos información importante sobre el estado de la conexión, configuración WAN, LAN, wireless, tráfico (información enviada y recibida), etcétera. Estos son datos importantes a la hora de configurar un router WiFi.

DIVISIONES GENERALES

Dividiremos las siguientes partes de la configuración en:

❏ **Configuraciones básicas / Basic Settings.** Configuración rápida / Quick Setup: sirve para ajustar los detalles esenciales del router. Entre los comandos más comunes, hay parámetros que detallaremos más adelante. Configurando adecuadamente esta sección, lo más

seguro es que podamos acceder a Internet en las PCs; aunque es mejor familiarizarnos con la configuración manual.

❏ LAN

Este valor es el que utilizamos para ingresar a la configuración del router (que generalmente es 192.168.0.1);

Página de estado. La página de inicio tiene detalles básicos y menús del router.



TP-LINK®
300M Wireless N Gigabit Router
Model No. TL-WR1043N / TL-WR1043ND

Status
Quick Setup
QoS
Network
Wireless
DHCP
Network Sharing
Forwarding
Security
Parental Control
Access Control
Static Routing
Bandwidth Control
IP & MAC Binding
Dynamic DNS
System Tools

Status

Firmware Version: 3.9.13 Build 090930 Rel.51043n
Hardware Version: WR1043N v1 00000000

LAN

MAC Address: 00-27-19-CD-74-62
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

Wireless

Wireless Radio: Enable
Name (SSID): TP-LINK_CD7462
Channel: Auto (Current channel 6)
Mode: 11bgn mixed
Channel Width: Automatic
Max Tx Rate: 300Mbps
MAC Address: 00-27-19-CD-74-62

WAN

MAC Address: 00-27-19-CD-74-63
IP Address: 0.0.0.0 **Dynamic IP**
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0 **Renew**
DNS Server: 0.0.0.0, 0.0.0.0

Status Help

The **Status** page displays the Router's current status and configuration. All information is read-only.

LAN - The following parameters apply to the LAN port of the Router. You can configure them in the **Network** → **LAN** page.

- **MAC Address** - The physical address of the Router, as seen from the LAN.
- **IP Address** - The LAN IP address of the Router.
- **Subnet Mask** - The subnet mask associated with LAN IP address.

Wireless - These are the current settings or information for Wireless. You can configure them in the **Wireless** → **Wireless Settings** page.

- **Wireless Radio** - Indicates whether the wireless radio feature of the Router is enabled or disabled.
- **Name (SSID)** - The SSID of the Router.
- **Channel** - The current wireless channel in use.
- **Mode** - The current wireless mode which the Router works on.
- **Channel Width** - The bandwidth of the wireless channel.
- **Max Tx Rate** - The maximum tx rate.
- **MAC Address** - The physical address of the Router, as seen from the WLAN.

WAN - The following parameters apply to the WAN ports of the Router. You can configure them in the **Network** → **WAN** page.

- **MAC Address** - The physical address of the WAN port, as seen from the Internet.
- **IP Address** - The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no connection to Internet.
- **Subnet Mask** - The subnet mask associated with the WAN IP Address.
- **Default Gateway** - The Gateway currently used by the Router is shown here. When you use **Dynamic IP** as



- Status
- Quick Setup
- QSS
- Network
- Wireless
- DHCP
- Network Sharing
- Forwarding
- Security
- Parental Control
- Access Control
- Static Routing
- Bandwidth Control
- IP & MAC Binding
- Dynamic DNS
- System Tools

Quick Setup

The quick setup will tell you how to configure the basic network parameters.

To continue, please click the **Next** button.

To exit, please click the **Exit** button.



Guía rápida.

Sección que nos guiará paso a paso en la configuración básica.

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 de la siguiente manera.

Tipo de conexión WAN / WAN ConnectionType. Entre las más comunes están las que describimos a continuación:

IP dinámica / Dynamic IP: es la 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.

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, y para que los demás dispositivos tengan acceso, esta debe estar declarada aquí.

WAN

Red de Área Extensa, es la interfaz por la cual ingresa la conexión a Internet; nos

- Status
- Quick Setup
- QSS
- Network
- Wireless
- Wireless Settings
- Wireless Security
- Wireless MAC Filtering
- Wireless Advanced
- Wireless Statistics
- DHCP
- Network Sharing
- Forwarding
- Security
- Parental Control
- Access Control
- Static Routing
- Bandwidth Control
- IP & MAC Binding
- Dynamic DNS
- System Tools

Wireless Security

- ☐ Disable Security
- ☐ WEP

Type:
 WEP Key Format:

Key Selected	WEP Key	Key Type
Key 1: ☐		Disabled
Key 2: ☐		Disabled
Key 3: ☐		Disabled
Key 4: ☐		Disabled
- ☐ WPA/WPA2

Version:
 Encryption:

 Radius Server IP:
 Radius Port: (1-65535, 0 stands for default port 1812)
 Radius Password:
 Group Key Update Period: (in second, minimum is 30, 0 means no update)
- ☐ WPA-PSK/WPA2-PSK

Version:
 Encryption:

 PSK Password:



Configuración Wireless. En esta sección vemos una configuración óptima de seguridad inalámbrica.

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: dirección IP del proveedor, máscara de subred, puerta de enlace para ingresar en la red y 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 (como telefónicas locales) requieren

nombre de usuario y contraseñas pre-determinadas 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 necesitemos 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; Conectar manualmente / Connect Manually: se conecta accediendo a esta sección de la configuración o desde el menú de Estado). Debemos elegir esta opción si contamos con una conexión a Internet mediante módem ADSL.

Otros: existen otros modos de configuración, pero son menos usados e,



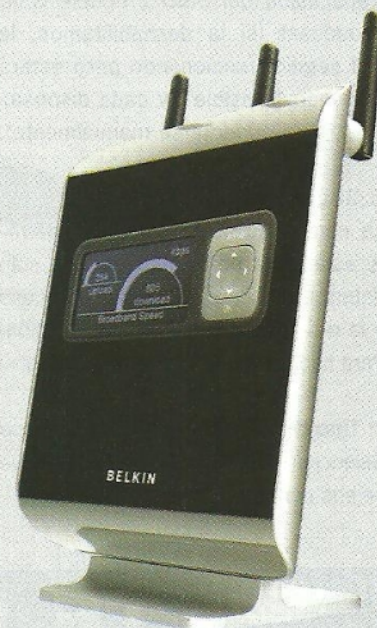
Configuración WAN.

Esta configuración depende del proveedor de Internet y el medio que utilice.

incluso, algunos dependen de las 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).

Wireless

A través de este apartado, permitiremos que todos los dispositivos inalámbricos se conecten adecuadamente a la red y 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. Lo que debemos configurar es:



SSID

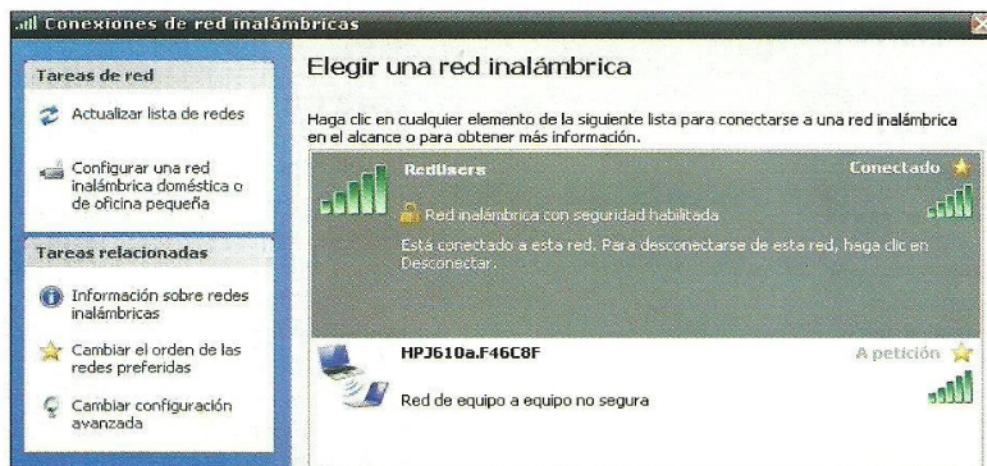
Asignamos el nombre que mostrará la señal de WiFi para identificar nuestra red.

Región

País en el cual se encuentra la red, para apegarse a la normativas de radiofrecuencia y canales habilitados. Puede provocar interferencia si la configuramos mal, por lo que no debemos descuidar este aspecto.

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.



Comprobación.
Una vez que terminamos de configurar todos los parámetros, corroboramos que la red con seguridad esté habilitada.

❏ 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 proteger la información. Para habilitarla, configuramos el tipo.

❏ Tipo de seguridad / Security Type

Seleccionamos el tipo de seguridad que se nos permite, entre los siguientes:

WEP (primer sistema de cifrado que prevaleció en redes wireless, pero 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 (Hexadecimal o ASCII); y desde una hasta cuatro claves diferentes.

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. Es 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 y relativamente más fácil de configurar.

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 les dará a las computadoras conectadas; si se supera el límite, no podrán conectarse nuevos equipos.

¿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). Si tienes alguna duda, comentario o quieres saber más, puedes contactarnos por medio de usershop@redusers.com

Accesorios inalámbricos

EN ESTA GUÍA VISUAL CONOCEREMOS LOS ACCESORIOS MÁS COMUNES PARA REDES INALÁMBRICAS. CADA ELEMENTO PUEDE RESULTAR ADECUADO PARA DETERMINADOS USOS Y EN ENTORNOS ESPECÍFICOS, PERO TODOS SIRVEN PARA MAXIMIZAR LA POTENCIA DE LOS ROUTERS WIFI.

Los routers WiFi vienen preparados de fábrica para brindar determinadas prestaciones, que la mayoría de las veces alcanzan para satisfacer las necesidades

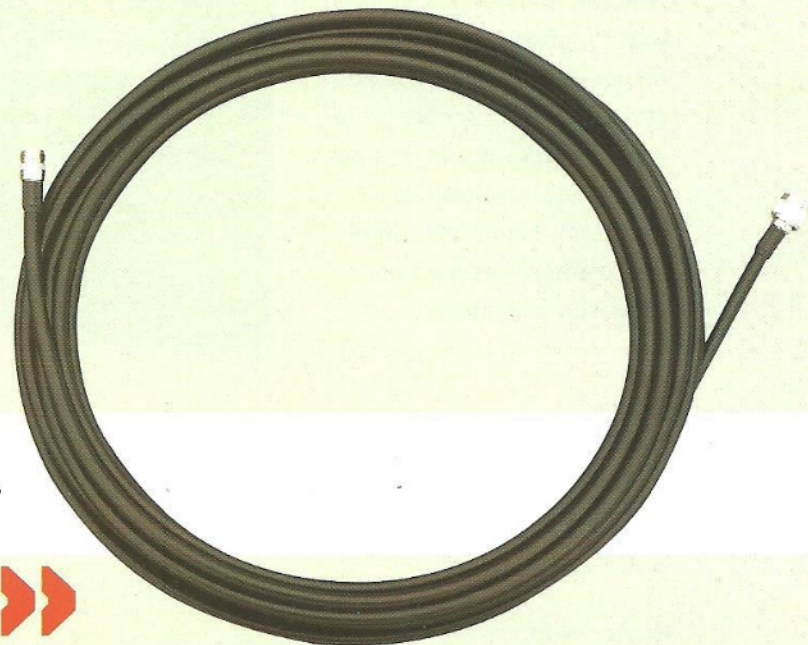
habituales para las que vamos a destinar el uso de este dispositivo. Sin embargo, es importante saber que estas prestaciones pueden ser potenciadas o cambia-

das mediante accesorios que encontramos en el mercado local y que mejorarán su rendimiento. En situaciones específicas, podrán ser una excelente opción.



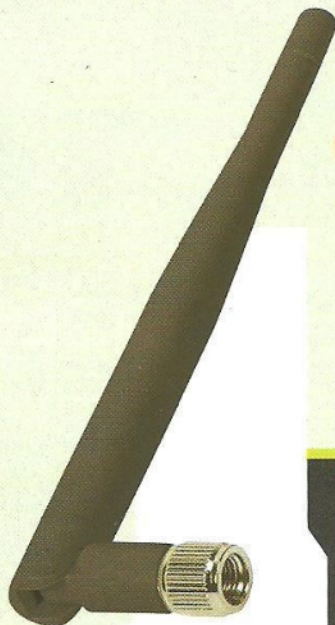
Pigtail

Un pigtail es un trozo de cable que lleva un conector en cada uno de sus extremos. Su utilidad es la de unir un dispositivo inalámbrico a una antena wireless.



Alargue

Una forma de extender el alcance de las redes o del router WiFi es mediante una prolongación de la antena. Este elemento viene fabricado con un conector idéntico a las antenas removibles de los routers para poder hacer su reemplazo.



Antena

La antena es una herramienta fundamental, porque es la que emite la señal. Existen dos familias de antenas, las omnidireccionales y las direccionales. Se trata de un elemento tan importante, que de él depende que la señal llegue hasta donde tenemos previsto, con el mayor nivel y calidad que sean posibles.

INSTALACIONES DOMICILIARIAS

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

Red WiFi hogareña

Una red inalámbrica moderna está formada por múltiples dispositivos conectados entre sí mediante un access point o router WiFi: desde equipos portátiles, móviles y de escritorio, hasta televisores inteligentes, pasando por impresoras wireless.



PC de escritorio

Al ser un equipo que cuenta con puerto Ethernet, generalmente se conecta al router mediante cable. De manera opcional, se le puede conectar una interfaz WiFi USB o PCI.

Módem

Es el dispositivo que recibe conectividad a Internet mediante cablemódem (cable coaxial) o vía ADSL (conexión de datos sobre el par telefónico).

Router WiFi

Es el componente principal de una red inalámbrica, ya que gestiona todas las transacciones en ella. Intermedia entre el módem y el resto de los dispositivos, brindándoles conexión a Internet.

Teléfono IP

La telefonía IP permite efectuar llamadas a costo reducido. Se conecta a Internet mediante el router.

Routers de última generación



Los routers de última generación cuentan con una pantalla táctil desde la cual es posible configurar parámetros básicos. Además, son de diseño estilizado y llamativo.

Smartphone

Los teléfonos inteligentes cuentan con soporte WiFi para evitar el consumo de tráfico 3G mientras estamos en casa, acelerar la velocidad de conexión y ahorrar dinero.

Tablet

Las tablets no poseen la capacidad ni el poder de procesamiento de una notebook, pero son más portátiles y cómodas para el entretenimiento.

LA GRAN MAYORÍA DE LOS APARATOS TECNOLÓGICOS DE HOY EN DÍA PUEDEN CONECTARSE ENTRE SÍ SIN NECESIDAD DE CABLES, GRACIAS A LA MASIFICACIÓN DE LAS CONEXIONES INALÁMBRICAS.

Smart TV

Los televisores inteligentes tienen la capacidad de conectarse a Internet vía cable o WiFi para navegar, jugar online y acceder a contenidos audiovisuales de streaming.

Disco duro WiFi

Las unidades externas de disco con conexión a redes inalámbricas pueden ubicarse en cualquier lugar y permiten almacenar contenido multimedia para reproducirlo en los demás dispositivos.

Notebook

Las computadoras portátiles, por su poder de procesamiento y capacidad, permiten hacer todo tipo de tareas desde cualquier lugar de la casa.

Impresora WiFi

Una impresora de red inalámbrica es capaz de recibir trabajos de impresión de todos los demás dispositivos conectados a la misma red.

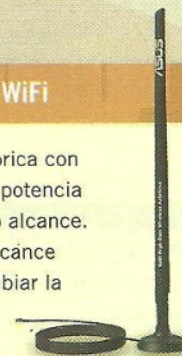
Cámara IP WiFi

Las cámaras inalámbricas de seguridad pueden situarse en cualquier lugar. Se conectan al router mediante WiFi y permiten monitorear desde cualquiera de los demás dispositivos.

Cómo potenciar la señal WiFi

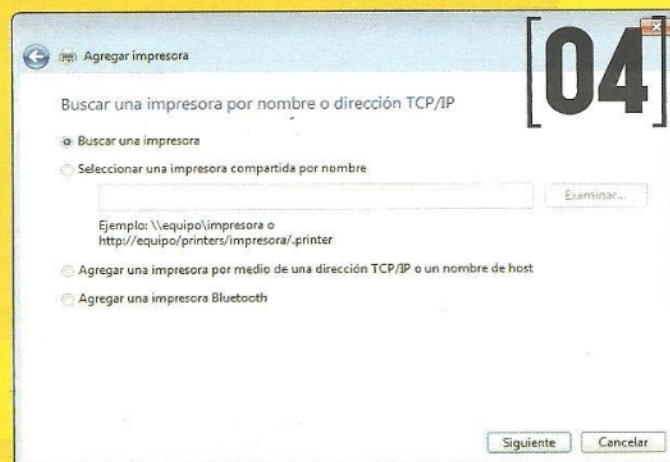
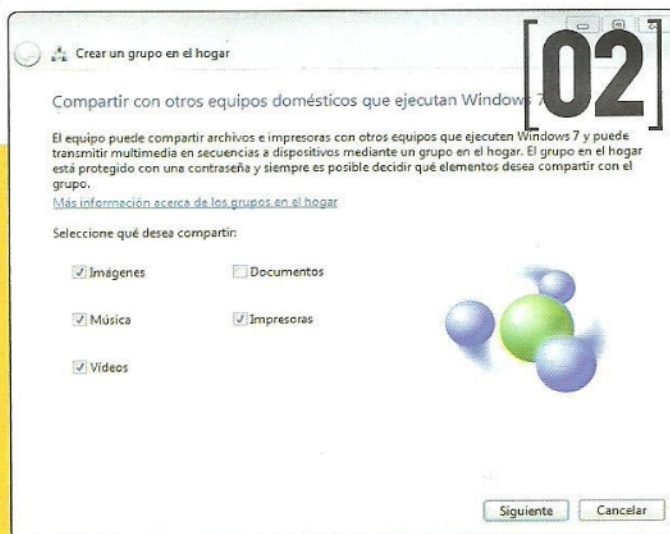
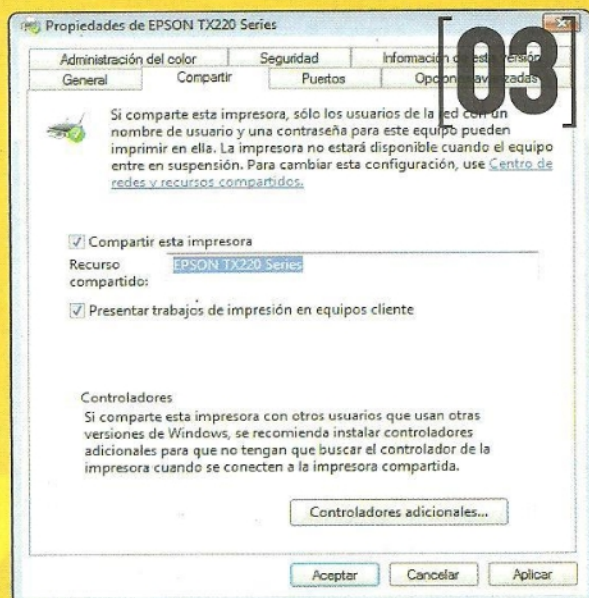
Las antenas provistas de fábrica con los routers son de muy baja potencia y, por lo tanto, de muy corto alcance. Ante una señal débil o de alcance insuficiente, lo ideal es cambiar la antena por una de mayor potencia.

Las antenas están fijadas al router mediante un conector roscado. El tipo de conector más popular es el SMA.



Compartir una impresora en red

EN ESTA SECCIÓN APRENDEREMOS A COMPARTIR UNA IMPRESORA HOGAREÑA EN UNA RED WINDOWS. SOLO DEBEMOS SEGUIR LOS PASOS QUE DESCRIBIMOS.



[01]

La tarea de compartir una impresora en una red Windows es sencilla. En primer lugar, debemos seleccionar la impresora que deseamos compartir y asegurarnos de que los drivers estén correctamente instalados en la computadora. Podemos utilizar los que vienen con el dispositivo.

[02]

Ingresamos en el [Panel de control] en Windows 8, buscamos [Redes e Internet] y accedemos al [Grupo Hogar]. Nos aseguramos de que el Grupo Hogar esté activo en el equipo y copiamos la contraseña adecuada en caso de ser necesario (para agregar los demás equipos al mismo grupo). Verificamos que la casilla para compartir impresoras esté activa.

[03]

Una vez que hayamos configurado el [Grupo Hogar], nos dirigimos a las propiedades de la impresora y la compartimos, aplicamos las opciones necesarias y aceptamos. Podemos especificar controladores adicionales para otros sistemas operativos.

[04]

Vamos al equipo donde deseamos instalar la impresora compartida, nos aseguramos de que se encuentre conectado a la red y lo agregamos al [Grupo Hogar] que corresponde. Iniciamos la instalación de una nueva impresora de red y seguimos las indicaciones del asistente.

Optimizar la señal WiFi

EN ESTA SECCIÓN REVISAREMOS EN DETALLE DIVERSOS CONSEJOS PARA QUE PODAMOS OPTIMIZAR LA SEÑAL WIFI ENTREGADA POR NUESTROS DISPOSITIVOS INALÁMBRICOS.

MEJORAR LA SEÑAL WIFI NO SIEMPRE IMPLICA QUE TENGAMOS QUE GASTAR MUCHO DINERO.



[01]

Si utilizamos una pantalla de material metálico (papel o lata) ubicada junto a la antena, con su cara convexa apuntada hacia el entorno donde se encuentran los dispositivos inalámbricos, las antenas WiFi omnidireccionales concentrarán su señal hacia esa dirección.

[02]

Podemos hacer que cualquier router, como el que vemos en la imagen, tome las señales débiles de un router originario y las intensifique, para ampliar considerablemente el área de cobertura. Para esto, lo configuramos como Repeater Bridge, indicamos el nombre de nuestra señal WiFi y desactivamos 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). Cambiar la antena por una de 5 o 9 dBi incrementará el alcance de la señal.

[04]

La señal WiFi se propaga desde la altura en que se encuentra la antena hacia abajo. Para tener una mejor prestación, conviene ubicar al router a la mayor altura posible. En un edificio de varios pisos, se aconseja situarlo en el más alto. También es una buena idea usar extensiones.

Maximizar la seguridad en redes inalámbricas

SI BIEN LA LIBERTAD DE CONECTAR NUESTRAS COMPUTADORAS A UNA RED INALÁMBRICA PROPORCIONA FACILIDAD Y COMODIDAD, LA SEGURIDAD ES UN TEMA QUE DEBEMOS TENER EN CUENTA, YA QUE SI DESCUIDAMOS ESTE ASPECTO, PODEMOS CORRER SERIOS RIESGOS DE QUE NOS ROBEN NUESTRA INFORMACIÓN.



[01]

Primero, establecemos un nombre de usuario y una contraseña para que solo nosotros podamos realizar modificaciones en el router y cambiar los datos previos. En [Herramientas de Sistema/Contraseña] (esto puede variar en diferentes marcas y modelos) establecemos los parámetros que deseamos.

[02]

Vamos a establecer el mayor parámetro de seguridad que pueda brindarnos nuestro router, que por lo general es WPA2-PSK, encriptación automática, y una contraseña de entre 8 y 63 caracteres. Tratemos de establecer una clave con letras, números y símbolos, para mejorar la seguridad al máximo.

[03]

Para que nadie vea la señal de nuestro router, vamos a [Deshabilitar] la transmisión del nombre o SSID. Se logra desmarcando [Enable SSID Broadcast]. La señal sigue activa en modo oculto, y habrá que ingresarla manualmente en la configuración de redes inalámbricas con su nombre.

[04]

Es importante realizar estas configuraciones conectándonos al router mediante un cable de red. Para esta tarea utilizaremos alguno de los puertos de red que encontramos en la parte trasera del dispositivo inalámbrico. Conectamos el cable y accedemos a la dirección IP del router.

SIEMPRE QUE CONFIGUREMOS UNA RED WIFI DEBEMOS ESTABLECER SU SEGURIDAD.

Basic Security

Firewall

SPI Firewall: ☒ Enable ☐ Disable

VPN

PPTP Passthrough: ☒ Enable ☐ Disable

L2TP Passthrough: ☒ Enable ☐ Disable

IPSec Passthrough: ☒ Enable ☐ Disable

ALG

FTP ALG: ☒ Enable ☐ Disable

TFTP ALG: ☒ Enable ☐ Disable

H323 ALG: ☒ Enable ☐ Disable

[05]

DHCP Settings

DHCP Server: ☐ Disable ☒ Enable

Start IP Address:

End IP Address:

Address Lease Time: minutes (1-2880 minutes, the default value is 120)

Default Gateway: (optional)

Default Domain: (optional)

Primary DNS: (optional)

Secondary DNS: (optional)

[06]

Local Management

Management Rules

☐ All the PCs on the LAN are allowed to access the Router's Web-Based Utility

☒ Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC 1:

MAC 2:

MAC 3:

MAC 4:

Your PC's MAC Address:

[07]

 **La conexión ha sido reiniciada**

La conexión al servidor fue reiniciada mientras la página se cargaba.

- El sitio podría estar no disponible temporalmente o demasiado ocupado. Vuelva a intentarlo en unos momentos.
- Si no puede cargar ninguna página, compruebe la conexión de red de su equipo.
- Si su equipo o red están protegidos por un cortafuegos o proxy, asegúrese de que Firefox tiene permiso para acceder a la web.

[08]

[05]

[06]

[07]

[08]

Configurando el firewall, podremos controlar la información que entra y sale, y desde dónde proviene. El origen puede controlarse mediante el filtrado de IP y de MAC. En cualquier caso, las reglas de filtrado que podemos definir son: [Permitir acceso] a una IP y [Denegar acceso] a una IP.

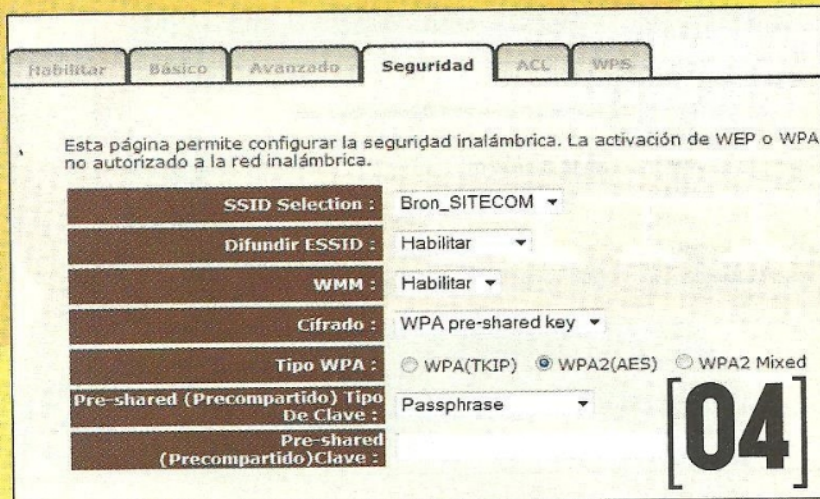
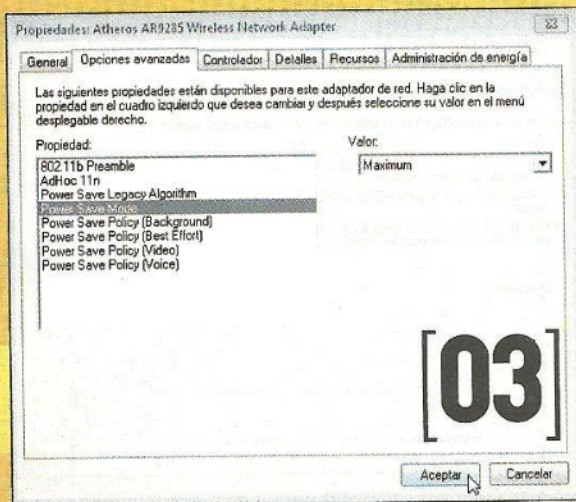
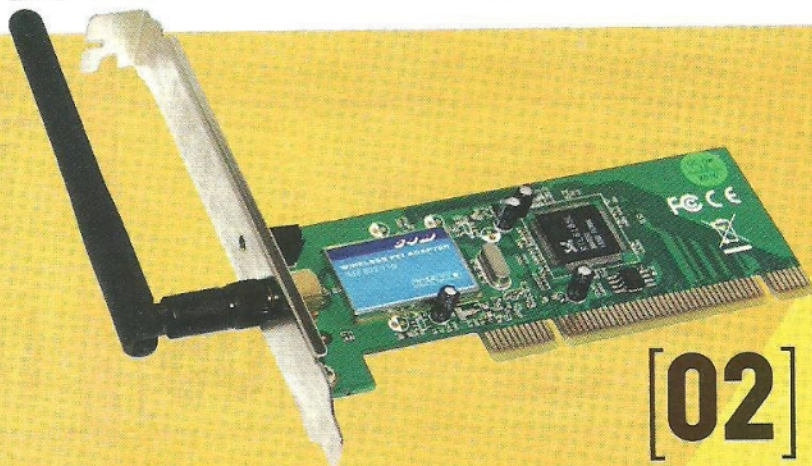
Vamos a [Filtro de IP], donde debemos asignar las reglas para controlar el acceso de información mediante rangos de direcciones IP (también rangos para direcciones del puerto WAN) que irán entre los valores que especifiquemos. Esto es útil cuando las PCs están configuradas manualmente y sabemos en qué rangos se encuentran las computadoras.

Cada dispositivo con acceso a la red cuenta con un número de MAC específico de fábrica que lo identifica. Mediante el filtro de MAC, podemos permitir o denegar el acceso a la red por esta dirección.

Recordemos realizar la configuración anotando todos los cambios, estar conectados al router mediante cable y registrar las contraseñas asignadas. Si estamos conectados al router en forma inalámbrica y no lo hemos configurado adecuadamente, probablemente tendremos problemas de conexión.

Problemas típicos en redes wireless

SEGURIDAD, ANCHO DE BANDA Y POTENCIA DE LA SEÑAL SON ALGUNOS DE LOS PROBLEMAS TÍPICOS QUE PRESENTAN LAS REDES INALÁMBRICAS. EN ESTA SECCIÓN CONOCEREMOS ALGUNAS SOLUCIONES DE OPTIMIZACIÓN QUE PODEMOS CONFIGURAR PARA QUE NUESTRA EXPERIENCIA INALÁMBRICA SEA MÁS EXITOSA.



[01]

La débil recepción que experimentan algunas placas wireless PCI en equipos de escritorio se soluciona incorporando una interfaz WiFi USB, que, mediante un cable extensor, puede acomodarse en una posición más despejada. Según la potencia del router emisor, puede ser con antena externa o sin ella.

[02]

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

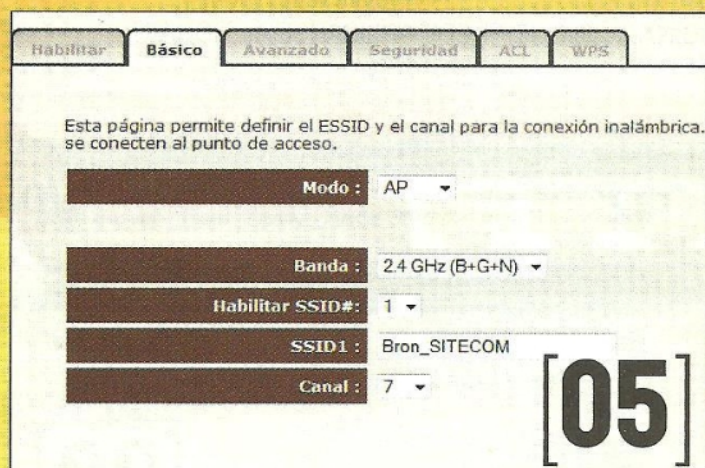
[03]

En los sistemas operativos de Microsoft, podemos aumentar el nivel de recepción mediante la función **PowerSaveMode**, a la que accedemos a través de las propiedades de la placa WiFi. En la opción [Configuración/Opciones Avanzadas], ponemos [Maximum].

[04]

La seguridad es un elemento ineludible en una red WiFi. Para evitar intromisiones, es conveniente encriptar el tráfico de red mediante una clave WAP (más segura que la WEP) y bloquear el acceso a la configuración del router cambiando la clave de fábrica (suele ser "admin" o "1234").

A VECES, EL MANUAL ES LA MEJOR FUENTE DE SOLUCIONES.



[06]



[07]



[08]

[05]

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

[06]

Muebles metálicos, así como puertas y ventanas metálicas, horno a microondas y todo aparato emisor o receptor de señales de radio u ondas electromagnéticas afectan la señal inalámbrica. Es preciso acomodar el router a la mayor distancia posible de estos elementos.

[07]

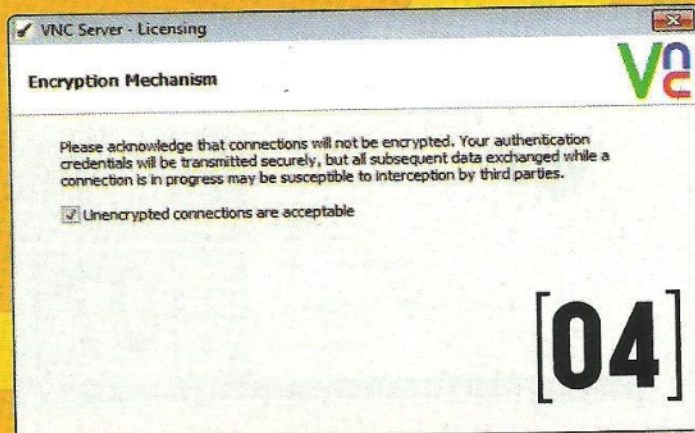
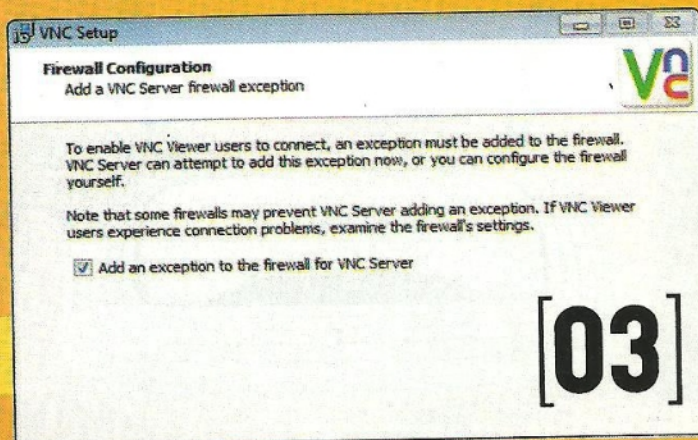
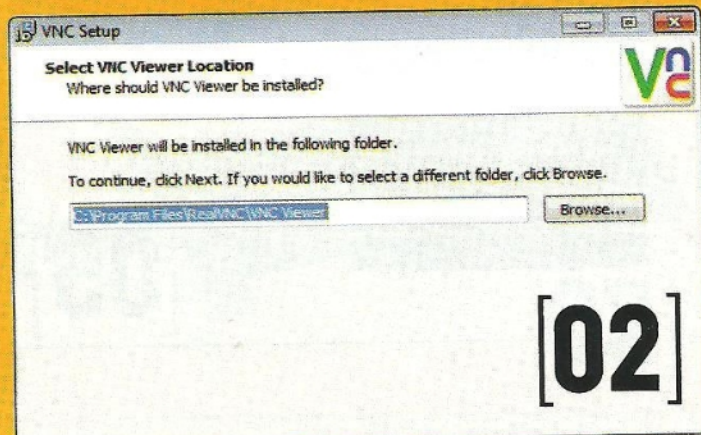
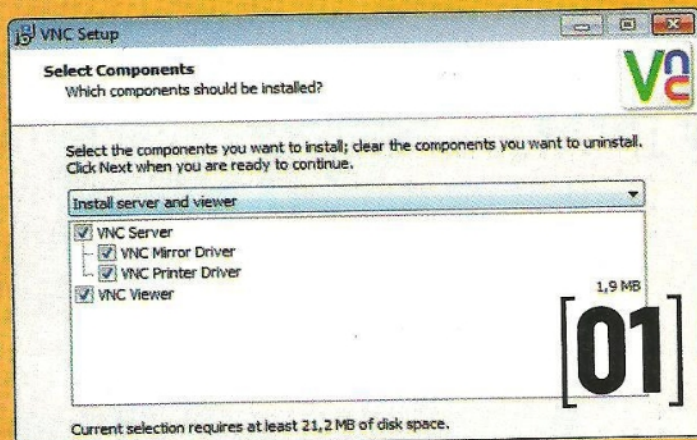
Periódicamente, y más aún si nuestro router tiene algunos años, debemos hacer actualizaciones del firmware, para reparar errores y potenciar el dispositivo. Por lo general, el software actualizado está disponible en la web del fabricante, y se descarga sin costo.

[08]

Si bien todos los routers, como el de la imagen, tienen alternativas de configuración parecidas, debemos consultar el manual de usuario al momento de establecer cuáles son nuestros requerimientos (hogar o empresa, conexión DNS o cablemódem) y qué parámetros alteraremos en función de eso.

Soporte a distancia: **UNC**

CONOCEREMOS AQUÍ REAL VNC, UNA APLICACIÓN CLIENTE-SERVIDOR QUE NOS PERMITIRÁ ASISTIR EN FORMA INMEDIATA A USUARIOS REMOTOS MEDIANTE LA CONEXIÓN A INTERNET. SUELE SER MUY UTILIZADA EN AMBIENTES DE OFICINA, AUNQUE PUEDE APLICARSE AL HOGAR.



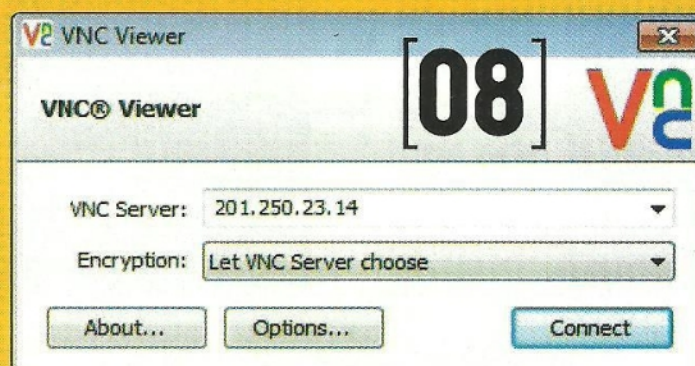
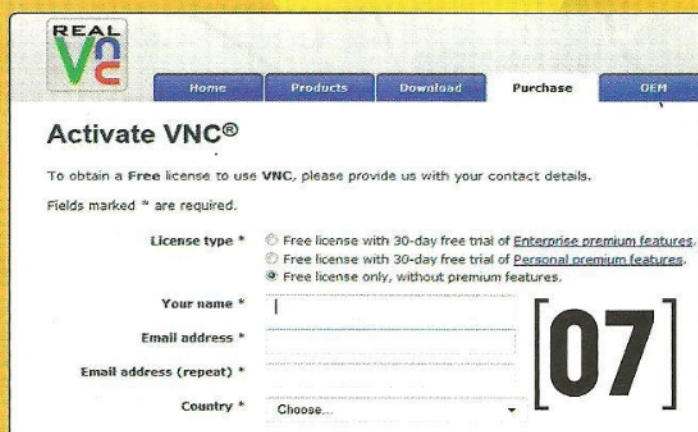
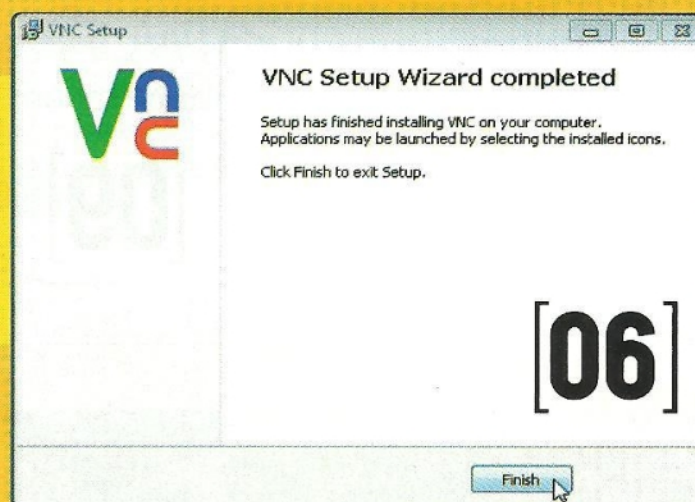
[01] Descargamos la aplicación desde www.realvnc.com y luego la ejecutamos. Durante la instalación, nos pregunta si deseamos instalar VNC Server (máquina a la que vamos a asistir) y VNC Viewer (máquina cliente). Dejamos las opciones predefinidas o marcamos [Server] y continuamos.

[02] Se nos advierte que la instalación del programa copiará los archivos en la ruta especificada. Es conveniente no cambiar la ubicación de la carpeta pensando en posibles actualizaciones. Simplemente, hacemos un clic en [Next>] hasta que aparezcan las opciones de las primeras configuraciones.

[03] El firewall de Windows puede llegar a bloquear conexiones entrantes por puertos determinados. Uno de esos puertos es el que VNC utiliza para comunicarse con el host. Dejar activa esta selección hace que, durante la instalación, VNC añada automáticamente la excepción en el firewall.

[04] Al marcar esta opción, permitimos que las conexiones no encriptadas sean aceptadas. La conexión se establecerá de forma segura, pero el intercambio podrá ser interceptado. Si utilizamos VNC para una asistencia en red local con IP de LAN, podemos activar la opción.

EN INTERNET ENCONTRAREMOS OTRAS APLICACIONES DE ESTE TIPO. SOLO DEBEMOS PROBARLAS PARA ELEGIR.



[05]

La instalación es rápida y no requiere de demasiados detalles técnicos. No obstante, es posible configurarla posteriormente según nuestras necesidades. Al terminar el proceso, se nos advierte que estamos activos para conexiones entrantes y se nos da el número de IP de nuestra máquina.

[06]

Una vez que terminamos con los pasos de la instalación, presionamos [Finish]. Veremos que en la carpeta Real VNC, instalada en el menú de programas, se encuentran el servidor y el visor de VNC. Para iniciar una conexión de asistencia remota a un server iniciamos la aplicación **Viewer**.

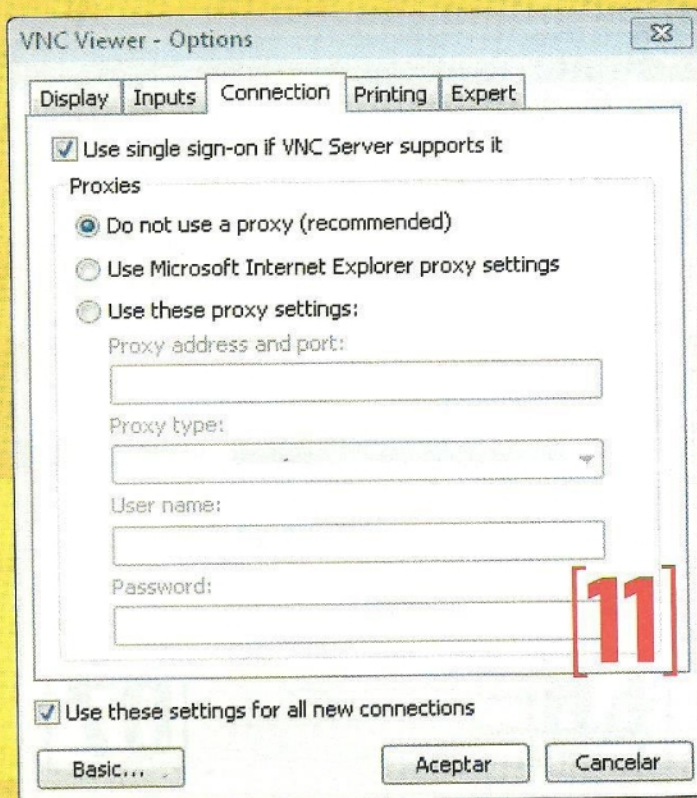
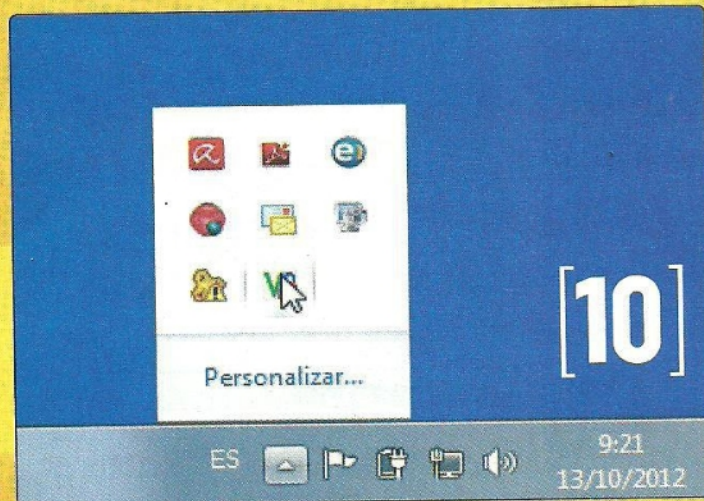
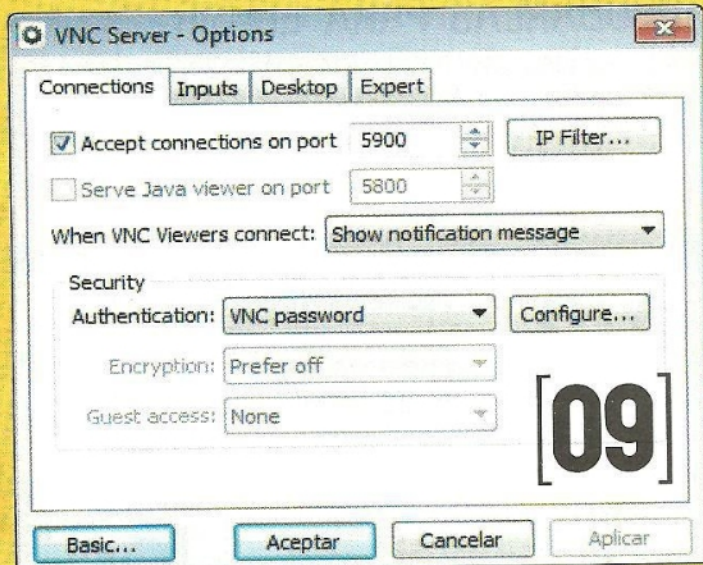
[07]

Antes de comenzar a utilizar la aplicación, **Real VNC** nos pide que activemos una licencia. Al aceptar, nos remite a la página. Elegimos el tipo de licencia y llenamos el formulario, tras lo cual nos da un número. Las licencias pagas tienen mayores prestaciones e incorporan soporte técnico.

[08]

Accedemos a una computadora por su IP. Si estamos dentro del mismo grupo o dominio, bastará con el número de IP local. También podemos utilizar el navegador y colocar la IP que tiene el server dentro de la red WAN y el número de puerto agregado en las excepciones del firewall durante la instalación.

ENTRE LAS OPCIONES
DE CONEXIÓN
PODEMOS CREAR
UNA CONTRASEÑA.



[09]

Dentro de las opciones de configuración de VNC, podemos encontrar el número de puerto exceptuado por el firewall para conexiones entrantes. Para acceder a una PC por medio del navegador, escribimos, por ejemplo: **192.168.1.33:5900** y permitimos las advertencias de seguridad que aparezcan. Siempre vamos a encontrarnos con varios carteles que nos preguntarán si estamos seguros de permitir el acceso remoto.

[10]

Podemos apreciar que el icono de VNC, ubicado en la barra inferior, a la derecha, al captar un controlador remoto, cambia del color blanco al negro. Todas las opciones del teclado y del mouse se transfieren a la PC Viewer, así como los drivers de impresión y la transferencia de archivos (en algunas licencias), por lo que el usuario remoto podrá tomar control de estas tareas.

[11]

Debemos tener en cuenta algo fundamental al realizar esta tarea y es que no será posible la comunicación entre computadoras remotas sin la instalación de VNC Server en la máquina que será controlada. Además, debemos cuidar siempre de habilitar los puertos correspondientes en routers y repetidores, y de especificar el número de IP de cada puerto/equipo.