USERS

CONSEJOS PARA OPTIMIZAR NUESTRA RED

REDES WI-FI

EN ENTORNOS WINDOWS

GUÍA PRÁCTICA DE APRENDIZAJE



- TOPOLOGÍAS Y CARACTERÍSTICAS DE RED
- INSTALACIÓN Y CONFIGURACIÓN DE HARDWARE Y SOFTWARE
- SEGURIDAD EN LA RED
- RESOLUCIÓN DE LOS PROBLEMAS MÁS COMUNES
- ANTENAS Y CONECTORES

ALCANCE EL MÁXIMO POTENCIAL DE SUS EQUIPOS

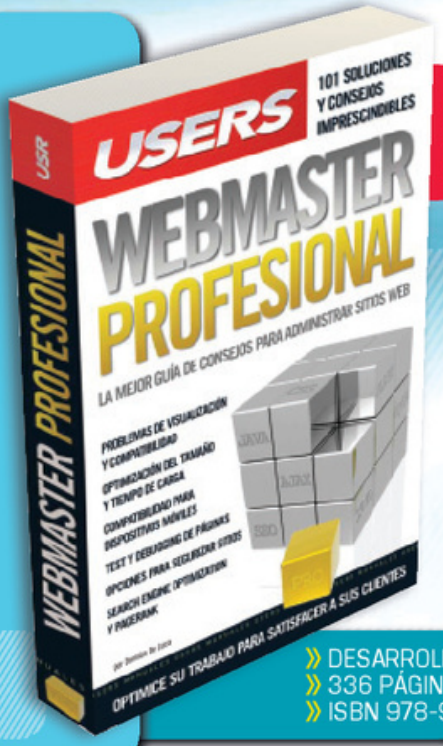
RU RedUSERS

CONÉCTESE CON LOS MEJORES LIBROS DE COMPUTACIÓN



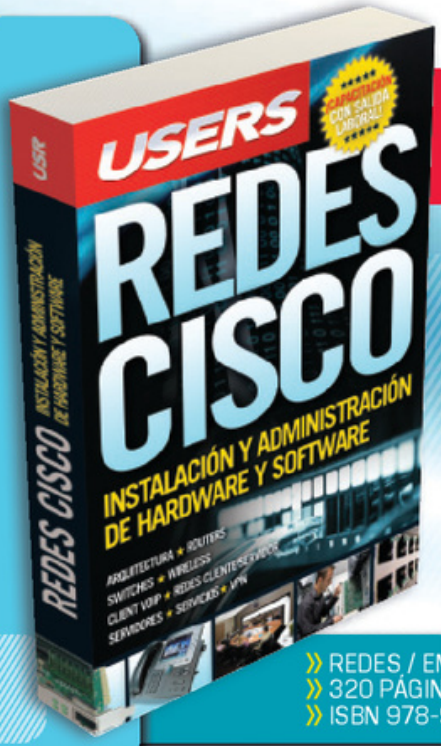
CONOZCA LAS MÁS NOVEDOSAS SOLUCIONES EN REPARACIÓN DE PC

» HARDWARE
» 320 PÁGINAS
» ISBN 978-987-1773-14-5



LOS MEJORES CONSEJOS DE LOS EXPERTOS PARA ADMINISTRAR SITIOS WEB

» DESARROLLO
» 336 PÁGINAS
» ISBN 978-987-663-011-5



PLANIFICACIÓN, INSTALACIÓN Y ADMINISTRACIÓN DE REDES COMPLEJAS

» REDES / EMPRESAS
» 320 PÁGINAS
» ISBN 978-987-663-024-5



¡EXPLICACIONES BASADAS EN EJEMPLOS PRÁCTICOS!

» MICROSOFT / EXCEL
» 368 PÁGINAS
» ISBN 978-987-26013-0-0

LLEGAMOS A TODO EL MUNDO VÍA OCA* Y DHL**

MÁS INFORMACIÓN / CONTÁCTENOS

usershop.redusers.com +54 (011) 4110-8700 usershop@redusers.com

*SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // **VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

REDES WI-FI EN ENTORNOS WINDOWS

GUÍA PRÁCTICA
DE APRENDIZAJE

RedUSERS



TÍTULO: Redes Wi-Fi en entornos Windows

COLECCIÓN: Manuales USERS

FORMATO: 17 x 24 cm

PÁGINAS: 192

Copyright © MMXII. Es una publicación de Fox Andina en coedición con DÁLAGA S.A. Hecho el depósito que marca la ley 11723. Todos los derechos reservados. Esta publicación no puede ser reproducida ni en todo ni en parte, por ningún medio actual o futuro sin el permiso previo y por escrito de Fox Andina S.A. Su infracción está penada por las leyes 11723 y 25446. La editorial no asume responsabilidad alguna por cualquier consecuencia derivada de la fabricación, funcionamiento y/o utilización de los servicios y productos que se describen y/o analizan. Todas las marcas mencionadas en este libro son propiedad exclusiva de sus respectivos dueños. Impreso en Argentina. Libro de edición argentina. Primera impresión realizada en Sevagraf, Costa Rica 5226, Grand Bourg, Malvinas Argentinas, Pcia. de Buenos Aires en X, MMXII.

ISBN 978-987-1857-64-7

Redes Wi-Fi en entornos Windows / coordinado por Gustavo Carballeiro. - 1a ed. - Buenos Aires : Fox Andina; Dalaga, 2012. v. 4, 192 p. ; 24x17 cm. - (Seriada)

ISBN 978-987-1857-64-7

1. Informática. I. Carballeiro, Gustavo, coord.

CDD 005.3



ANTES DE COMPRAR

EN NUESTRO SITIO PUEDE OBTENER, DE FORMA GRATUITA, UN CAPÍTULO DE CADA UNO DE LOS LIBROS EN VERSIÓN PDF Y PREVIEW DIGITAL. ADEMÁS, PODRÁ ACCEDER AL SUMARIO COMPLETO, LIBRO DE UN VISTAZO, IMÁGENES AMPLIADAS DE TAPA Y CONTRATAPA Y MATERIAL ADICIONAL.

RedUSERS
COMUNIDAD DE TECNOLOGIA

redusers.com

Nuestros libros incluyen guías visuales, explicaciones paso a paso, recuadros complementarios, ejercicios, glosarios, atajos de teclado y todos los elementos necesarios para asegurar un aprendizaje exitoso y estar conectado con el mundo de la tecnología.



LLEGAMOS A TODO EL MUNDO VÍA OCA* Y DHL**

*SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // **VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

usershop.redusers.com // usershop@redusers.com

Prólogo



Sabemos que la tecnología informática avanza a pasos muy acelerados, y entonces cobra especial relevancia la frase de Ikujiro Nonaka:

"En un mundo donde la única certeza es la incertidumbre, la única fuente segura de ventaja competitiva es el conocimiento"

Esta frase no solo se acerca a la informática sino también al mundo de las redes y la conectividad, porque siempre necesitamos aprender cosas nuevas y profundizar las que ya conocemos. En todo ámbito, no solo en las nuevas tecnologías, el deseo de aprender y la curiosidad que se presenta en forma inconsciente nos permiten avanzar.

El conocimiento es un gran capital intangible, que en un mundo globalizado marca la diferencia para cualquier empresa con participación en la llamada "batalla competitiva", disputada día a día por el mercado. En este sentido, la importancia de este libro radica en el hecho de comunicar un gran cúmulo de conocimientos a los usuarios y entusiastas de la redes, proporcionándoles herramientas útiles al momento de enfrentar diferentes desafíos para que así puedan tener esa ventaja competitiva que tanto desean las empresas.

Desde el inicio de la obra se tienen en cuenta los temas más relevantes relacionados con la teoría de redes, incluyendo contenido útil referido a las redes inalámbricas, haciendo énfasis en los usuarios sin mucha experiencia y profundizando en algunos conceptos importantes para usuarios más avanzados.

Análisis del hardware necesario y su configuración, identificación y solución de problemas comunes, seguridad de la red, antenas y enlaces. Cada uno de los temas seleccionados posee un valor agregado: se trata del resultado de varios años de experiencia en el trabajo de redes hogareñas.

Gracias a esta obra, el lector podrá permitirse entrar en un mundo tal vez desconocido para él y divertirse aprendiendo nuevos saberes. Es nuestro deseo que este texto sirva para todos aquellos que pretendan iniciarse en las redes inalámbricas. ¡Éxito en sus primeros pasos!

Claudio Alejandro Peña Millahual
Autor y Editor RedUSERS
cpena@redusers.com

El libro de un vistazo

Este libro está destinado a todos aquellos que quieran iniciarse (o ya estén iniciados) en las redes inalámbricas con sistemas Windows. Trataremos los conceptos básicos de red para que quienes carecen de conocimientos previos comiencen a dar sus primeros pasos. Además, los usuarios con experiencia podrán encontrar conceptos y configuraciones avanzadas.

*01 INTRODUCCIÓN A LAS REDES INALÁMBRICAS

Comenzamos el libro explicando el concepto de red y el modelo OSI, que nos proporciona una base ordenada de conocimientos que necesitamos para hacer frente a la gestión de redes inalámbricas. Luego, entraremos en el mundo inalámbrico identificando los componentes que necesitamos para armar este tupo de redes.

*02 HARDWARE PARA REDES INALÁMBRICAS

En este capítulo nos encargaremos de presentar la configuración e instalación de los equipos que pueden ser utilizados en una red inalámbrica, discriminando entre clientes y puntos de acceso a la red. Basándonos en el modelo OSI, revisaremos el hardware que necesitamos y las características de cada uno de ellos. También aprendremos a seleccionar los mejores componentes y daremos algunos consejos que nos servirán a la hora de utilizar las redes inalámbricas.

*03 CONFIGURACIÓN EN WINDOWS

Con la ayuda de este capítulo, vamos a identificar y configurar el hardware de la red para el sistema Windows. Veremos diferentes tipos de configuraciones para nuestra red y la forma de conectarnos a esta.

*04 SEGURIDAD EN LA RED

La seguridad en la red es un tema fundamental que trataremos en profundidad. Desarrollaremos los conceptos básicos para entender cómo proteger nuestra información y de esta manera crear y mantener redes inalámbricas.

*05 RESOLVER PROBLEMAS

Este capítulo enseñará un método ordenado para identificar y corregir problemas en las redes inalámbricas. Tomaremos el modelo OSI para crear una "receta" y, simplificar y ordenar la búsqueda de fallas en nuestra red.

*06 ENLACES

Los enlaces de larga distancia se pueden considerar como una configuración avanzada en redes inalámbricas hogareñas. Por otra parte, cuando utilizamos nuestro teléfono celular con Bluetooth para transferir archivos a la PC estamos formando redes de corta distancia. En este capítulo nos encargaremos de analizar las características de los enlaces de corta distancia y los enlaces de larga distancia, describiendo el potencial de cada uno de ellos y los elementos que necesitaremos.

*07 ANTENAS

Las antenas se consideran componentes fundamentales de una red inalámbrica. A través de este capítulo podremos conocer en forma detallada su funcionamiento cada una de las características básicas que necesitamos para comprender cómo se transmite la información. Además veremos las dversas clasificaciones en las cuales se agrupan las antenas y diferenciaremos sus características, de esta forma sabremos cuando es recomendable utilizar uno u otro tipo de antena.

INFORMACIÓN COMPLEMENTARIA

A lo largo de este manual podrá encontrar una serie de recuadros que le brindarán información complementaria: curiosidades, trucos, ideas y consejos sobre los temas tratados. Para que pueda distinguirlos en forma más sencilla, cada recuadro está identificado con diferentes iconos:


CURIOSIDADES E IDEAS


ATENCIÓN


DATOS ÚTILES Y NOVEDADES


SITIOS WEB

RedUSERS
MEJORA TU PC

La red de productos sobre tecnología más importante del mundo de habla hispana



Libros
Desarrollos temáticos en profundidad

Coleccionables
Cursos intensivos con gran desarrollo visual





Revistas
Las últimas tecnologías explicadas por expertos



RedUSERS
redusers.com
Noticias al día
downloads, comunidad



Newsletters
El resumen de noticias
que te mantiene actualizado
Regístrate en redusers.com



RedUSERS PREMIUM
premium.redusers.com
Nuestros productos en versión digital con contenido ampliado y a precios increíbles



Usershop
usershop.redusers.com
El ecommerce de RedUSERS, revistas, libros y fascículos a un clic de distancia. Entregas a todo el mundo

Contenido

Prólogo 4
El libro de un vistazo 6
Información complementaria 7
Introducción 12

*01 Introducción a las redes inalámbricas

¿Qué es una red? 14
El modelo OSI 14
Funciones de cada capa 15
El modelo TCP/IP 17
Redes inalámbricas 19
Ventajas de utilizar redes inalámbricas 21
Desventajas de utilizar redes inalámbricas 22
Componentes de las redes inalámbricas 24
Puntos de acceso 25



Modos de operación 28
Modo ad hoc 28
Modo infraestructura 30
El estándar IEEE 32
Mejoras de la IEEE 802.11 34
Resumen 37
Actividades 38

*02 Hardware para redes inalámbricas

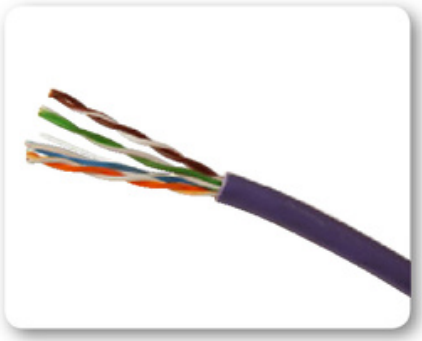
Introducción al hardware inalámbrico 40
Configuración de puntos de acceso 42
Pautas generales a tener en cuenta 42
Instalar el hardware y actualizarlo 44
Configurar con el modelo OSI 49
Capa física 49
Capa de enlace 52
Capa de red 56
Capa de aplicación 57
Resumen 57
Actividades 58



*03 Configuración en Windows

Instalar clientes en Windows 60
¿Qué hardware utilizar? 61
Instalar el hardware es fácil 62
Configurar el hardware en Windows 65

Configurar la red inalámbrica.....79
Configuración de red inalámbrica modo Infraestructura.....87
Resumen.....91
Actividades.....92



*04 Seguridad en la red

Seguridad inalámbrica.....94
Seguridad de la información + WLAN.....96
Atributos de seguridad.....97
Confidencialidad en WLAN.....98
¿Puedo usar WEP?.....98
Luego de WEP, nacen WPA y WPA2.....99
Modos de funcionamiento de WPA.....100
Modos de funcionamiento de WPA2.....104
Autenticación en redes inalámbricas.....105
Evitar difundir la SSID.....106
Filtrar direcciones MAC.....107
Portal cautivo.....108
Integridad de datos en WLAN.....109
Disponibilidad en WLAN.....111
No repudio en redes inalámbricas.....112
Las 10 amenazas más comunes.....113
Resumen.....115
Actividades.....116



*05 Resolver problemas

Enfoque metodológico.....118
Pasos fundamentales a verificar.....120
Tensión eléctrica estable.....**120**



Actualizaciones.....124
Nuestro método.....124
Delimitar el problema.....125
Encerrar la causa del problema.....126
Planear la solución.....127
Corroborar los resultados.....134



Documentar los resultados 135
Caso práctico 136
¿Qué herramientas usar para resolver problemas? 138
Escenarios prácticos 140
Resumen 143
Actividades 144

*06 Enlaces

Enlaces de larga distancia 146
¿Qué es un radioenlace? 149
Tipos de enlaces 152
Alineación de antenas 160
Con extremos visibles 160
Con extremos no visibles 162
Enlaces de corta distancia 162
Los grupos de trabajo de la IEEE 164
¿Dónde se aplica la tecnología WPAN? 166
Bluetooth: ¿qué es y cómo funciona? 167
Topología de red 168
Resumen 169
Actividades 170

*07 Antenas

Antenas 172
Características específicas 172
Clasificación de las antenas 178
Según el patrón de radiación 179
Según su construcción 180
Resumen 183
Actividades 184

* Servicios al lector

Índice temático 186



Introducción



Sabemos que el desarrollo de las telecomunicaciones ha dado un cambio de dirección en los últimos años, entregándonos velocidades de conexión y acceso a información en forma más expedita. Muchos sistemas basados en cable (xDSL, fibra óptica o cable coaxial) que llegan hasta el usuario para ofrecer conectividad a Internet tienen un costo de instalación alto.

Teniendo en mente las limitaciones topográficas y tecnológicas, se han buscado alternativas de conexión en las que la transferencia de información no dependa de un medio físico como el cable. De esta manera, al no utilizar cables, el tiempo necesario para desplegar la tecnología y los servicios asociados se reduce en forma considerable.

Con esta problemática planteada, nacieron y se desarrollaron los estándares inalámbricos IEEE 802.11 (conocidos como WiFi), que constituyen una alternativa a los medios convencionales con los que se accedía al servicio.

Estas nuevas redes que no requieren cables para intercambiar información surgen de la necesidad que tiene el usuario de aumentar su movilidad sin tener que modificar su esquema de red actual. De esta manera, se evita tener que realizar tendidos de cables en edificios o casas particulares, lo que implica un ahorro de tiempo y dinero.

Esta obra presenta la tecnología inalámbrica a los lectores que no tengan conocimiento sobre este tema y aporta nuevos puntos de vista para los usuarios experimentados en redes sin cables. Por lo tanto, este libro es una fuente de nuevos aprendizajes, como así también un material de consulta permanente.

Su desarrollo implicó un aspecto fundamental: lograr explicar con un lenguaje claro y sencillo conceptos que muchas veces parecen difíciles o imposibles de entender. Partir de la base del modelo OSI nos permite luego poder recurrir a este conocimiento para aplicar un método de resolución de problemas. También tratamos las topologías de red más comúnmente usadas, para después adentrarnos en el mundo de lo inalámbrico. Quedan los lectores en buenas manos.

*01 –

Introducción a las redes inalámbricas

En este primer capítulo, nos introduciremos en la teoría básica de las redes. Conoceremos qué es una red de computadoras, con el modelo OSI y TCP/IP como base. Esto nos permitirá estudiar el comienzo histórico de las redes, las configuraciones más usadas y su evolución.

- ¿Qué es una red? 14
- El modelo OSI 14
- El modelo TCP/IP 17
- Redes inalámbricas 19
- Componentes de redes inalámbricas 24
- Modos de operación 28
- El estándar IEEE 32
- Resumen 37
- Actividades 38



↗↗↗

¿Qué es una red?

En estos tiempos que corren, la gran mayoría de las personas ya tienen incorporado el concepto de **red**, pero vale la pena aclararlo. Llamamos **red** a un conjunto de computadoras que están conectadas entre sí por algún medio que puede ser **físico** (**cables**) o no (**ondas electromagnéticas**). El objetivo principal de la red es que se puedan compartir recursos e información entre todos los elementos que la integran, y tener flexibilidad para así optimizar tareas o procesos que los usuarios realizan. Las redes de computadoras evolucionan para obtener mayor movilidad y/o rendimiento de las tareas.

El modelo OSI

El **modelo de referencia OSI** (**Open System Interconnection**, en español: Interconexión de Sistemas Abiertos), creado en **1984** por la **ISO** (**International Organization for Standardization**, en español: **Organización Internacional para la Normalización**), nació de la necesidad de poder comunicarse y trabajar de forma conjunta con las diferentes redes que existían tiempo atrás. Cada red podía usar una especificación diferente, lo que resultaba en incompatibilidades a la hora de comunicarse entre sí. Estas incompatibilidades eran en su mayoría diferencias en el hardware y software que se utilizaba, y esto hacía imposible que la comunicación fuera exitosa. La ISO creó un idioma en común, de manera de asegurar la compatibilidad.

El modelo OSI consta de **7** capas numeradas, y cada una de ellas cumple una función de red específica. Con esta **división en capas** se

PRINCIPIO DEL MODELO OSI

En el año **1980**, las redes se encontraban en un verdadero estado de caos y desorden: crecían en tamaño y cantidad sin regulación. Luego, cuando las empresas vieron las ventajas de interconectarse, nació el modelo OSI, que sigue vigente. Podríamos decir que se hablaban diferentes idiomas hasta que, con el modelo OSI, todos se unificaron en un idioma universal.

logra que los usuarios puedan ver las funciones de red de cada capa y, así, comprendan cómo son transportados los datos.

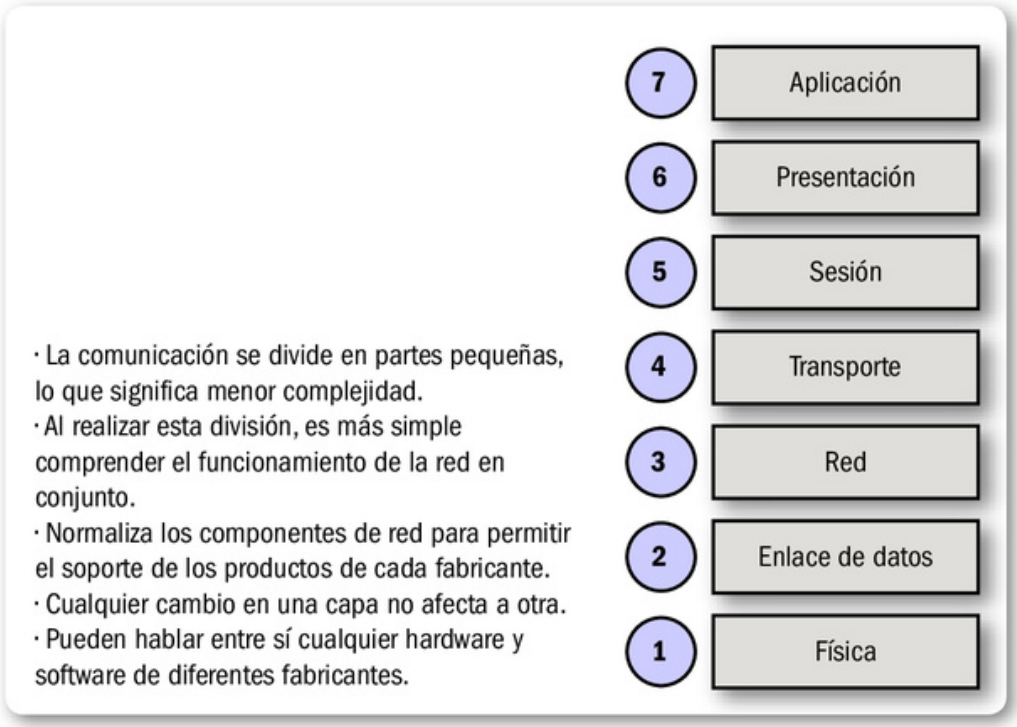


Figura 1. La división en capas de las funciones en una red planteada por el modelo OSI nos permite tener algunas ventajas.

Funciones de cada capa

En el modelo OSI identificamos que cada una de las 7 capas debe realizar un conjunto de funciones para que los datos viajen en la red desde el emisor hasta el receptor, y que, de este modo, la información

NACIMIENTO DEL TCP/IP

El modelo TCP/IP nació de la necesidad del **Departamento de Defensa de EE.UU.** de tener una red que pudiera soportar cualquier catástrofe, como, por ejemplo, una guerra nuclear. TCP/IP asegura que los datos enviados desde un emisor lleguen a destino bajo cualquier condición. Este modelo se transformó en el estándar a partir del cual se creó Internet.

pueda ser transmitida sin problemas. Para ilustrar este proceso realizaremos una breve descripción de las capas, tomando como referencia el esquema que se presenta en la figura siguiente.

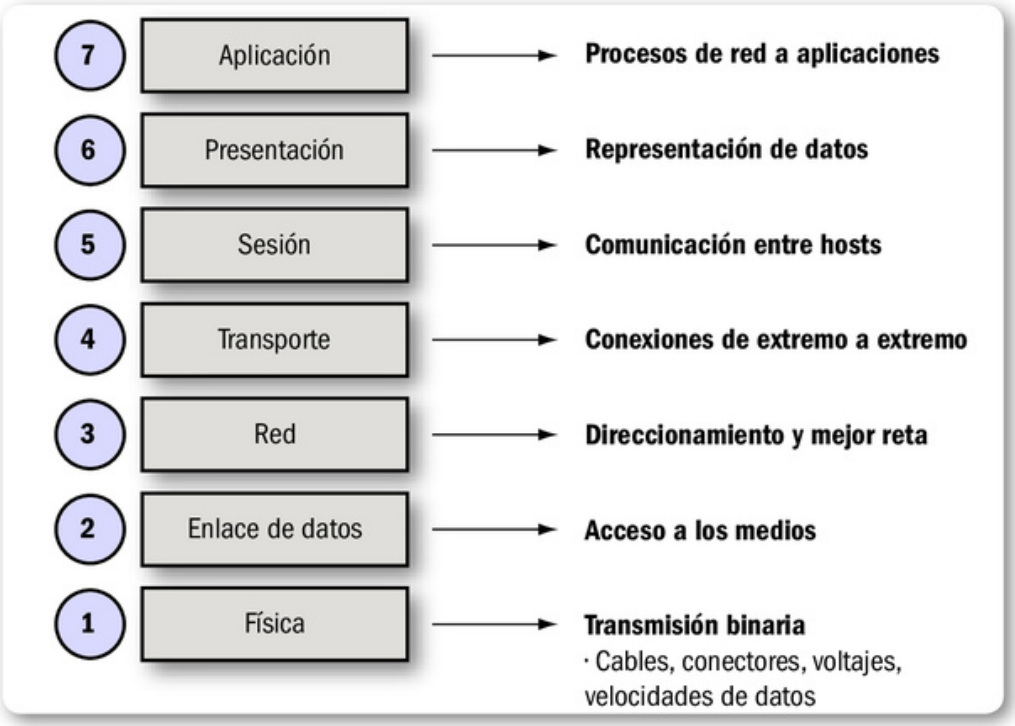


Figura 2. Cada una de las capas del modelo OSI posee funciones que, con ayuda de este esquema, podremos recordar fácilmente.

- **7- Capa de Aplicación**: esta es la capa con la que más interactúa el usuario. No da servicios a las demás capas del modelo OSI, sino solo a aplicaciones fuera del modelo. Cuando un usuario necesita realizar una actividad (leer o escribir e-mails, enviar archivos, usar una hoja de cálculo, un procesador de texto o similar), el sistema operativo va a interactuar con esta capa para llevarla a cabo.
- **6- Capa de Presentación**: acá se busca tener un formato de datos en común, para garantizar que los datos enviados por la capa 7 de un sistema puedan ser entendidos por la misma capa 7 pero de otro sistema. En caso de ser necesario, la información será traducida usando un formato en común. Algunos ejemplos en esta capa pueden ser los formatos **MP3**, **JPG** y **GIF**, entre otros.
- **5- Capa de Sesión**: en esta capa establecemos, mantenemos y

terminamos las comunicaciones entre los dispositivos de red que se están comunicando. Podemos pensar esta capa como una conversación.

- **4- Capa de Transporte**: verifica si los datos vienen de más de una aplicación e integra cada uno de ellos en un solo flujo de datos dentro de la red física. A esto lo llamamos **control de flujo de datos**. Por otra parte, se encarga de realizar la verificación de errores y también la recuperación de datos.
- **3- Capa de Red**: se trata de la capa que determina cómo serán enviados los datos al receptor. También efectúa la conexión y la selección de la ruta entre dispositivos que pueden estar en diferentes redes.
- **2- Capa de Enlace de Datos**: a los datos provenientes de la capa 3 se les asigna el correspondiente protocolo físico (para hablar el mismo idioma), se establece el tipo de red y la secuencia de paquetes utilizada.
- **1- Capa Física**: es la parte de hardware del modelo. Acá se definen las especificaciones o características físicas de la red, como niveles de voltaje, cableado, distancias de transmisión máximas y conectores físicos usados, entre otros atributos descriptos dentro de las especificaciones de la esta capa.

> LA CAPA DE RED SE ENCARGA DE DETERMINAR EL ENVÍO DE DATOS AL RECEPTOR

El modelo TCP/IP

Debemos tener en cuenta que existe otro modelo paralelo al OSI llamado **TCP/IP**. Se trata de un modelo que es mucho más conocido entre los usuarios de redes informáticas. Este es el estándar abierto de Internet, que hace posible la comunicación entre computadoras ubicadas en cualquier parte del mundo. **TCP/IP** significa **Protocolo de Control de Transmisión/Protocolo de Internet** y, a diferencia del modelo OSI, posee cuatro capas: **Aplicación**, **Transporte**, **Internet** y **Acceso a la red**.

Las capas del modelo OSI se entremezclan y dan como resultado las 4 capas que corresponden al modelo TCP/IP.

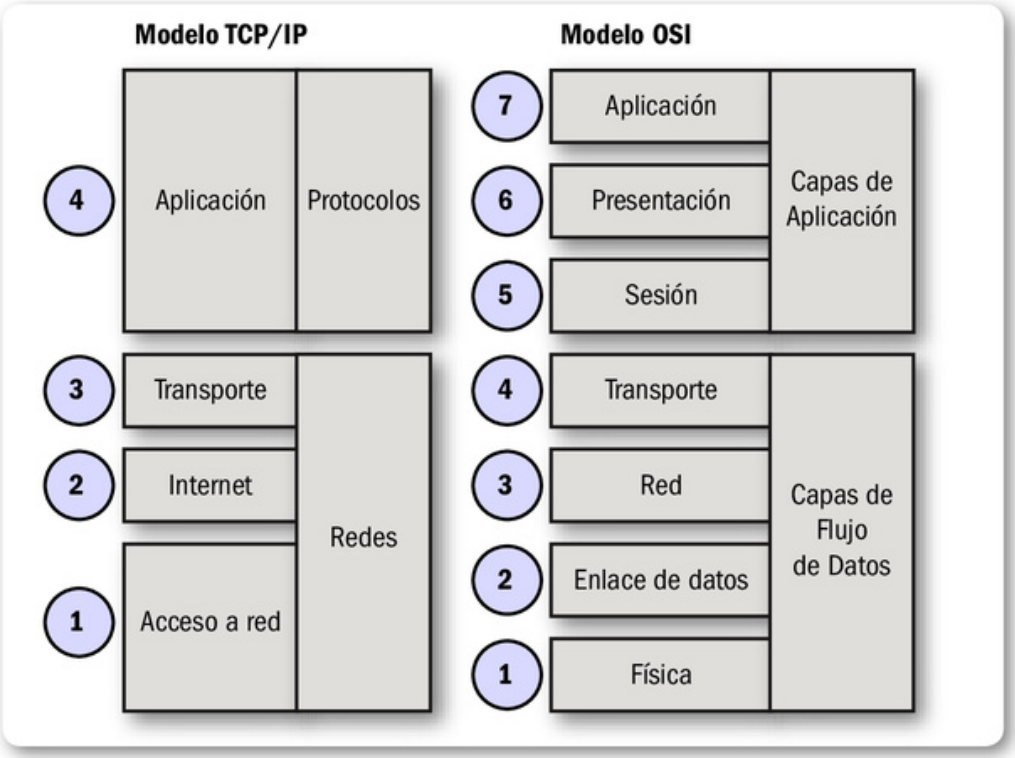


Figura 3. Comparación entre el modelo TCP/IP de 4 capas y el modelo original OSI de 7 capas. Vemos las capas que se entremezclan en el modelo OSI para obtener las equivalentes en TCP/IP.

- **4- Capa de Aplicación**: aquí se combinan todos los aspectos relacionados con las aplicaciones. De esta forma, las capas de Sesión, Presentación y Aplicación del modelo OSI son equivalentes a la Capa de Aplicación en TCP/IP, que nos garantiza la correcta disposición de los datos para la siguiente capa.
- **3- Capa de Transporte**: esta capa del modelo TCP/IP directamente se corresponde con la Capa de Transporte del modelo OSI.
- **2- Capa de Internet**: corresponde a la Capa de Red del modelo OSI. El principal objetivo de esta capa es realizar el envío de datos desde cualquier red y que estos lleguen al destino, independientemente de la ruta o redes necesarias para llegar.
- **1- Capa de Red**: combinando la Capa Física y la de Enlace de Datos del modelo OSI, obtenemos esta capa del modelo TCP/IP. Su objetivo es enrutar los datos entre dispositivos que se encuentren en la misma red informática.

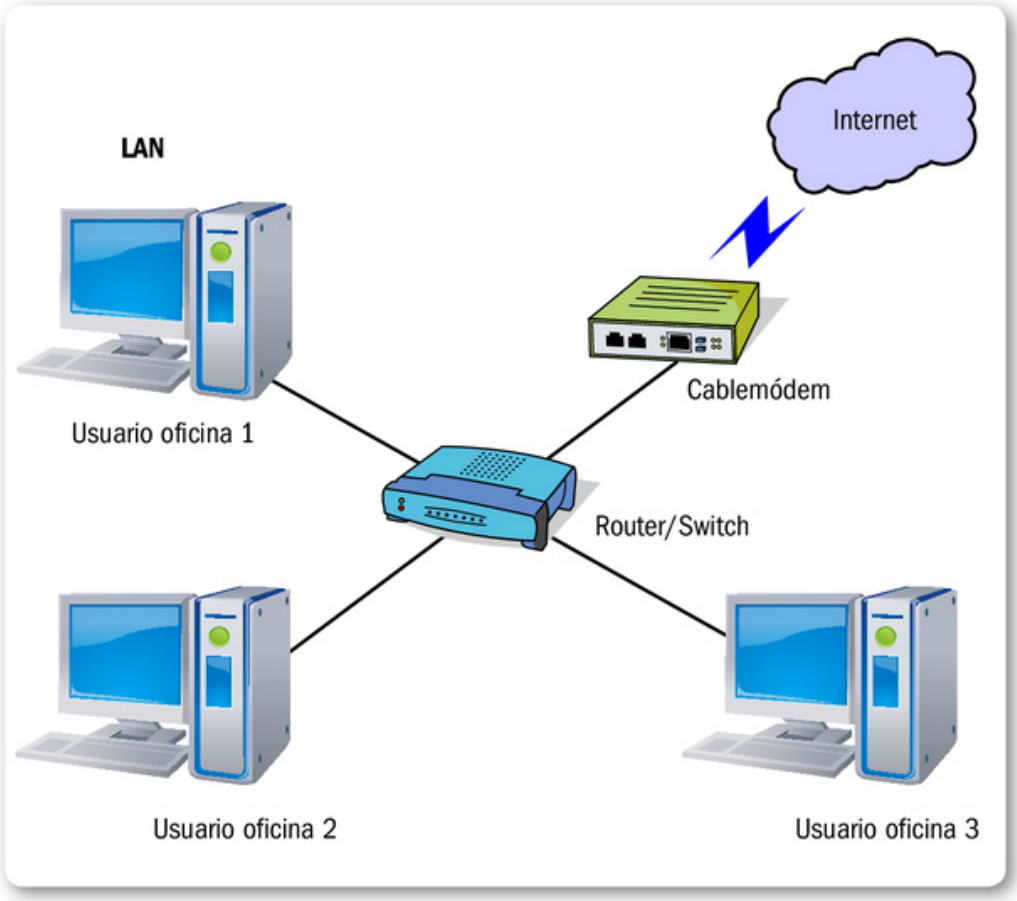


Figura 4. Ejemplo de una red LAN. En este caso, perteneciente a una pequeña oficina con tres usuarios.

Redes inalámbricas

Inalámbrico hace referencia a la tecnología sin cables que nos permite conectar dispositivos entre sí para formar una red.

Podemos clasificar a las redes inalámbricas de la misma manera que lo hicimos con las redes cableadas; en este caso, tendremos cuatro categorías, basándonos en el alcance: redes WAN, redes MAN, redes LAN y redes PAN. Cada una de ellas se diferencia del resto según la extensión física que cubre, aunque para las redes inalámbricas encontraremos que los límites son más difusos, por tratarse de medios de dispersión no físicos.

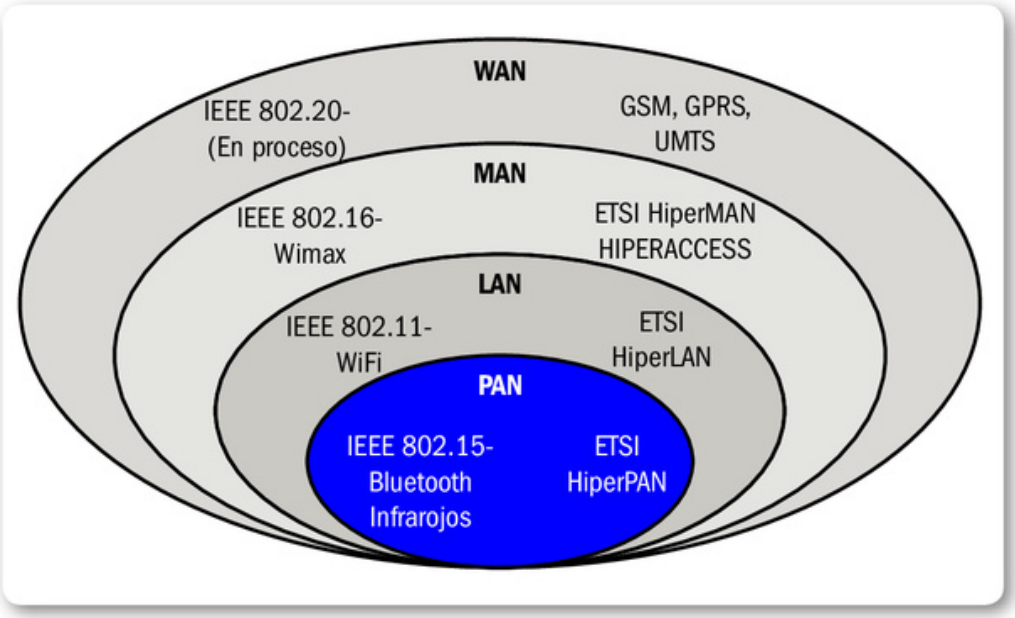


Figura 5. Estas son las diferentes tecnologías inalámbricas junto con sus estándares. Para LAN, tenemos **IEEE 802.11-WiFi**.

Nos centraremos en la categoría **LAN**, en la que definimos una red de área local inalámbrica como una red de alcance local que tiene como medio de transmisión el aire (**WLAN**). A este tipo de red inalámbrica se la conoce en el mercado como **WiFi** y opera en la banda de **2,4 GHz**.

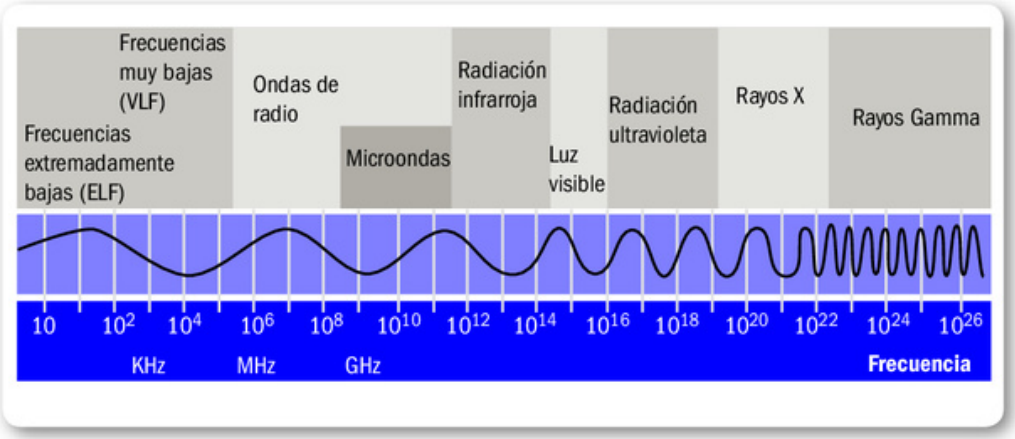


Figura 6. Espectro electromagnético y los diferentes usos según la banda de frecuencia que corresponde.

Ventajas de utilizar redes inalámbricas

Vamos a describir algunas ventajas que obtenemos al usar una red inalámbrica comparándola con las redes cableadas clásicas. La primera ventaja que surge, y una de las más importantes, es la **movilidad** que adquiere el usuario de estas redes.

La **portabilidad** es otro punto fundamental, ya que permite a los usuarios moverse junto con los dispositivos conectados a la red inalámbrica, tales como **notebooks**, **netbooks** o similares, sin perder el acceso a la red. Así, se facilita el trabajo, al permitir la movilidad por toda el área de cobertura.

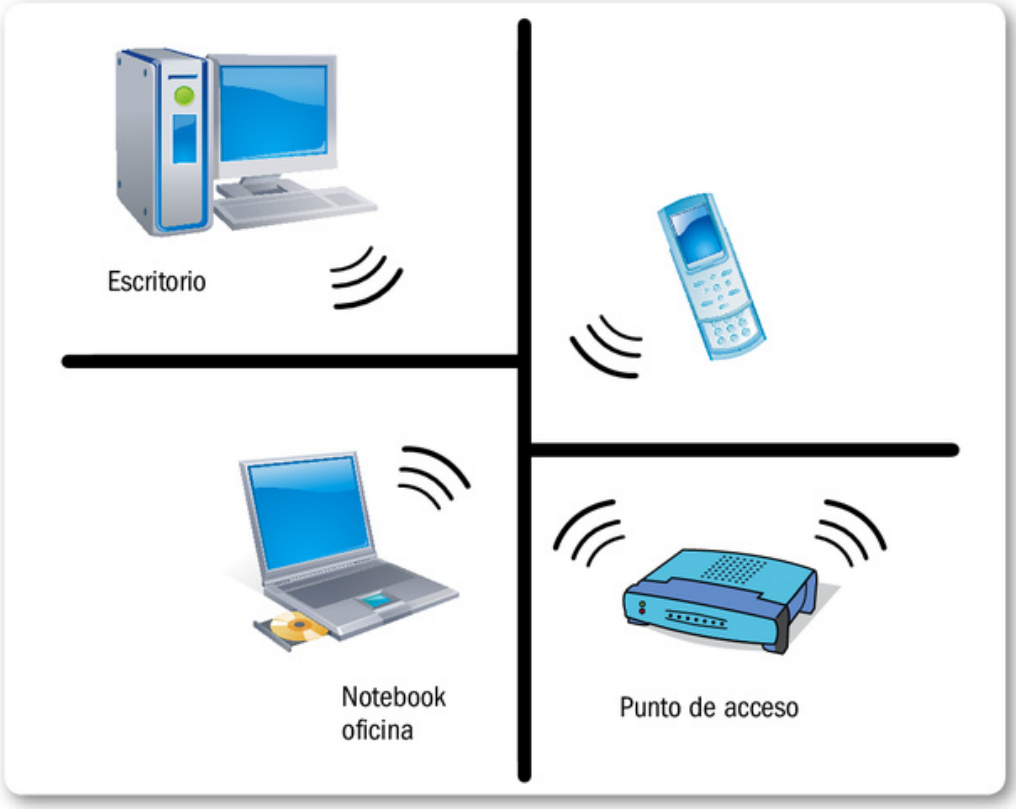


Figura 7. Entre las ventajas de las redes inalámbricas hogareñas encontramos la portabilidad y la flexibilidad.

La **flexibilidad** es otra ventaja de las redes sin cables. Podemos situar nuestra notebook sobre la mesa del escritorio para luego desplazarla hacia el dormitorio, sin tener que realizar el más mínimo cambio de configuración de la red.

Al tratar de extender una red cableada clásica, se presentan ciertos problemas, ya que esta no es una tarea fácil ni barata. En cambio, cuando queremos expandir una red inalámbrica, luego de su instalación inicial, simplemente debemos adquirir una placa de red inalámbrica (si es que la computadora no cuenta con una), y ya estaremos conectados. Esto se llama **escalabilidad**, que se define como la facilidad de expandir la red después de haberla instalado.

Desventajas de utilizar redes inalámbricas

Las redes cableadas, en la actualidad, trabajan con velocidades de 100 Mbps a 10.000 Mbps, que se reduce en redes sin cables y se traduce en una **menor velocidad**. WiFi trabaja en velocidades de 11 a 108 Mbps, aunque existen soluciones y estándares propietarios que llegan a mejores velocidades, aunque a un precio muy superior.

Podemos decir que, en este caso, es necesario hecer una **mayor inversión inicial**, ya que el costo de los equipos de red inalámbricos es superior al de los requeridos en una red cableada. Pero no se trata de una diferencia inalcanzable para una red pequeña hogareña.

Dijimos anteriormente que una ventaja de las redes inalámbricas es que no necesitan un medio físico para funcionar. Esto se convierte en desventaja cuando tenemos en cuenta la **seguridad** de la red. En este sentido, pensemos que cualquier persona con una notebook, un teléfono u otro dispositivo con WiFi puede intentar acceder a nuestra red tan solo estando en el área de cobertura.

El **alcance** de una red inalámbrica está determinado por la potencia de los equipos y la ganancia que caracterice a las antenas. Así, si estos



BANDA BASURA

La historia del WiFi inicia en **1985**, cuando el gobierno de los Estados Unidos (junto con la **Comisión Federal para las Comunicaciones**) decidió que se pudieran usar ciertas bandas del espectro sin tener una licencia. La llamada **banda basura de 2,4 GHz** era una de estas bandas, que solo era utilizada para hornos microondas o equipos similares que generaban ruido de radiofrecuencia.

parámetros no son suficientes, encontraremos puntos en nuestra casa u oficina donde no tendremos la cobertura adecuada.

Por último, pero no menos importante, otra desventaja son las interferencias sufridas en la banda de frecuencias de 2,4 GHz. Al no requerir licencia para operar en esta banda, muchos equipos del mercado la utilizan (**teléfonos inalámbricos** y **microondas**, entre otros), sumado a que todas las redes WiFi funcionan en la misma banda de frecuencias, incluida la de nuestro vecino.



Figura 8. Las interferencias son una de las principales desventajas en las redes. En este caso, el horno microondas y el teléfono provocan una pérdida de señal.

CENTRO DE GRAVEDAD

La señal wireless de un router es de 360 grados. Se expande en todas direcciones, reduciéndose a medida que aumenta la distancia o se encuentran obstáculos. Así, lo importante es encontrar el centro de gravedad de la sala para situar el punto de acceso WiFi.

Componentes de las redes inalámbricas

En esta sección conoceremos los diferentes dispositivos que son necesarios para implementar nuestras propias redes inalámbricas. Los fundamentales son los siguientes: placa de red inalámbrica, punto de acceso (**AP**, **Access Point** en inglés), router inalámbrico y antenas. Además, tengamos en cuenta que existen otros equipos y accesorios que se utilizan, pero los veremos con menos detalles.

- **Placa de red inalámbrica**: recibe y envía información entre las computadoras de la red; es una parte imprescindible para conectarnos de forma inalámbrica. Existen placas de diferentes velocidades, entre 54 Mbps y 108 Mbps. Todas tienen una antena (que puede ser externa o interna), en general, de baja ganancia, que puede ser reemplazada por otra de mayor ganancia para mejorar la conexión (cuando el dispositivo lo permita). Veremos más sobre antenas en el capítulo correspondiente. Si poseemos una notebook o algún celular de última generación, la placa viene integrada.

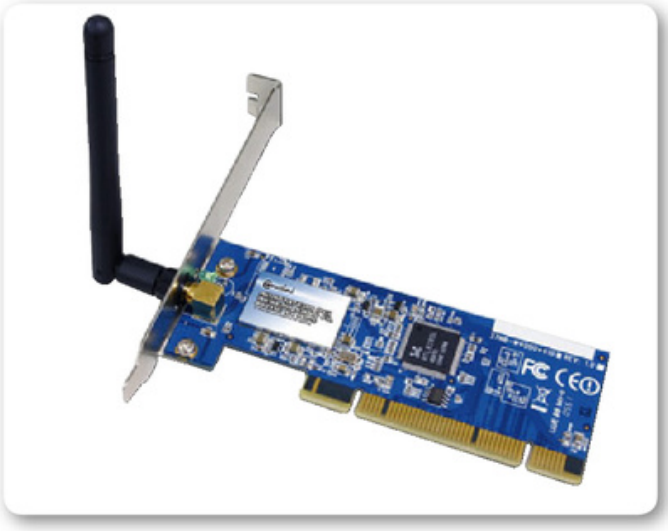


Figura 9. Las placas PCI inalámbricas son utilizadas en PC hogareñas para evitar conectarnos con cables a la red de datos.

Existen tres tipos de adaptadores para utilizar: PCI, usados en nuestras PCs de escritorio; PCMCIA/PCcard, utilizados en las primeras laptops o notebooks; y USB, que son muy comunes hoy en día para notebooks o netbooks.

Puntos de acceso

Se considera como el punto principal de emisión y recepción. Este punto concentra la señal de los nodos inalámbricos y centraliza el reparto de la información de toda la red local. También realiza el vínculo entre los nodos inalámbricos y la red cableada; por esto se lo suele llamar **puente**.



Figura 10. La figura nos muestra un típico AP (Access Point) que encontramos en el mercado.

Cuando conectamos varios AP (**sincronizados**) entre sí, podemos formar una gran red sin utilizar cables. Si necesitamos una idea

ROUTER INALÁMBRICO

Es muy común confundir el término Access Point con router inalámbrico. Este último es un Access Point combinado con un router y puede realizar tareas más difíciles que las del AP. Pensemos al router inalámbrico como un **puente** (que une la red cableada y la no cableada) y un **direccionador** (que selecciona el destino según el enrutamiento del protocolo IP)

práctica para entender el concepto de punto de acceso, podemos situarnos del lado del cliente (notebook, por ejemplo) y pensar que el **punto de acceso** provee un cable virtual entre cada cliente asociado a él. Así, este cable inalámbrico nos conecta a la red cableada como a cada uno de los demás usuarios de la red inalámbrica.



Figura 11. Un router inalámbrico nos permite usar las diversas configuraciones en nuestra red.

- **Router inalámbrico**: si tenemos una conexión **ADSL** que nos da acceso a Internet a través de la línea telefónica, este dispositivo será el encargado de conectarnos. Pero esta no es la única función, ya

MÚSICA EN TODOS LADOS

La empresa **Sonos**, que fabrica equipos inalámbricos, presentó un sistema de música distribuida para toda nuestra casa. Funciona ubicando sistemas en diferentes puntos, que se enlazan mediante WiFi para que, luego, el usuario seleccione la canción que desea escuchar en cada zona de su hogar.

que, además, permite distribuir Internet mediante cables y de forma inalámbrica mediante el punto de acceso que tiene integrado. También realiza restricciones de acceso, por usuarios, servicios y horarios, entre otras opciones, y puede controlar el ancho de banda y las prioridades de acceso por cliente conectado o servicio.



Figura 12. Algunos modelos de routers inalámbricos que existen en el mercado poseen antenas externas.

- **Antena**: se trata de un elemento muy importante en la red, porque se encarga de transformar la energía de corriente alterna, generada en los equipos inalámbricos de la red, en un campo electromagnético, o viceversa, para que la comunicación pueda realizarse entre los equipos. Si la transformación es eficaz, obtendremos mayor área de cobertura (o alcance) sin importar el equipo que tengamos. Pensemos en la antena como en un dispositivo que nos permite convertir la señal eléctrica en ondas electromagnéticas. Solamente de la antena depende más del 50% de la calidad de conexión para un dispositivo de la red; por eso necesitamos que este elemento sea bueno o superior.



Figura 13. Existen muchas variedades de antenas según sus características, como ganancia y tamaño, entre otras.

Modos de operación

Cuando pensamos en los modos de operación de las redes inalámbricas, y refiriéndonos a los **estándares 802.11**, podemos definir dos modos fundamentales: **ad hoc** e **infraestructura**.

Modo ad hoc

Este modo se presenta como el más sencillo para configurar. Los únicos elementos necesarios para conformar una red en **modo ad hoc** son los dispositivos móviles que poseen placas de red inalámbricas. También se lo conoce con el nombre de punto a punto, ya que permite establecer comunicación directa entre los usuarios sin necesidad de involucrar un punto de acceso central que realice el vínculo.

WIFI + PICNIC + REUNIÓN

WiFiPicning es la última moda para conocer gente. Nacida en Francia pero extendida a otros lugares, agrupa a personas con sus notebooks en torno a un Hot Spot donde comparten charlas, bebidas y tiempo. Lo llamativo es que los participantes se conectan a un chat e interactúan desde sus computadoras.

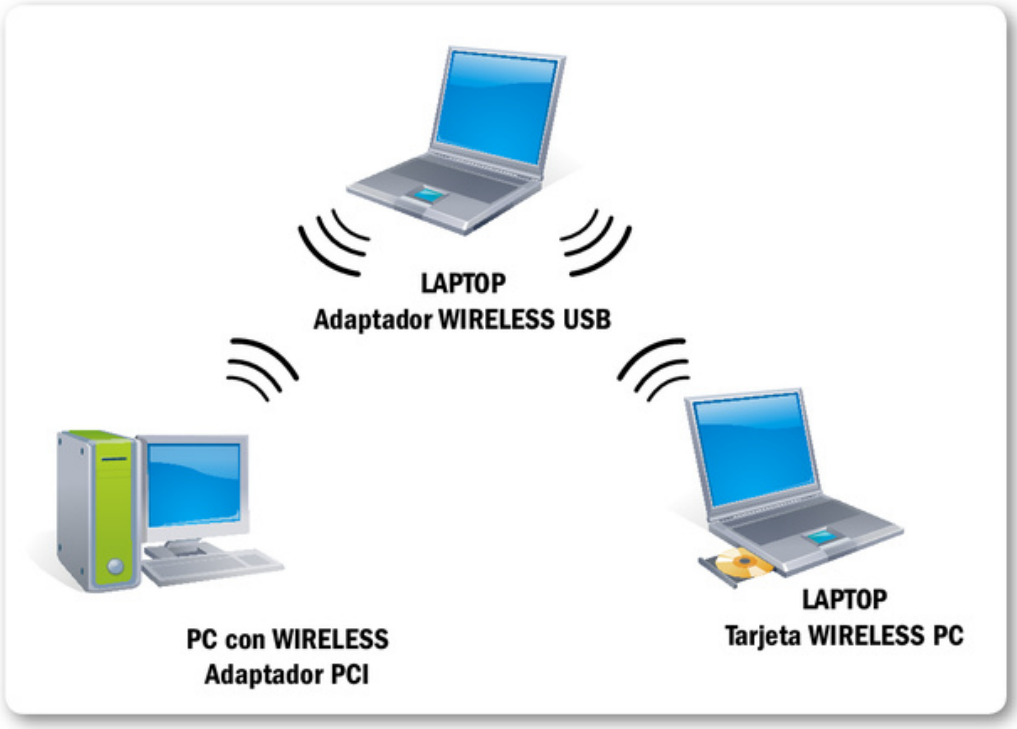


Figura 14. Ejemplo de una red ad hoc conformada por dispositivos comunes en cualquier hogar.

En pocas palabras, todos los nodos de una red ad hoc se pueden comunicar directamente con otros dispositivos y no es necesario ningún tipo de gestión administrativa de la red (punto de acceso).

Este tipo de red es común entre usuarios que desean compartir contenidos sin tener que conectar sus computadoras a redes habilitadas, ya que supone una configuración rápida y sencilla, para lo cual, en sistemas Windows, solo hay que seguir un asistente.

802.11 EN JAPÓN Y EUROPA

Debido a su tardía llegada al mercado, la norma conocida como **802.11a** no fue exitosa. Esto se sumó a que en **Europa** la frecuencia de **5 GHz** está reservada para **HiperLan**, porque posee mayor penetración comercial que 802.11a. Por otra parte, en **Japón**, la frecuencia de 5 GHz también está parcialmente disponible, por lo que no es muy común encontrar dispositivos que usen 802.11a. Todo esto contribuyó a que no se considere la mejor opción en los dos lugares mencionados.

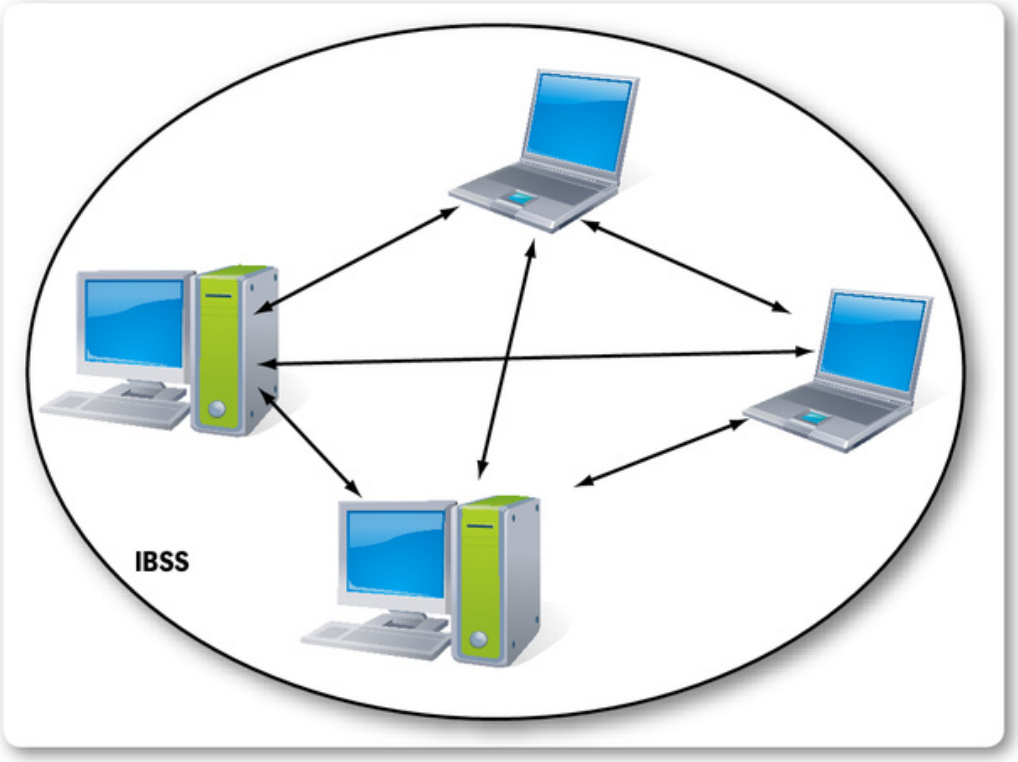


Figura 15. El modo ad hoc, según el estándar inalámbrico, se denomina **Conjunto de Servicios Básicos Independientes** (IBSS, por sus siglas en inglés).

Modo infraestructura

En las configuraciones en modo infraestructura usamos el concepto de **celda**, similar al implementado en la red de telefonía celular. Entendemos por celda al área en la que una señal radioeléctrica es efectiva. Así, una red inalámbrica puede tener una celda de tamaño reducido y, por medio de varios puntos de emisión, es posible combinar las celdas y tener un área mayor.

Logramos esto utilizando los famosos puntos de acceso, que funcionan como **repetidores** y, por eso, pueden duplicar el alcance de la red, ya que en este caso, la distancia máxima no es entre estaciones, sino entre una estación y un punto de acceso. Estos dispositivos capaces de extender una red son colocados en lugares estratégicos, en general, altos y, además, realizan la coordinación del funcionamiento entre usuarios. Con solo un punto de acceso podemos soportar un

grupo acotado de usuarios, y el rango será de entre 30 metros y varios cientos de metros. Si queremos conectar varios puntos de acceso y usuarios, todos deben configurar el mismo SSID.



Figura 16. Como vemos en esta imagen, un mismo punto de acceso puede proveer de comunicación a usuarios con diferentes adaptadores de red inalámbrica en modo infraestructura.

VER A TRAVÉS DE LAS PAREDES CON WIFI

En la **Universidad de Utah**, en EE.UU., aseguran que investigadores lograron ver a través de las paredes utilizando señales de redes inalámbricas. Estas señales se llaman **imágenes tomográficas de radio** basadas en la varianza y utilizan el protocolo **IEEE 802.15.4**, muy común en servicios como **Zigbee**.

El estándar IEEE

Un **estándar** se define como un conjunto de normas y recomendaciones técnicas que se encarga de regular la realización de ciertos procesos o la fabricación de componentes para garantizar la interoperabilidad y compatibilidad entre ellos.

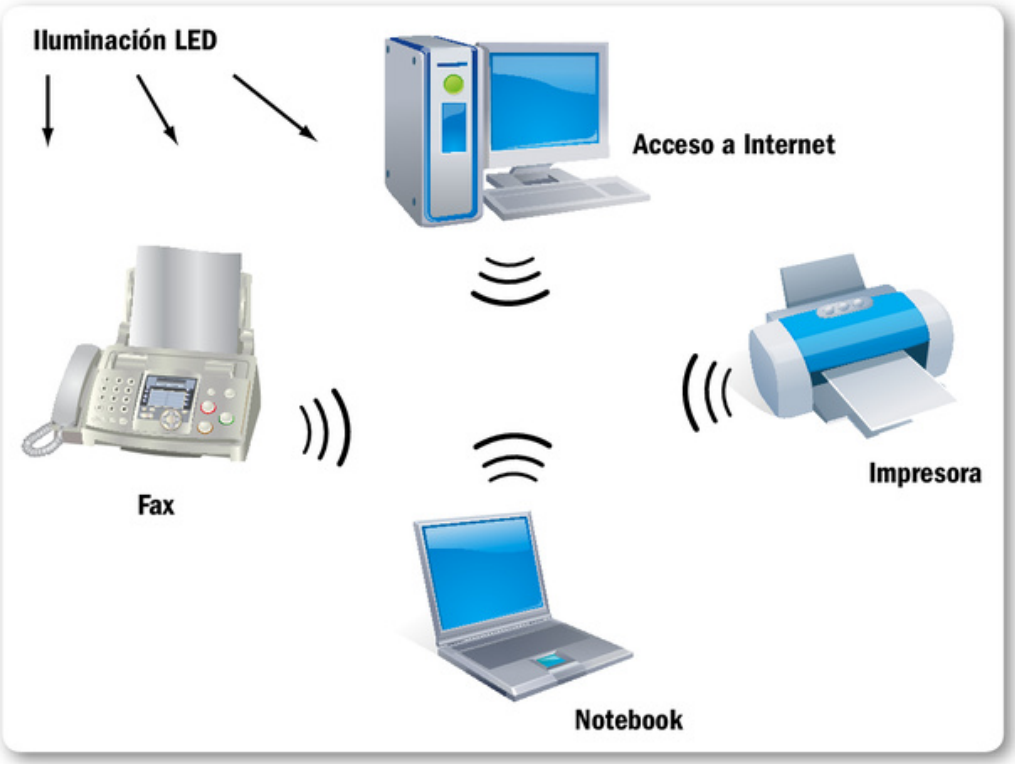


Figura 17. Poseer un estándar permite que diferentes artefactos en nuestros ámbitos interactúen y realicen funciones sin que haya problemas de compatibilidad entre ellos.

CONFUSIÓN DE NOMBRES

No solo es común confundir el conepto del término WiFi: se da otra confusión con Wireless LAN o WLAN, que es la denominación usada para redes de área local inalámbrica, en las que se emplean ondas de radio para comunicarse entre usuarios conectados. De esta forma, podemos notar que Wireless LAN se utiliza como un nombre alternativo del estándar IEEE 802.11.

En el campo de las telecomunicaciones, el **Instituto de Ingenieros Eléctricos y Electrónicos** (**IEEE** por sus siglas en inglés) es líder en la promoción de estándares internacionales.

Los estándares para redes LAN/MAN son unos de los productos más conocidos, en los que se incluyen el de redes cableadas (Ethernet **IEEE 802.3**) y el de redes inalámbricas (**IEEE 802.11**).



Figura 18. El logo del Instituto de Ingenieros Eléctricos y Electrónicos certifica la calidad en productos del mercado.

IEEE 802.11 también recibe el nombre de **WiFi** y hace referencia a los sistemas DSSS operando a 1, 2, 5.5 y 11 Mbps, donde todos cumplen con la norma de forma retrospectiva (o sea, ofrecen compatibilidad con productos anteriores). Tener esta **compatibilidad hacia atrás** es importante, ya que nos permite actualizar la red sin necesidad de cambiar nada.

Luego, en la IEEE 802.11a abarcamos los dispositivos WLAN que operan en la banda de 5 GHz; por lo tanto, no se permite la interoperabilidad con dispositivos funcionando a 2,4 GHz, como los de 802.11b.

Una nueva enmienda llamada IEEE 802.11g nos ofrece compatibilidad hacia atrás para dispositivos 802.11b utilizando una tecnología de modulación llamada **multiplexión por división de frecuencia ortogonal** (OFDM, por sus siglas en inglés) y, además, obtenemos la misma tasa de transferencia que 802.11a.

> LA COMPATIBILIDAD HACIA ATRÁS NOS PERMITE ACTUALIZAR LA RED SIN CAMBIAR DISPOSITIVOS



Figura 19. Podemos encontrar en cualquier café o espacio el famoso logo de WiFi, creado por la WiFi Alliance.

Mejoras de la IEEE 802.11

Muchas reformas fueron realizadas desde la original IEEE 802.11 que define nuestras redes inalámbricas. Veremos de manera resumida las mejoras en las enmiendas b, a, g, s y n. Existen muchas más que resumiremos con menos detalles en un cuadro.

802.11b

En comparación con el estándar original, se mejoró la tasa de transmisión, al elevarla hasta 11 Mbit/s (se lee mega bits por segundo).

Como dato extra, podemos decir que, inicialmente, se soporta hasta 32 usuarios por AP si utilizamos este estándar.

802.11a

Al igual que el estándar anterior, usamos la misma tecnología de base que el estándar original; la principal diferencia está en que operamos en la banda de 5 GHz usando OFDM, lo que nos permite una tasa de transmisión máxima de 54 Mbit/s.

La mayor velocidad de transmisión es una de las ventajas, así como la ausencia de interferencias en esta frecuencia de trabajo. Como desventaja podemos mencionar la incompatibilidad con 802.11b, ya que opera en diferente frecuencia.

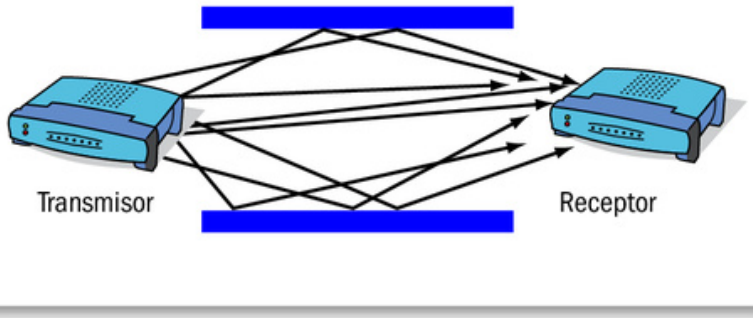


Figura 20. El concepto **MIMO** es aprovechar señales sin tratarlas como ruido, para tener la señal principal más fuerte.

802.11g

Funciona en la misma banda de 802.11b, lo que hace que exista compatibilidad con dispositivos trabajando bajo este estándar.

La tasa máxima de transferencia de datos es de 54 Mbit/s, ya que usamos la modulación OFDM.

Tenemos las mismas capacidades que en 802.11b y sumamos el incremento de la velocidad.

802.11s

Este es el estándar para redes malladas (Mesh), las cuales mezclan las topologías de redes ad hoc e infraestructura. La norma 802.11s trata de regular la interoperabilidad entre diferentes fabricantes en cuanto a este protocolo malla, ya que cada uno tiene su propios protocolos para la autoconfiguración de rutas entre AP.

TASA DE TRANSMISIÓN

Cuando reducimos la tasa de transmisión de datos, estamos logrando menor sensibilidad a la interferencia y atenuación, dado que utilizamos un método más redundante para codificar la información. De este modo, con tasas de 2 Mbit/s y 1 Mbit/s tendremos menor probabilidad de sufrir interferencias o pérdidas de datos.



Figura 21. Equipo que trabaja con el estándar **802.11n**, el cual se encuentra disponible en el mercado actual.

802.11n

Se nos presenta como la cuarta generación en los sistemas sin cables WiFi, compatible con estándares anteriores.

Trabaja en las frecuencias de 2,4 GHz y 5 GHz, y brinda una mejora importante respecto a estándares anteriores, que es el uso de varias antenas de transmisión y recepción.

Se trata de un concepto que es llamado MIMO (cuya sigla en inglés proviene de **Multiple Input, Multiple Output**), el cual se encarga de

TÉCNICAS DE CODIFICACIÓN

Utilizar diferentes técnicas de codificación de datos antes de transmitirlos hacia el destino significa lograr un incremento en el índice de tasa de transferencia de información. Este es el caso de 802.11b, en el que, al mismo tiempo, se transfiere mayor cantidad de datos.

aumentar significativamente la tasa de transferencia de datos y el alcance. Lo notable es que MIMO aprovecha lo que otros estándares consideran un obstáculo: la **multitrayectoria**.



Figura 22. Las placas inalámbricas internas también hacen uso de la tecnología **MIMO** en 802.11n.

RESUMEN

En conclusión, existen diferentes topologías que dependerán del objetivo que tenga la red. La topología define la distribución física y lógica en que se conectarán los nodos. Aprendimos que un estándar es de suma importancia para los fabricantes y para los consumidores, ya que nos asegura el correcto funcionamiento y la interoperabilidad entre productos del mercado. También vimos que seguir un estándar favorece el desarrollo y promueve la competencia entre empresas. Finalmente, comparamos y detallamos las características específicas de cada estándar de la IEEE 802.11x.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Cuál es el objetivo de armar una red?
2. ¿Qué trata de asegurar la ISO con el modelo OSI de 7 capas y qué se logra con esta división por capas?
3. ¿Cuál es la topología inalámbrica más usada?
4. ¿A qué tipo de red llamamos WLAN y en qué banda opera?
5. ¿Qué significa el término SSID y para qué sirve?
6. ¿Cuáles son los dos modos fundamentales de operación en los estándares 802.11?
7. ¿Cuál es la diferencia entre estándar abierto y cerrado?
8. ¿En qué banda funciona IEEE 802.11g y qué modulación utiliza?
9. ¿Cuándo se recomienda el uso de repetidores en los enlaces PtP?
10. ¿Por qué razón IEEE 802.11a es incompatible con IEEE 802.11b?

ACTIVIDADES PRÁCTICAS

1. Identifique cada una de las capas del modelo OSI.
2. Identifique la topología de red usada en una instalación física.
3. Identifique el SSID de su red.
4. Enumere algunos ejemplos de estándar abierto.
5. Mencione ejemplos de estándar cerrado.

*02

Hardware para redes inalámbricas

Ahora tenemos la oportunidad de ver en detalle cada una de las partes físicas necesarias para armar nuestra red inalámbrica. Esto nos permitirá comprender cómo se maneja el traspaso de información de un lugar a otro. Instalaremos el hardware, actualizaremos el firmware y aprenderemos cómo configurar los puntos de acceso.

- **Introducción al hardware inalámbrico 40**
- **Configuración de puntos de acceso 42**
  - Pautas generales para tener en cuenta 42
  - Instalar el hardware y actualizarlo 44
- **Configurar con el modelo OSI 49**
  - Capa Física 49
  - Capa de Enlace 52
  - Capa de Red 56
  - Capa de Aplicación 57
- **Resumen 57**
- **Actividades 58**

Introducción al hardware inalámbrico

Nuestras redes sin cables se basan en los mismos principios que usan los aparatos inalámbricos que tenemos en nuestras casas. Pensemos en teléfonos celulares, teléfonos inalámbricos, **radios AM** y **FM**, antenas de televisión satelital, entre otros. En todos ellos, un transceptor (que se define como la combinación de un transmisor y un receptor) envía señales emitiendo ondas electromagnéticas desde una antena y las propaga hasta llegar a destino; esta antena también recibe señales desde otro emisor. Si ambas antenas están calibradas en la frecuencia apropiada, se concreta la recepción de la información.



Figura 1. Un router inalámbrico que no realiza modificaciones en la información enviada funciona como punto de acceso para nuestra red.

Tengamos en cuenta que, básicamente, necesitamos de dos partes de hardware para conformar cualquier red inalámbrica: por un lado, un punto de acceso; y por el otro, un adaptador de red.



Figura 2. Los usuarios que desean utilizar nuestra red inalámbrica deben contar con un adaptador de red en su computadora.

Los dispositivos que posibilitan el acceso a nuestra red se llaman **estaciones inalámbricas**. Estos pueden ser configurados como **puntos de acceso** o como **clientes inalámbricos** de la red.

Siempre es importante separar el procedimiento en diferentes pasos cuando deseamos realizar la instalación de los clientes para una red. En general, podemos decir que estos pasos son:

1. Elección del hardware que vamos a usar
2. Instalación
3. Configuración

Como sabemos, estos pasos se aplican para cualquier sistema operativo con el que trabajemos. En nuestro caso usaremos MS Windows 7, así es que no tendremos mayores problemas en las etapas 1 y 2 (lo mismo sucederá con cualquier versión de MS Windows). Si el sistema operativo fuese una distribución Linux (Open Source o diferente de Microsoft Windows), no será tan sencillo, y estos dos primeros pasos requerirán mucha atención del administrador de red.

Configuración de puntos de acceso

Siempre que vayamos a configurar cualquier dispositivo, es recomendable seguir ciertas directivas o pautas que nos permitirán trabajar de forma ordenada y sistemática. De esta manera, si fuese necesario verificar algún paso por motivo de un error o problema, será algo muy fácil de realizar.

Pautas generales para tener en cuenta

- Tener el manual del **punto de acceso** a mano y leerlo antes para conocer el dispositivo y la configuración que trae por defecto.
- Mirar y estudiar dónde se ubicará el punto de acceso una vez finalizada la configuración, ya que las condiciones del lugar físico donde será instalado son importantes. Corroborar si hay donde conectar la fuente de alimentación, la temperatura del lugar y la humedad del ambiente, entre otros factores.
- Hacer un dibujo de la red (TCP/IP), el cual servirá como un plano con las indicaciones para seguir. Con esto lograremos identificar la topología usada en la red. Debemos incluir la mayor cantidad de información posible, desde los datos de nuestro proveedor de Internet (ISP) hasta, en caso de tener, los de la red cableada (LAN), tratando de ser lo más específicos posible.
- Si estamos consultando material en alguna página web, es importante bajarlo para tenerlo en caso de que nuestra conexión sufra algún problema. Descarguemos todo de modo de poder trabajar aun sin tener conexión a Internet.

MÉTODOS PARA TELECOMUNICARSE

Los primeros métodos para comunicarse a distancia eran muy primitivos. Desde el empleo de **runners** (personas que corrían largas distancias para llevar el mensaje), palomas mensajeras, señales de humo (usadas por los indios norteamericanos), espejos (que reflejan la luz del sol), hasta el invento del telégrafo. Este último marcó el inicio de lo que hoy conocemos como telecomunicaciones.

- Recomendamos tener papel y lápiz a mano para tomar nota de cada paso que realicemos; esto será muy útil cuando tengamos que cambiar direcciones IP, contraseñas, opciones de red, etc.
- Siempre verificar que tengamos todo el hardware necesario para nuestra red (computadora, tarjeta de red y cables de red, en caso de ser necesarios, entre otros elementos).

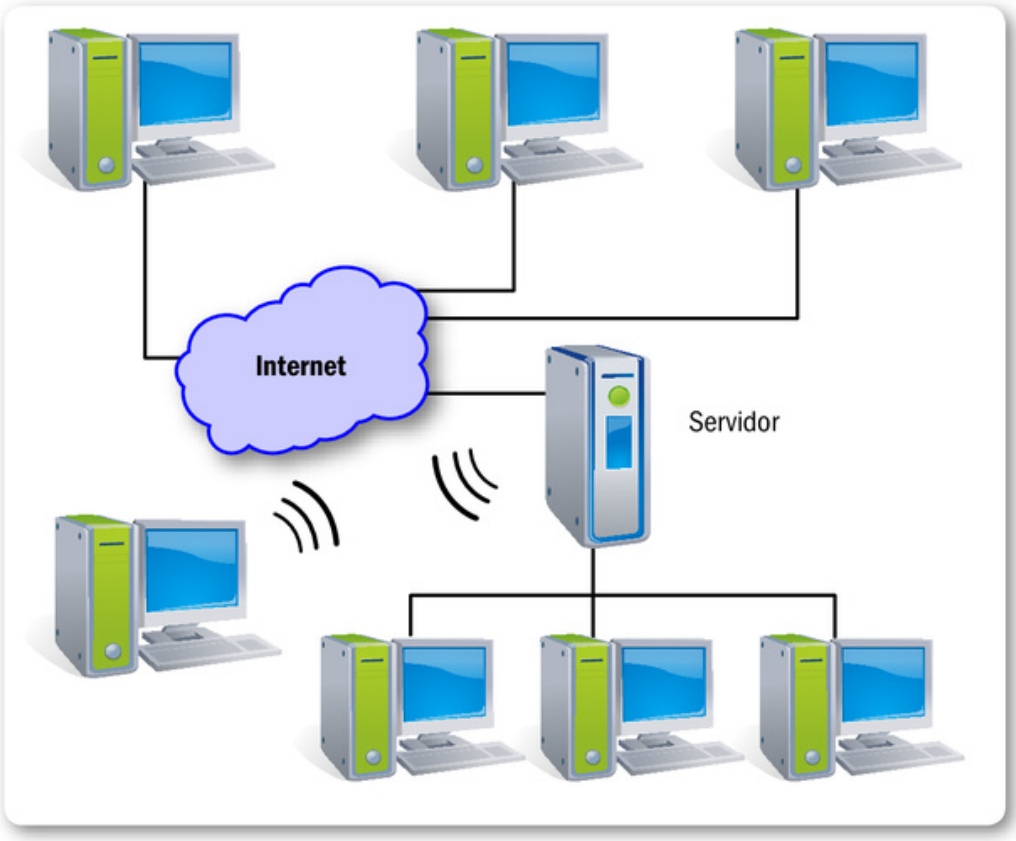


Figura 3. Tener un diagrama de la red nos permite hacer cambios de última hora antes de iniciar las configuraciones.

ANTENAS INTELIGENTES

Las antenas poseen una característica llamada patrón de radiación, que representa de forma gráfica cómo una antena irradia energía. Este parámetro es fijo, pero existen **antenas inteligentes** que tienen un patrón de radiación dinámico. Esta característica es interesante ya que ayuda a solucionar problemas en los sistemas de comunicaciones que cambian por factores como el clima.

- Por último, debemos tener el software necesario para instalar nuestra placa de red inalámbrica (drivers), actualizaciones de firmware, etc. A esto le podemos sumar algún programa para verificar/medir las señales inalámbricas. Ejemplos de estos programas son Netstumbler, inSSIDer o Xirrus WiFi Inspector.

Instalar el hardware y actualizarlo

Iniciamos la tarea instalando la parte física de la red, el **hardware**. Vamos a conectar el punto de acceso a nuestra computadora y actualizaremos el **firmware** (esto es opcional). En un principio, el firmware existía en el límite entre el hardware y el software (el término hace referencia al software firme, fijo o sólido). Se define como un software compuesto por un bloque de instrucciones con un fin específico, y que se almacena y ejecuta desde la memoria del dispositivo. Está integrado en la parte del hardware; así, podemos decir que el firmware es hardware y software al mismo tiempo.

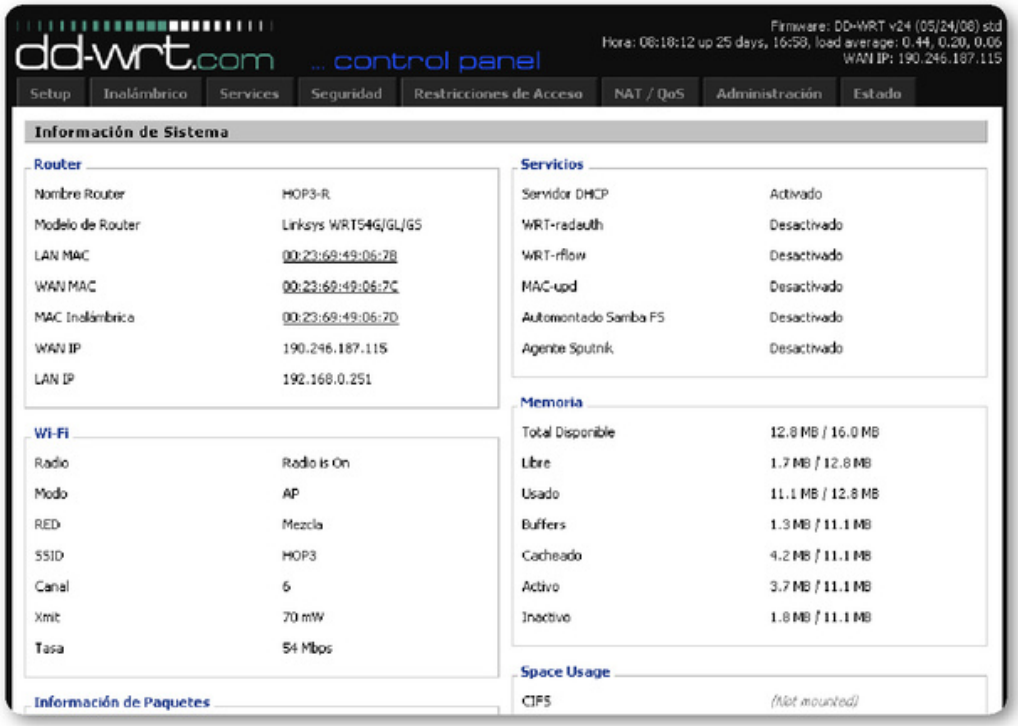


Figura 4. Algunas distribuciones de firmware creadas por terceros nos permiten tener un mayor número de opciones de configuración.

La finalidad del firmware es ejercer el control de las operaciones que se van a realizar; estas instrucciones se incluyen en la memoria ROM del dispositivo desde su fabricación.

Instalar el dispositivo físicamente

Siempre debemos prestar atención a dos partes bien diferenciadas en un punto de acceso:

1. Las **luces** o **LEDs** (diodos emisores de luz) que posee en el frente y nos indican el estado.
2. Las interfaces de conexión Ethernet e inalámbrica.



Figura 5. En caso de un problema, lo primero que verificaremos será el estado de los LEDs del punto de acceso inalámbrico.

Como dijimos, los LEDs de estado se encuentran en la parte frontal del punto de acceso y nos indican, con una luz fija o intermitente (en general, de color verde), información sobre algunos de los siguientes parámetros:

1. Alimentación de energía eléctrica conectada o no del dispositivo.
2. Puertos conectados y/o activos.
3. Datos enviados y/o recibidos.
4. Conexión a la red cableada (puertos Ethernet).
5. Conexión a la red inalámbrica (WLAN).
6. Acceso a Internet.

LOS LEDS DE ESTADO NOS INDICAN DIVERSOS PARÁMETROS DEL DISPOSITIVO



Figura 6. La gran mayoría de los dispositivos en el mercado tienen uno o más **puertos Ethernet** en su parte posterior.

Sumado a lo anterior, identificamos que nuestro punto de acceso posee una o más antenas. Las podemos encontrar en el exterior o dentro del aparato fijadas a la tapa superior.

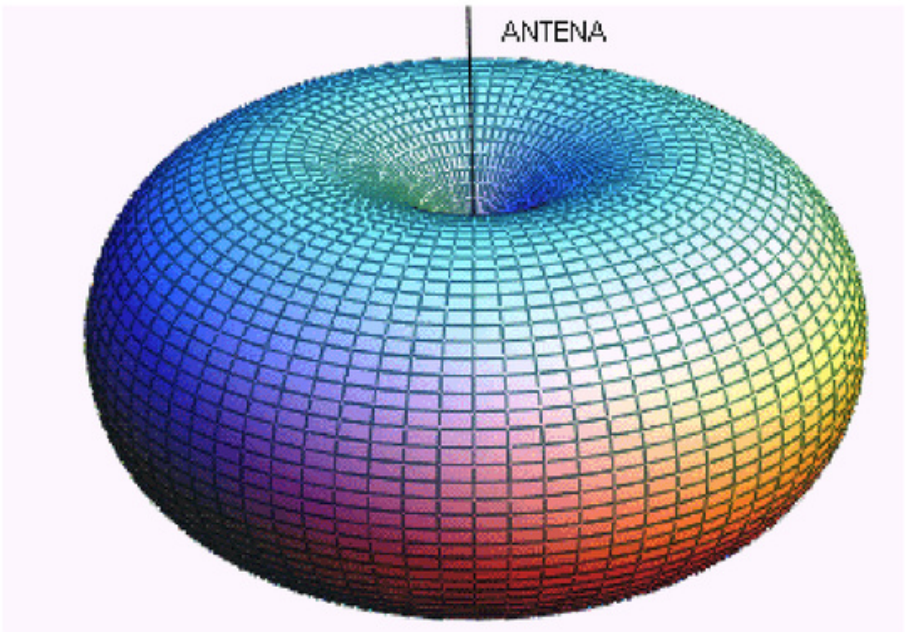


Figura 7. El diagrama de radiación de una antena es una representación de la energía producida junto con su dirección.

Configurar el punto de acceso desde la PC

Ahora es el momento de conectarnos al punto de acceso desde nuestra computadora portátil o de escritorio y configurar la red. Se puede realizar este vínculo usando una conexión por cable o de forma inalámbrica. Para efectuar la conexión por cable, usaremos un cable UTP (que generalmente viene con el dispositivo), mientras que en el otro caso no hace falta nada. Siempre es mejor hacer la primera configuración usando el cable y, luego, cuando tengamos todos los parámetros básicos de la red configurados, cambiar y usar la conexión inalámbrica para administrar o modificar configuraciones.

> ES RECOMENDABLE REALIZAR LA PRIMERA CONFIGURACIÓN UTILIZANDO UN CABLE UTP

Lo más fácil y común es conectarse usando un cable Ethernet junto con el **protocolo HTTP**; así, solamente será necesario un **navegador web** (por ejemplo, Mozilla o Internet Explorer).



Figura 8. El cable Ethernet usado para conectarnos se llama patch cord, y consta de un cable UTP y conectores RJ-45 en cada uno de sus extremos.



Figura 9. Si nuestro dispositivo permite conexión serie, usaremos un cable con una ficha RJ-45 y uno o dos DB9 o DB25.

Una vez que ingresemos en la configuración del punto de acceso desde el navegador, veremos la interfaz de usuario. Las interfaces varían según fabricantes y modelos, pero son similares.

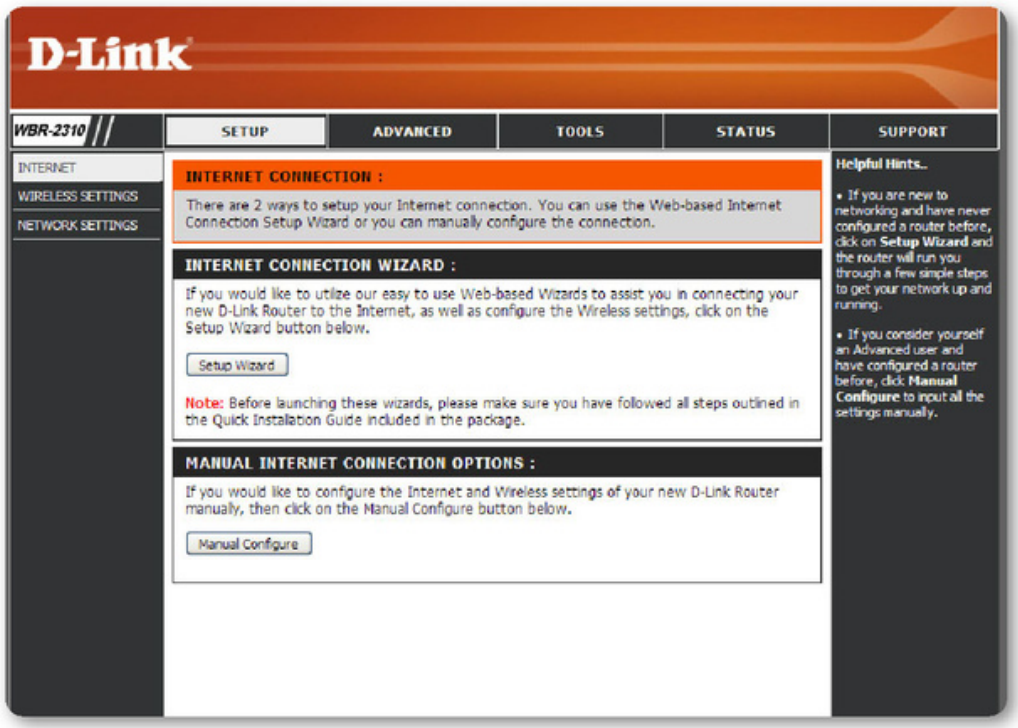


Figura 10. La interfaz de los dispositivos D-Link que tenemos al usar el protocolo HTTP muestra un menú prolijo y posee ayuda para el usuario.

Configurar con el modelo OSI

Suele ser difícil para una persona con poca o nada de experiencia tratar de entender o distinguir cuáles son las opciones básicas y avanzadas en los manuales de estos dispositivos (muchos poseen gran cantidad de hojas). Por este motivo, es común que nos asustemos ante tanta cantidad de opciones para configurar en un principio.

Veremos ahora una aproximación teórica a la configuración necesaria del hardware en la que seguiremos el modelo OSI descripto en el primer capítulo. Necesitamos ver qué función realiza cada uno de los parámetros que configuraremos y por qué son necesarios, para tener plena seguridad al momento de implementar la red.

Capa Física

Algunos de los parámetros básicos que se ven afectados en un punto de acceso a la hora de configurar son: el número de canal, la potencia de transmisión y la tasa de velocidad de transmisión. Pasaremos a detallar cada uno de ellos para tener una idea general.

Número de canal

Seleccionar el canal que vamos a utilizar implica fijar la gama de frecuencias en que operará el dispositivo. Estas frecuencias se especifican en GHz (**gigahercio**). Se recomienda tener conocimiento de las frecuencias que están siendo usadas en las cercanías del lugar donde se va a implementar la red inalámbrica.



HOMERF, COMPETENCIA DE WIFI

HomeRF fue un estándar desarrollado por un grupo industrial que prometía competir con WiFi. El desarrollo se basó en el del teléfono inalámbrico digital mejorado (DECT, por sus siglas en inglés), similar al estándar de la telefonía celular (GSM). Se pretendía diseñar un dispositivo central en cada casa, que vinculara los teléfonos y proporcionara mayor ancho de banda.

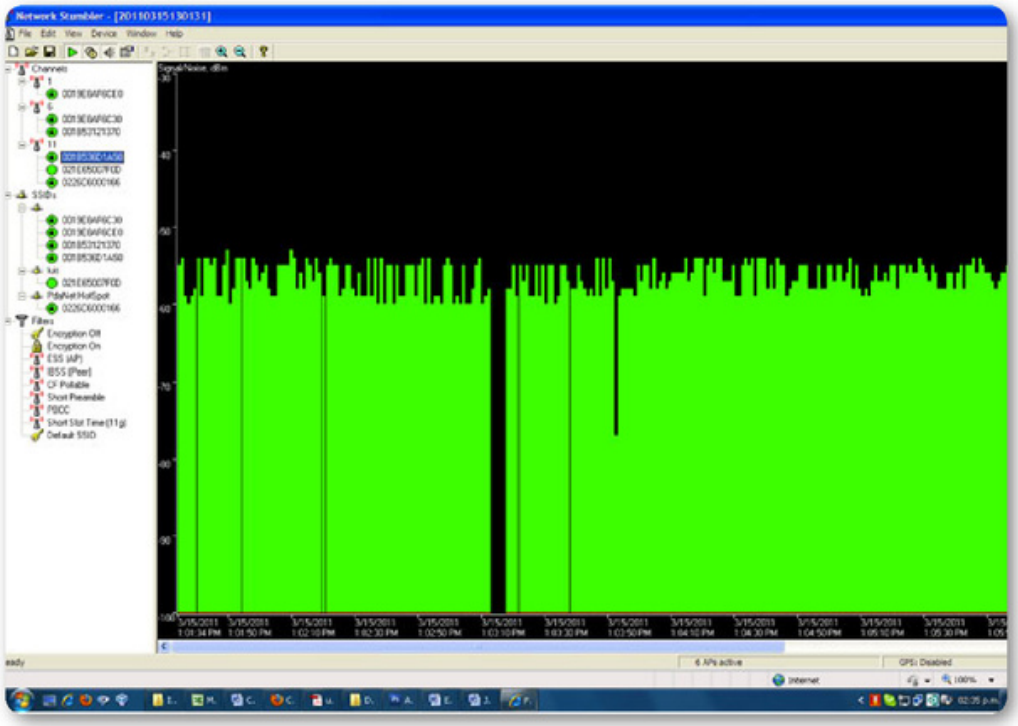


Figura 11. Al seleccionar un canal o SSID específico, Netstumbler nos muestra un gráfico del tráfico de datos en tiempo real.

Como información adicional a lo visto en el capítulo anterior, si usamos la norma **IEEE 802.11b**, es recomendable utilizar los canales 1, 6 u 11 para así poder asegurar que exista suficiente separación de frecuencias entre los canales y evitar cualquier conflicto. Esto es solo una recomendación, ya que podemos seleccionar cualquier canal.

En cambio, para la norma **IEEE 802.11a** no se corre ningún riesgo de superposición de canales; solo se debe tener la certeza de que otros puntos de acceso cercanos que usen esta misma norma operen en canales diferentes del que usamos nosotros.

WEP Y WPA/WPA2

Las configuraciones WEP y WPA/WPA2 realizadas en el punto de acceso siempre se deben reflejar en el lado del cliente. Debemos verificar que el dispositivo cliente soporte WEP, WPA o WPA2 según corresponda, el tipo de autenticación y la longitud de la clave que hemos configurado en el punto de acceso.



Figura 12. Al seleccionar el canal que vamos a utilizar, vemos que se especifica la frecuencia en GHz, además del número de canal.

Potencia de transmisión

Es verdad que, cuanto mayor sea la potencia de transmisión de nuestro punto de acceso, mayor será su rango de cobertura. De esta forma, si configuramos la potencia de transmisión con el parámetro máximo permitido, vamos a obtener la mayor cobertura posible.

Hay que tener en cuenta que en algunos países esto está regulado y existen valores máximos permitidos; en ciertas zonas, es 100 mW (20 dBm) y en otras, como rn EE.UU. o Canadá, el límite es 1 W.

Tasa de transmisión

Debemos tener presente que la gran mayoría de los puntos de acceso que encontramos en el mercado poseen la opción para cambiar a nuestro gusto la tasa de **transmisión** deseada.

ACCESS POINT EN LA PC

Los AP no necesariamente deben ser un dispositivo separado. Existe software para diferentes sistemas operativos que nos permiten transformar una PC con una placa de red inalámbrica en un AP operado por software. Una ventaja es que no gastamos en hardware y reutilizamos una computadora que, quizás, estaba olvidada. Quienes estén interesados en el tema pueden leer más en **www.zeroshell.net**.



Figura 13. Si vemos las configuraciones avanzadas del dispositivo, encontraremos opciones más específicas.

Capa de Enlace

En la Capa de Enlace veremos los siguientes parámetros: Modos de operación, SSID, Control de acceso al medio, Filtrado MAC, Encriptación (WEP, WPA) y WDS.

Modos de operación

En este punto es importante aclarar a qué hace referencia el modo de **un punto de acceso**, ya que muchas veces se puede confundir con los dos modos básicos **de radio** en que puede configurarse cualquier placa inalámbrica conectada a la computadora (que son los tan nombrados modos infraestructura y ad hoc).

En un punto de acceso, el modo se refiere al tipo de tareas que este realiza. Muchos fabricantes cambian los nombres para identificar esta opción, por lo que debemos prestar mucha atención.

OVERCLOCKING DE POTENCIA

Muchas veces podemos aumentar la potencia de salida de un dispositivo para lograr mayor alcance mediante algún software, pero, generalmente, esto incrementa la interferencia producida en los canales adyacentes y deteriora el espectro transmitido. Por eso no es aconsejable realizarlo.



Figura 14. Vemos en la figura un router con firmware dd-wrt desarrollado por programadores independientes.

SSID (Service Set Identifier)

El **SSID** es el nombre que asignamos a nuestra red LAN inalámbrica, el cual también se incluye en todos los paquetes **baliza** (**beacon** en inglés) que envía el punto de acceso. Una baliza es un paquete de información que se manda desde un dispositivo conectado a todos los demás, para anunciar su disponibilidad. Un intervalo de baliza es el período de tiempo (enviado con la baliza) que debe transcurrir antes de que se vuelva a enviar la baliza. El intervalo de baliza puede ajustarse en términos de milisegundos (ms).

Control de acceso al medio

Existen opciones avanzadas que pueden ser útiles cuando nuestra red está congestionada, es decir, con mucho tráfico de datos. Vamos a ver algunos parámetros, como intervalos de **beacon** y fragmentación.

- **Intervalo de beacon**: se define como la cantidad de tiempo que existe entre la transmisión de un **beacon** y otro en un punto de acceso. Por defecto, se usa generalmente 10 ms (milisegundos); así, en cada segundo se envían 10 beacons. Si nos estamos moviendo dentro de casa, con estos beacons tendremos conocimiento sobre la existencia del punto de acceso sin ningún problema. Este valor se puede modificar, pero no es recomendable hacerlo, salvo que tengamos conocimientos avanzados y una buena razón para esto.

- **Fragmentación**: nuestro estándar IEEE 802.11 posee una característica opcional que permite a las placas de red inalámbricas y los puntos de acceso fragmentar los datos enviados en pequeñas piezas para tratar de mejorar el rendimiento cuando existen interferencias. El valor de **fragmentación** normalmente está entre 256 y 2048 bytes, y puede ser modificado por el usuario.

Filtrado MAC

Llamamos dirección **MAC** (**Media Access Control**, en español: control de acceso al medio) a un identificador de 48 bits que está grabado en las placas de red (en todas) y que identifica físicamente a nuestra placa. Este valor viene establecido de fábrica, y cada dirección **MAC** es diferente según el fabricante.

De esta forma, el filtrado MAC significa que solo un grupo limitado de direcciones MAC conocidas por nosotros pueden conectarse al punto de acceso. Es una medida de seguridad bastante débil, pero la podemos usar combinada con otras un poco más avanzadas.

Encriptación (WEP, WPA)

Un antiguo protocolo de encriptación llamado **WEP** (**Wired Equivalent Privacy**, o privacidad equivalente a la cableada) se emplea en la mayoría de los puntos de acceso. Aunque este mecanismo de encriptación (o cifrado de datos) posee grandes falencias y muchos no lo consideran como una opción segura para proteger sus datos, es común que un usuario con conocimientos intermedios lo use.

> WEB, UN ANTIGUO PROTOCOLO DE ENCRIPTACIÓN, SE USA AÚN EN PUNTOS DE ACCESO

Cuando habilitamos WEP, debemos borrar las claves que provee el fabricante por defecto e ingresar las nuestras propias.

Existen alternativas al protocolo WEP, y una es **WPA** (**Wi-Fi Protected Access**, o acceso protegido Wi-Fi), el cual es un protocolo de encriptación que fue diseñado para corregir las deficiencias del sistema WEP. Además, debemos saber que existe una segunda generación llamada WPA2, que se basa en el estándar 802.11i y que es la versión certificada del estándar de la IEEE.

WDS (Wireless Distribution System)

Un **sistema de distribución inalámbrica** o **WDS** es un sistema que permite la conexión inalámbrica entre puntos de acceso en una red IEEE 802.11. De esta forma, la red inalámbrica puede ser ampliada mediante múltiples puntos de acceso sin necesidad de un cable que los vincule. Esto se realiza haciendo el puenteo a nivel de la Capa 2 del modelo OSI entre todas las estaciones registradas (clientes) en los puntos de acceso que están conectados mediante WDS.

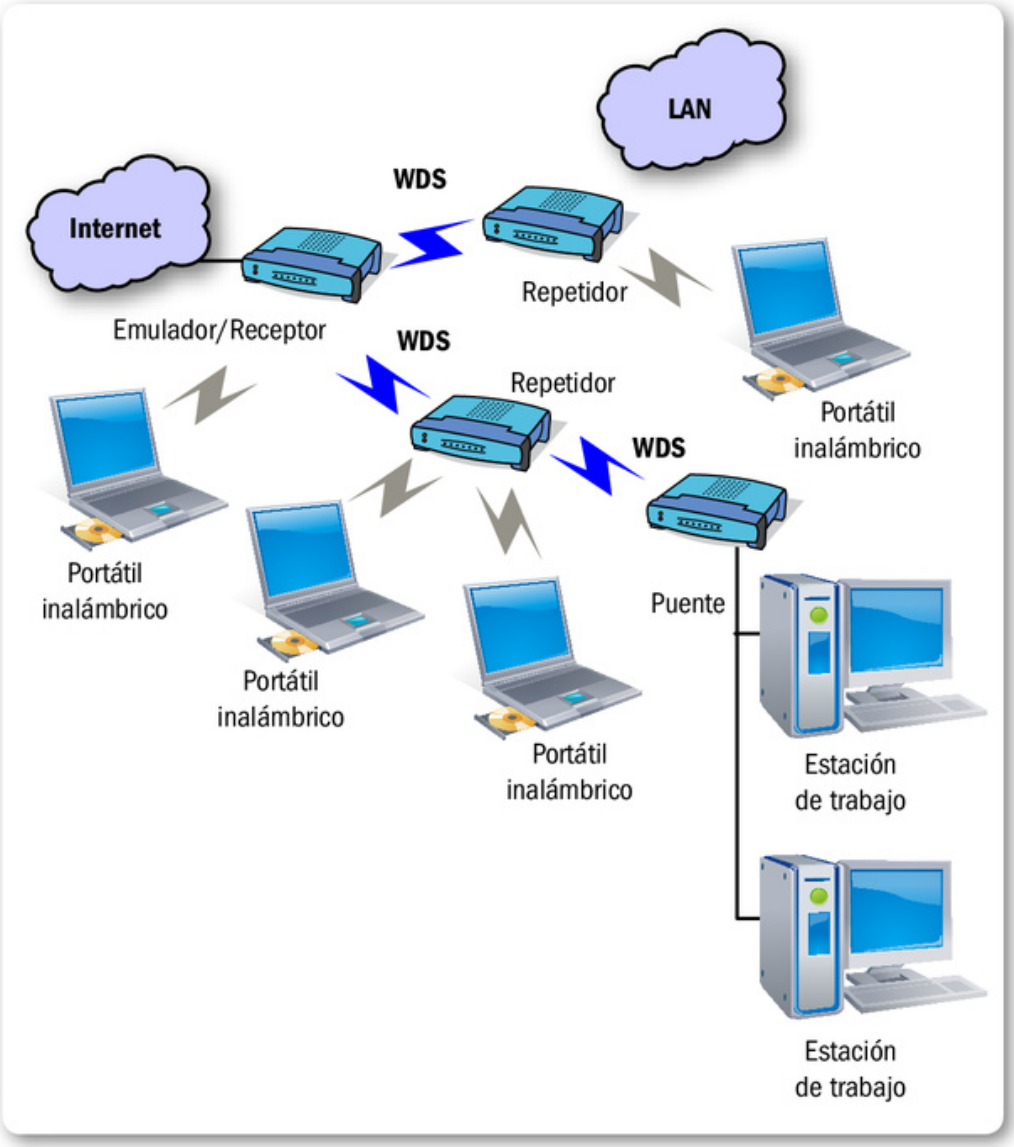


Figura 15. En esta imagen podemos ver un esquema de implementación del sistema denominado WDS.

Capa de Red

Estrictamente hablando, la **capa de red** no es parte de las redes inalámbricas de comunicación. Sin embargo, algunos puntos de acceso no son transparentes y tienen funciones extra, como enrutamiento y enmascaramiento (NAT).

En la tabla siguiente vemos cada uno de los parámetros que juegan un papel importante en la capa de red:

▼ PARÁMETRO	▼ DESCRIPCIÓN
Dirección IP	Configurar la dirección IP en un punto de acceso no es necesario para realizar sus tareas básicas (es decir, ser un concentrador inalámbrico). La usamos para ingresar al dispositivo desde una aplicación web, y poder configurar el equipo de forma rápida y fácil. Tendremos que configurar de forma apropiada la dirección IP si usamos el punto de acceso como enrutador inalámbrico, ya que esta debería estar en la misma subred del enrutador al que está unida, y fijar las reglas apropiadas de enrutamiento (lo veremos más adelante).
Máscara de red	Comúnmente llamada en inglés Netmask. Es una combinación de bits que sirve para poder delimitar el ámbito de una red. Tiene como función indicar a todos los dispositivos qué parte de la dirección IP es el identificador de red, incluyendo la subred, y qué parte pertenece al dispositivo.
Gateway	También podemos encontrarlo mencionado como pasarela. Es la dirección IP correspondiente a la conexión de salida de su red.
DNS	Domain Name System o DNS (en español, sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras conectadas a Internet o LAN. La función principal es traducir nombres inteligibles para los humanos (como una dirección de una página web, por ejemplo, www.redusers.com) en identificadores binarios. Estos identificadores se vinculan a equipos conectados a la red para así poder localizarlos y direccionarlos mundialmente. Es una base de datos que almacena esta información. Debemos usar la dirección IP del servidor de DNS que se informará usando DHCP a todos los clientes inalámbricos conectados.

Tabla 1. Vemos las opciones que debemos tener en cuenta en un punto de acceso relacionado a la capa de red.

Capa de Aplicación

Nuestro punto de acceso viene con una contraseña por defecto que protege las configuraciones del dispositivo cuando intentamos ingresar a través de la Web. Esta contraseña de administrador que viene en la configuración original es normalmente la misma (usuario: admin y contraseña: admin.), por lo que se recomienda cambiarla inmediatamente por otra que sea más segura.

Debemos evitar usar **contraseñas** que se relacionen directamente con datos nuestros (DNI, número de teléfono, fechas de nacimiento, etc.), porque se pueden deducir fácilmente y estaríamos exponiendo nuestra configuración. Si alguien sin autorización accede a nuestro punto de acceso, tendrá total control sobre las configuraciones, y sin problemas podrá cambiar la contraseña de administrador y, de esa forma, dejarnos sin acceso a nuestro equipo inalámbrico. La única solución para esto es resetear manualmente el punto de acceso, o usar el puerto serie para conectarse sin necesidad de contraseña y tomar el control del equipo (esto último, si nuestro dispositivo posee ese puerto serie).

Consideramos que los ajustes más importantes del proceso de configuración se encuentran en la Capa de Aplicación.

RESUMEN

Según lo visto en este capítulo, concluimos que, cuando necesitamos instalar un punto de acceso o router inalámbrico, es necesario que identifiquemos el hardware que vamos a utilizar y conozcamos qué tipo de red queremos implementar. Aquí conocimos parámetros como el SSID, la velocidad de transmisión y la potencia de transmisión vinculados a la Capa Física. En la Capa de Enlace, consideramos el método de encriptación o el control de acceso MAC para la seguridad básica de nuestra red. Por último, definimos parámetros de la Capa de Red, como NAT o DHCP, para adicionar funcionalidades de red a nuestro punto de acceso, siempre y cuando este lo permita.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué es un transceptor y qué funciones cumple?
2. ¿Cómo pueden ser configuradas las estaciones inalámbricas?
3. ¿Cuál es la finalidad del firmware que viene grabado en la memoria no volátil de ciertos dispositivos electrónicos?
4. ¿Cuál es la utilidad del puerto WAN que se encuentra en la parte trasera de los puntos de acceso?
5. ¿Cómo logramos una recepción óptima con antenas externas a nuestro equipo?
6. Describa los pasos necesarios para realizar una copia de seguridad de su configuración actual en el punto de acceso.
7. ¿Con qué cables puede hacer la conexión de un punto de acceso con su computadora?
8. ¿Cuál es la IP, nombre de usuario y contraseña que vienen por defecto en la gran mayoría de los puntos de acceso?
9. ¿Qué función cumple el SSID en una red inalámbrica?
10. ¿Qué valor se modifica en nuestro punto de acceso según la técnica de modulación empleada para transmitir datos?

ACTIVIDADES PRÁCTICAS

1. Conecte su punto de acceso a la alimentación y trate de verificar el estado de los LEDs siguiendo el manual.
2. Use el software NetStumbler o inSSIDer para monitorear señales inalámbricas, e identifique las opciones básicas y avanzadas.
3. Realice el proceso completo de copia de seguridad de su configuración del punto de acceso.
4. Ingrese a la configuración de su punto de acceso, y modifique el usuario y contraseña que tiene por defecto.
5. Ingrese a la interfaz web de su punto de acceso y reconozca los parámetros que desarrollamos en las diferentes páginas sobre configuración.

*03

Configuración en Windows

En este capítulo nos introduciremos directamente en la configuración de nuestra red utilizando una computadora de escritorio o portátil con el sistema operativo Windows 7 y los dispositivos que describimos en capítulos previos.

- **Instalar clientes en Windows... 60**
- **¿Qué hardware utilizar? 61**
  Instalar el hardware es fácil 62
- **Configurar el hardware en Windows 65**
  Configurar la red inalámbrica 79
  Configuración de red inalámbrica modo Infraestructura 87
- **Resumen 91**
- **Actividades 92**

Instalar clientes en Windows

En general, la instalación de clientes bajo el sistema operativo Windows es un proceso que no presenta dificultades. De todas formas, necesitamos poner especial atención a ciertas situaciones que pueden causar problemas o conflictos.

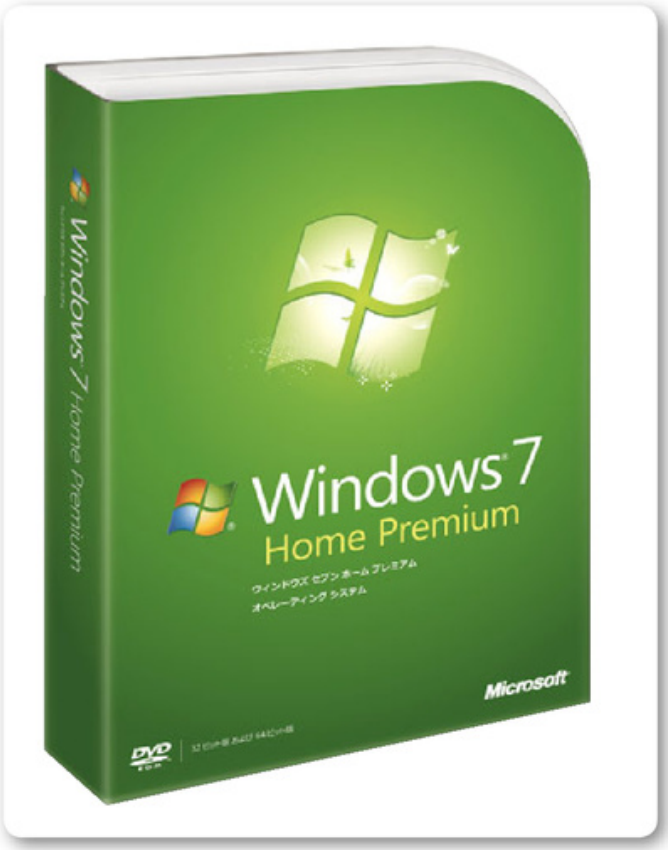


Figura 1. El último sistema operativo de Microsoft que presenta buenas prestaciones para el usuario se llama Windows 7.

- Muchas computadoras portátiles poseen un botón para encender o apagar nuestra interfaz inalámbrica. Esta posibilidad de cambiar de encendida a apagada (lo encontramos como **on/off** en muchos casos) es desconocida por parte de nuevos usuarios de equipos portátiles, y si la interfaz permanece apagada, no será posible realizar la conexión a la red. Tenemos que asegurarnos de que, al momento de iniciar las configuraciones del dispositivo, la interfaz se encuentre encendida (**on**).
- Las placas inalámbricas que instalaremos, en general, traen una herramienta de gestión de configuración, mientras que nuestro

sistema operativo Windows también tiene su propio gestor. En caso de que ambos programas estén activos, se ocasionará un conflicto que puede causarnos algún inconveniente. Para evitarlo, seleccionaremos solo un gestor de configuración y desactivaremos el otro. Recomendamos usar el gestor que provee MS Windows.

PARA EVITAR CONFLICTOS, DEBEMOS ACTIVAR SOLO UN GESTOR DE CONFIGURACIÓN

¿Qué hardware utilizar?

Windows lidera el mercado en materia de sistemas operativos para usuarios hogareños, aquellos que no poseen mucha experiencia o quienes necesiten una plataforma fácil de instalar y que funcione de manera estable. Las últimas versiones de Microsoft Windows que se encuentran presentes en el mercado cumplen con estas condiciones indispensables para este tipo de usuario.

Necesitaremos, entonces, seleccionar un hardware que sea soportado por Windows. Esta tarea no presenta dificultades, ya que la mayoría de los fabricantes (por no decir todos) dan soporte de sus productos para Windows. Así, podrá utilizarse cualquier hardware.

Deberemos prestar especial atención a que los parámetros de la placa de red inalámbrica se adapten a lo que nosotros precisamos. Tendremos que considerar, por ejemplo, parámetros como la sensibilidad del dispositivo, la potencia de salida y la posibilidad de conectar una antena externa en caso de que utilicemos una placa de red externa para nuestra computadora.

INSTALLSHIELD COMO HERRAMIENTA

Para crear instaladores de programas que nosotros desarrollamos, podemos usar InstallShield, una herramienta de software creada por la empresa Stirling Technologies, que luego se llamó InstallShield Corporation. Se usa para software de escritorio, pero también es útil para administrar aplicaciones y programas en dispositivos móviles y portátiles.

Instalar el hardware es fácil

Cuando instalamos nuestro hardware, siempre es necesario tener los **drivers** (controladores) en el sistema operativo correctamente configurados. Los drivers son programas que permiten que el sistema controle un dispositivo de hardware. De esta forma, la interacción entre el dispositivo nuevo (placa de red inalámbrica) y el sistema operativo se realiza sin conflictos. Nosotros que estamos usando Windows 7 no vamos a tener mayores problemas, dado que esta nueva versión tiene soporte para gran cantidad de dispositivos. En caso de usar alguna versión anterior (Windows 98, Windows 2000 o Windows XP, por ejemplo) o algún dispositivo viejo, se puede requerir un poco más de esfuerzo en la instalación.

Debemos saber que hay varias maneras de instalar un driver, dependiendo de la manera en que se distribuye (muchas veces contamos con un CD con los archivos que nos provee el fabricante o podemos buscarlo en Internet) y de que su instalación implique, a su vez, la instalación de programas adicionales.

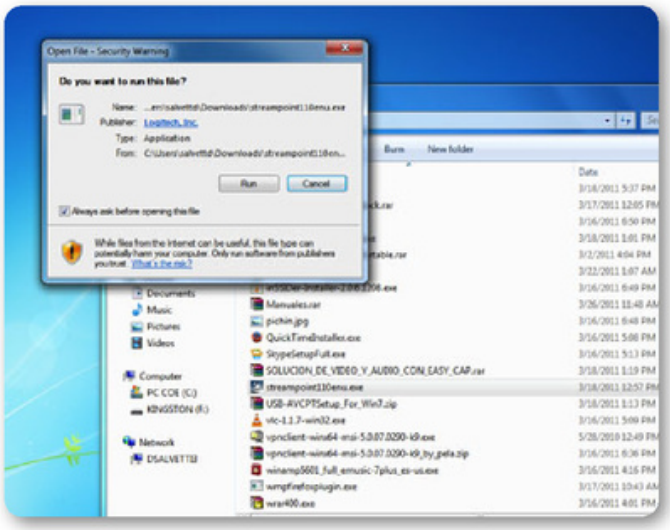


Figura 2. Cuando instalamos un driver, se presenta una ventana donde se nos pregunta si queremos ejecutar el programa.

Tenemos una tercera opción para instalar los drivers sin necesidad de cargarlos. Una vez detectado el dispositivo por el sistema P&P, vamos al Administrador de dispositivos, que identificará el elemento que no tiene driver (en general, lo marca con una señal amarilla de precaución). Luego veremos las características del dispositivo al hacer clic con el botón derecho sobre su nombre y seleccionar **Propiedades**.

Si vamos a la pestaña **Controlador** (o driver) podemos pulsar en **Actualizar Controlador**. En este punto es posible seleccionar una instalación automática, en la que el propio sistema trata de localizar e instalar el driver; o podemos hacerlo de forma manual, buscando nosotros mismos la ubicación del controlador.

EN LA PESTAÑA CONTROLADOR PODEMOS ACTUALIZAR LOS DRIVERS INSTALADOS

Hay que prestar atención a nuestros drivers. Es preciso verificar la existencia de un archivo **.INI** en el directorio donde tenemos todos los archivos correspondientes a los drivers. El archivo con extensión **.INI** contiene información que permite al sistema reconocer el driver como el necesario para el correcto funcionamiento del dispositivo.

En todos los casos, cualquiera sea el sistema de instalación de drivers que usemos, es muy importante hacer algo que nadie suele hacer de manera previa a instalar un dispositivo: leer los manuales de instalación de lo que vamos a instalar.

Cuando conectamos una tarjeta PCMCIA o USB, Windows 7 automáticamente detectará el nuevo dispositivo conectado y buscará el driver apropiado para que funcione correctamente.

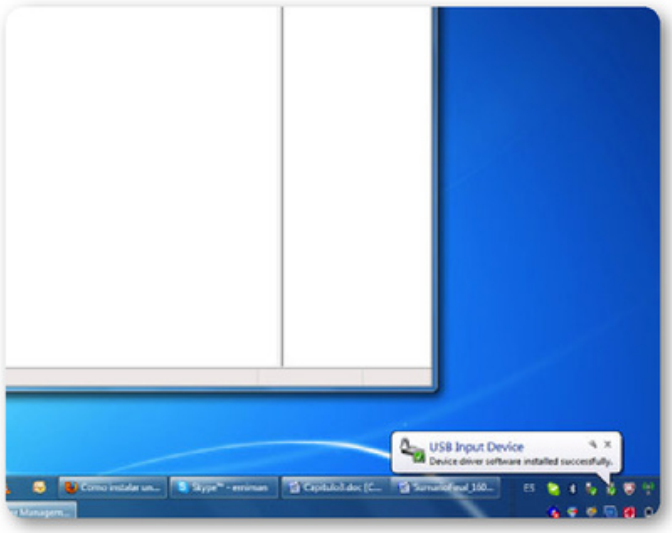


Figura 3. Windows nos informará que ha detectado e instalado los drivers necesarios para nuestro dispositivo.

En caso de que ya tengamos acceso a Internet en nuestra computadora por medio de cable, podremos descargar la versión más reciente del driver, y proceder con su instalación.

Si estamos instalando una placa inalámbrica PCI, debemos apagar la computadora, desconectar la alimentación, luego quitar la carcasa y buscar un lugar vacío para enchufar la nueva placa inalámbrica. Este lugar vacío se llama **slot PCI** y se encuentra en la placa madre (**motherboard**).

> PARA INSTALAR UNA PLACA WIFI, DEBEMOS BUSCAR UN SLOT VACÍO EN EL MOTHERBOARD

Los zócalos de expansión, básicamente, son ranuras de plástico que poseen en su interior conectores eléctricos donde se introducen las tarjetas o placas de expansión (placas de video, placas de sonido y de red, entre otras). Los slots presentan diferente tamaño y, a veces, distinto color. Esto es así para distinguir la tecnología en que se basan cada uno.

Una vez conectada la placa PCI, volvemos a enchufar la fuente de alimentación (previamente, tenemos que cerrar el gabinete por seguridad) e iniciar Windows. El mismo sistema operativo reconocerá que existe un nuevo hardware y solicitará permiso para instalar el mejor driver. Si tenemos un driver que nos provee el fabricante del dispositivo, recomendamos usarlo. De no contar con él, podemos dejar que Windows instale el que corresponda.

Tomemos, como ejemplo, la instalación de la placa PCI en una computadora de escritorio. Aunque la instalación de una placa inalámbrica PCI puede parecer casi como una aventura desconocida, al final descubriremos que, para los no experimentados, simplemente consiste en abrir el gabinete de la CPU, descubrir dónde colocar la placa, cerrar el gabinete y luego instalar los controladores o drivers tal como lo describimos previamente. Si nunca abrimos el gabinete de nuestra computadora, no debemos hacernos problema: basta con seguir algunas recomendaciones para no tener inconvenientes.

MEZZANINE O PCI

PCI es una especificación desarrollada para realizar la correcta interconexión de componentes en computadoras personales. El bus PCI también es llamado Mezzanine (en español significa entrepiso, en relación a un piso que está a media altura entre el nivel del suelo y el primer piso de un edificio), dado que funciona como un nivel añadido al viejo bus ISA/VESA tradicional del motherboard.

Configurar el hardware en Windows

En estos momentos estamos listos para configurar nuestro dispositivo inalámbrico y, de esta forma, tener acceso a la red. En general, Microsoft Windows siempre intentará conectarse a la red inalámbrica que presente la señal más intensa. Nos va a solicitar confirmación antes de concretar la conexión a una red que no tenga contraseña de seguridad ingresada. Esto ocurrirá siempre que tengamos habilitado el dispositivo inalámbrico.

Cuando nuestro cliente (nuestra placa inalámbrica instalada) esté dentro del rango de un punto de acceso, notaremos en el área de notificación de la barra de tareas que hay un icono que indica la existencia de conexiones disponibles. Al hacer clic allí, veremos la lista de las redes inalámbricas detectadas.

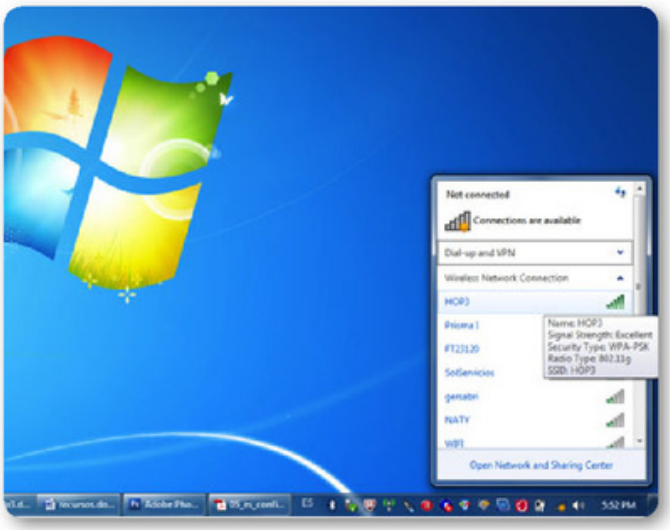


Figura 4. En el área de notificación, vemos el icono de conexión con un signo de admiración.

Si dejamos el puntero del mouse sobre alguna de las redes, podremos acceder a información básica y útil de la red, como el SSID, el método de cifrado que utiliza o la calidad de la señal.

El icono al lado del nombre de la red indica cómo nos llega la señal, y según la intensidad, se completan las barras con color verde. Si este icono tiene un pequeño **escudo naranja**, estará indicando que la red no posee contraseña de seguridad para conectarse y es insegura.

Selección de la red

Como primer paso en nuestra configuración, vamos a seleccionar una red disponible a través del SSID de la red deseada. Como vimos anteriormente, el SSID (identificador de conjunto de servicio) es el nombre de la red. Cuando más de un punto de acceso usa el mismo SSID, se llama ESSID (identificador de conjunto de servicio extendido).

Si seleccionamos una red que no esté usando ningún tipo de seguridad, como WEP/WPA, cuando identifiquemos y seleccionemos su SSID y nos conectemos, nos daremos cuenta de que aparecerá una advertencia de que la red es insegura y, por consiguiente, nuestros datos podrán estar en riesgo.

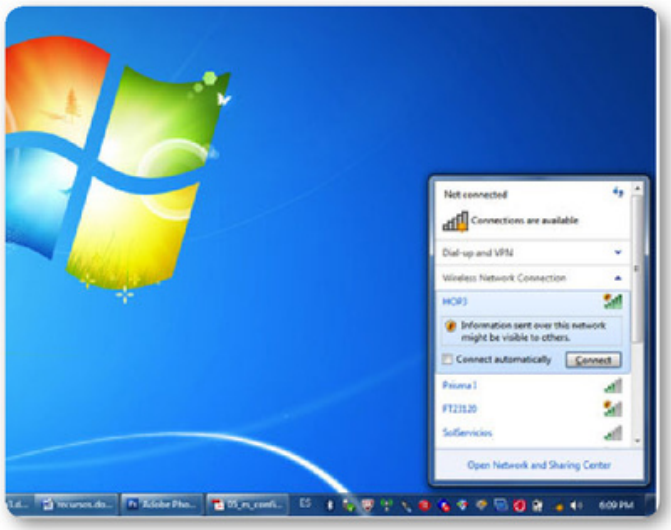


Figura 5. Cuando la red no posee contraseña, el sistema nos informará que nuestros datos pueden ser vistos por intrusos.

Si nuestra red tiene seguridad por contraseña (configurada en el punto de acceso), necesitaremos tener conocimiento de la clave antes de poder conectarnos. La clave de seguridad debería ser la misma con la

DIFERENCIA ENTRE BSSID Y ESSID

Debemos tener en cuenta que los términos BSSID y ESSID muchas veces resultan confusos. ESSID significa Extended Service Set ID, y es el nombre identificable de la red. BSSID significa Basic Service Set Identifier, y se trata de la dirección MAC (física) del punto de acceso al que nos conectamos. Si sabemos el significado, es difícil que nos confundamos.

que se configuró el punto de acceso que se utiliza en la red.

Como se muestra en la imagen, tendremos una ventana emergente que nos solicitará la contraseña que corresponde a la red. Al ingresarla, veremos cada uno de los caracteres, salvo que tengamos marcada la opción **Esconder caracteres** (**hide characters**), con la que solo veremos puntos al momento de escribir la clave.

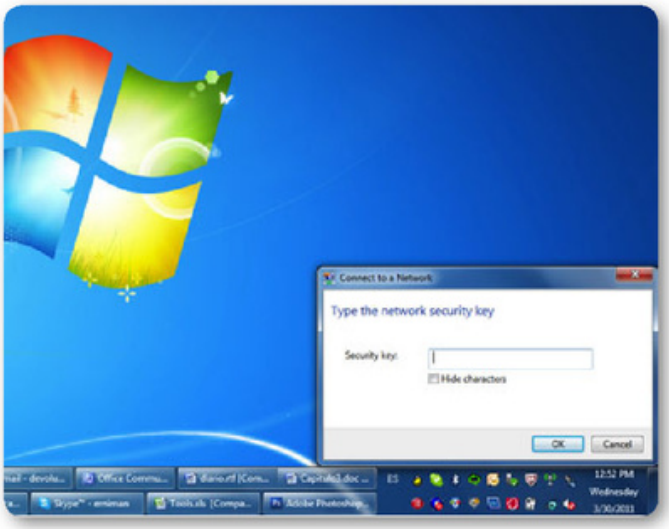


Figura 6. Cuando nuestra red tiene contraseña, se comparte la clave o contraseña de red entre el punto de acceso y sus clientes.

Configurar opciones de TCP/IP

Ahora vamos a verificar y ajustar las opciones del protocolo TCP/IP. En esta instancia, según cómo hayamos configurado nuestro punto de acceso, podremos obtener una IP dinámica a través del uso del protocolo DHCP, o fijar, de forma manual, una dirección IP estática para la tarjeta inalámbrica de la computadora.

> UNA DIRECCIÓN IP ES UN CÓDIGO COMPUESTO POR CUATRO OCTETOS DE INFORMACIÓN

Para refrescar conceptos, decimos que una dirección IP es un código de **4 octetos** (un **octeto** está formado por ocho unidades de información; en este caso, un octeto es un grupo de ocho bits). Cada octeto se separa por puntos, que pueden tener valores entre 0 y 255. Un ejemplo es la dirección IP 127.0.0.1. Utilizamos las direcciones IP para identificar un equipo en la red (comúnmente llamado **host**). Cuando hablamos de equipo, puede tratarse de un usuario conectado

a una red privada (LAN) o de un servidor que ofrece un servicio conectado a una red de área extensa (WAN), entre otros.

Por ejemplo, una dirección IP es un número que identifica a una computadora o un dispositivo conectado a Internet. Esto no significa que exista una IP por computadora: un grupo de computadoras de una misma red pueden tener la misma IP. Esta dirección puede cambiar al reconectarnos a la red; si es así, se la denomina **dirección IP dinámica**. Si la dirección no varía, se llama **dirección IP fija**.

UNA DIRECCIÓN IP SE ENCARGA DE IDENTIFICAR A UNA COMPUTADORA O DISPOSITIVO

También se puede distinguir entre **IP privada** (también llamada IP de red) e **IP pública** (IP de Internet). Una IP pública es aquella que tenemos en Internet. La IP privada es la que tenemos en nuestra propia red local, dentro de la red, posicionados en nuestro dispositivo, el router, por ejemplo.

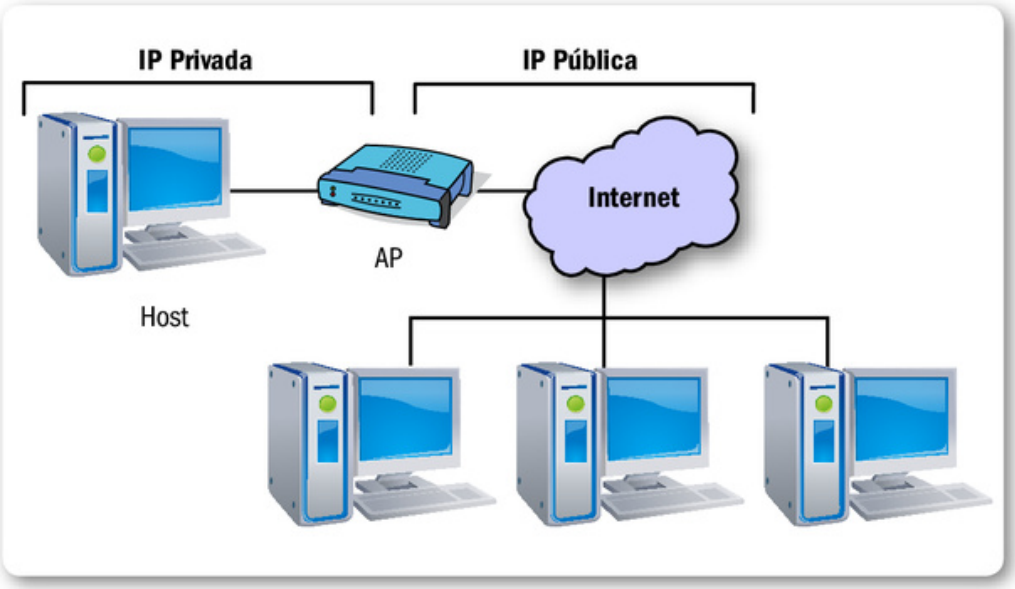


Figura 7. Diferenciamos IP privada y pública tomando como referencia el acceso a la Red de redes (Internet).

- IP privada: es la dirección que tiene una computadora o un dispositivo de red (este puede ser un punto de acceso, por ejemplo) dentro de la red LAN (red privada de área local).

- IP pública: es aquella que tiene una computadora o red, y que se usa para establecer comunicación entre una computadora o red y una red de área extensa (WAN). La denominamos IP pública dado que, cuando se establece conexión con otro host (desde nuestra computadora dentro de una red privada), se envía esta dirección como parámetro para que este pueda contestar.

Muchas veces surge la siguiente pregunta: ¿la IP pública puede ser igual a la IP privada? La respuesta es: depende. Si nuestro caso es que solamente tenemos una computadora, no pertenece a una ninguna red y se conecta a través de un módem o un router, entonces podemos decir que las dos IP van a ser iguales.

En caso de tener una red vinculada a un router (u otro dispositivo de red), estas IP serán diferentes.

Si ingresamos al sitio **www.ip2location.com**, podremos obtener la IP pública, entre otros datos de nuestro proveedor de Internet o ISP. A continuación, veremos de qué forma podemos conseguir nuestra IP privada con los comandos básicos de Windows. Esto nos ayudará cuando, en capítulos posteriores, aprendamos un método para la resolución de problemas.

Utilidad **Ipconfig** es una aplicación del sistema operativo Windows que muestra valores de configuración de red en una **consola**. El término **consola** hace referencia a un intérprete de comandos en sistemas operativos que permite ejecutar líneas de comando sin hacer uso de una interfaz gráfica (como la gran mayoría de las aplicaciones en Windows). Algunos comandos, sobre todo los de tareas administrativas del sistema o los que requieren vincular varios archivos, son más fáciles de implementar desde una consola y, muchas veces, esta es la única manera de realizarlo.



ASIGNACIÓN DE IP POR DHCP

Sin DHCP, cada dirección IP debe configurarse manualmente en los clientes, y si estos se mueven a otra parte de la red, se debe configurar otra dirección IP diferente. El DHCP permite al administrador de la red supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si el cliente se conecta en otro lugar de la red.

Una función bastante importante de **ipconfig** es la de renovar la dirección IP de una placa de red, siempre y cuando el servidor DHCP que entrega las direcciones se encuentre disponible.

Para abrir la consola, tenemos que ir a **Inicio**, luego a **Ejecutar** y ahí escribir **cmd**, como se muestra en las figuras siguientes.



Figura 8. Desde la opción **Ejecutar** (**Run**), el sistema operativo Windows nos permite ejecutar comandos.

Veamos algunos usos básicos de este comando:

- Para obtener información de configuración, ingresamos en la consola el comando **ipconfig**, que nos mostrará únicamente detalles básicos de la conexión (tales como dirección IP asignada, máscara de subred, puerta de enlace o gateway, entre otros).

Si queremos obtener más información con este comando, ejecutamos en la consola **ipconfig /all** y esperamos mientras se muestran los datos.

Debemos tener en cuenta que si la IP fue obtenida por DHCP, se mostrará el tiempo durante el cual es válida; por lo tanto, transcurrido este tiempo, la IP expirará y habrá que renovarla. Si esto sucede, el

DHCP automáticamente asignará una nueva IP. En este caso, podemos darnos cuenta que el tiempo figura como **Concesión obtenida** o también como **Concesión expirada** (**Lease obtained** o **Lease expires**).

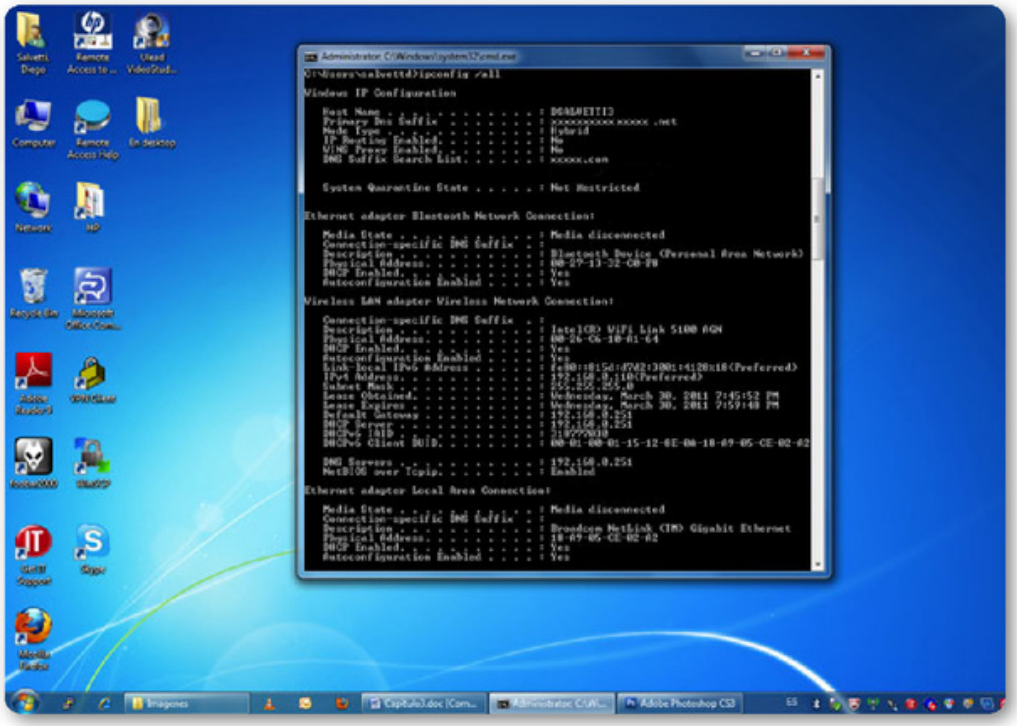


Figura 9. Este comando nos brinda información como nombre de host, IP privada y dirección de la puerta de enlace, entre otros datos.

Aprovechemos para hablar un poco más del protocolo DHCP, que tanto estamos nombrando. El protocolo de configuración dinámica de clientes DHCP (**Dynamic Host Configuration Protocol**) es un protocolo de red que permite a los **nodos** (esto incluye a clientes y dispositivos) de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo del tipo cliente-servidor (esto significa que el cliente trabaja en conjunto con el servidor, que es el que ofrece los parámetros de configuración). El servidor tiene una lista de direcciones IP dinámicas que va asignando a los clientes conforme estas van quedando libres. Al tener esta lista, el servidor sabe en todo momento qué dirección IP posee cada cliente de la red, cuánto tiempo lleva con ella y otros puntos importantes para el funcionamiento del protocolo.

Ahora que tenemos mayor conocimiento acerca del protocolo DHCP, podemos ver cómo es la renovación de la dirección IP al usar DHCP.

Cuando usamos DHCP y nuestra computadora obtiene sus parámetros automáticamente (dirección IP, máscara de red, entre otros), es probable que necesitemos renovar nuestra dirección IP. Para hacerlo, ejecutamos el comando **ipconfig** desde una consola (como vimos anteriormente).

Renovar la dirección IP suele ser una solución cuando, debido a cortes de electricidad, por ejemplo, nuestro router entra en conflicto con la IP que nos fue asignada. En este momento aparecen los famosos problemas de conexión a Internet. Haciendo esta renovación de dirección IP, nos evitamos resetear (o reiniciar) el router de la red o, tal vez, el trabajo de reiniciar nuestra propia computadora.

En una consola vamos a escribir estas líneas, una por una, seguida de la presión de la tecla **ENTER** luego de cada comando:

```
ipconfig /release
ipconfig /renew
```

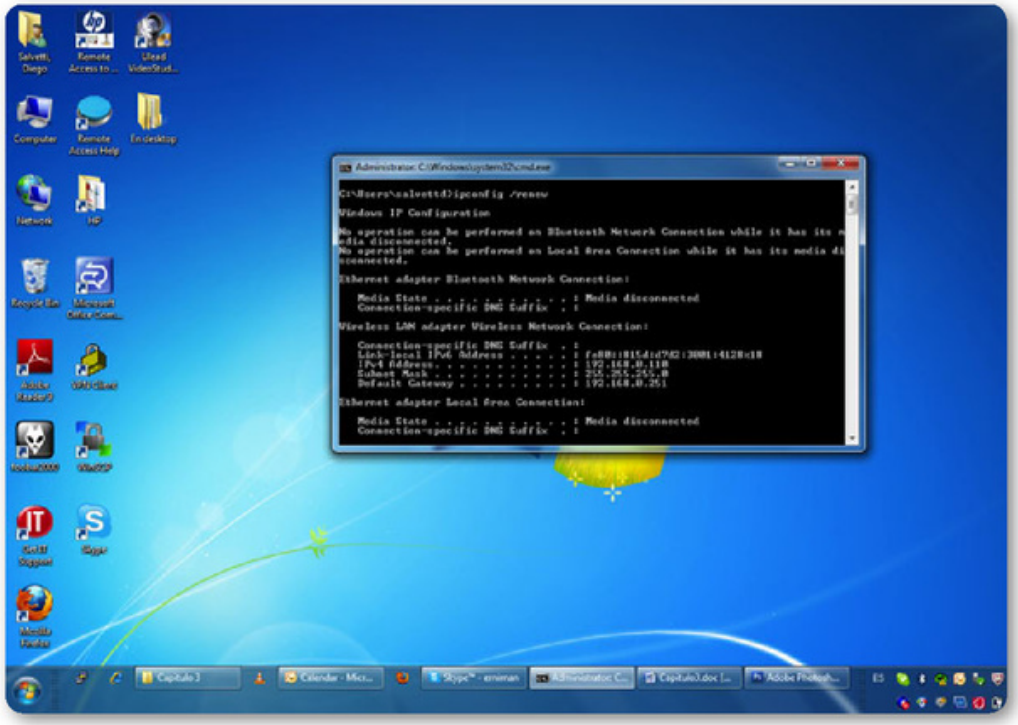


Figura 10. Luego de liberar la dirección IP de nuestra placa de red, ejecutar **ipconfig/renew** nos permite obtener una nueva IP.

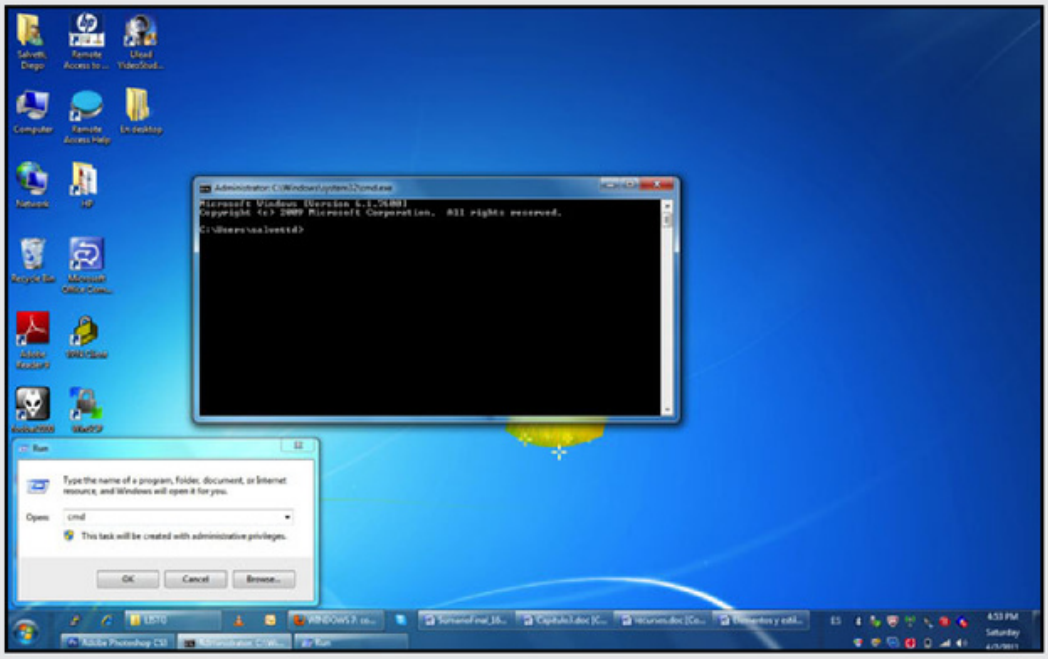
Si lo que deseamos es fijar de forma manual una dirección IP estática para nuestra placa inalámbrica, podemos seguir unos pasos básicos para realizarlo. Tengamos en cuenta que esta es solo una manera de realizar esta asignación, y existen otras que no veremos ahora dado que son similares pero por diferentes caminos.

> DEBEMOS ESCRIBIR LA CONFIGURACIÓN ACTUAL ANTES DE REALIZAR ALGÚN CAMBIO

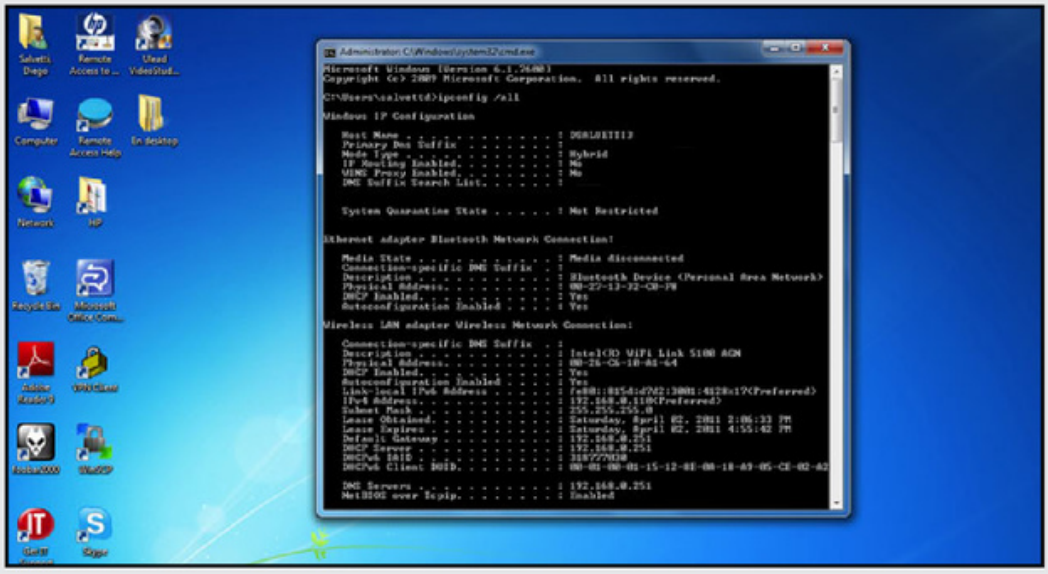
Antes de describir los pasos para asignar una dirección IP estática a nuestra placa inalámbrica, escribamos en un papel (documento de Word o similar) cuáles son las configuraciones que tenemos en ese momento (esto es en caso de que la red ya esté configurada). En este punto, si nos damos cuenta de que algo no sale como lo planeamos, siempre podremos volver a la configuración inicial si la tenemos.

CONFIGURACIÓN DE IP ESTÁTICA ■ PASO A PASO

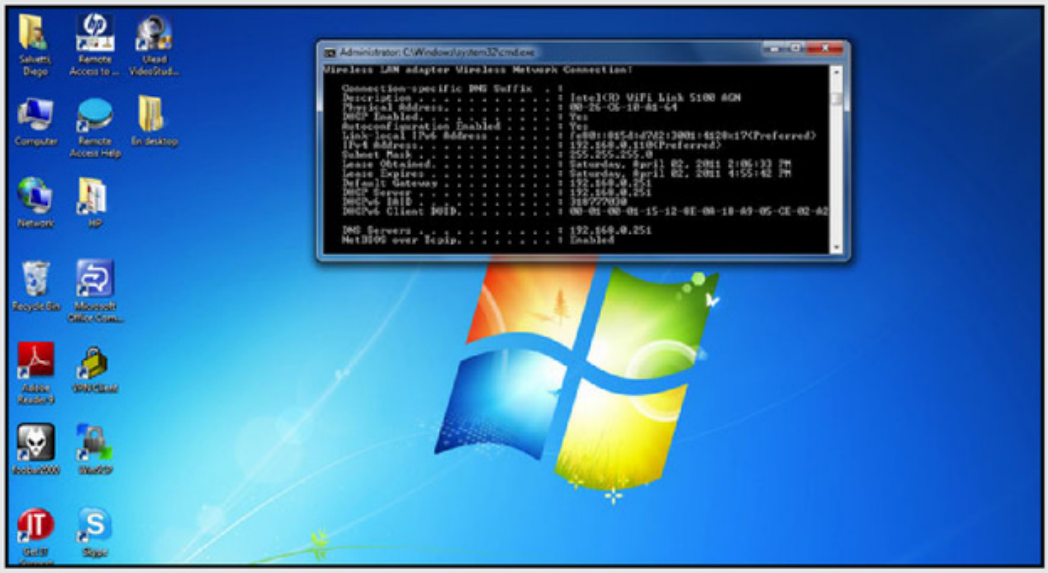
01 Copie la información que actualmente posee para su placa inalámbrica. Puede saltear este paso si no tiene ninguna configuración previa para su dispositivo inalámbrico. Abra una consola como se mostró anteriormente, haciendo clic en `Inicio` y, luego, en `Ejecutar` (o Run) y escriba `cmd`.



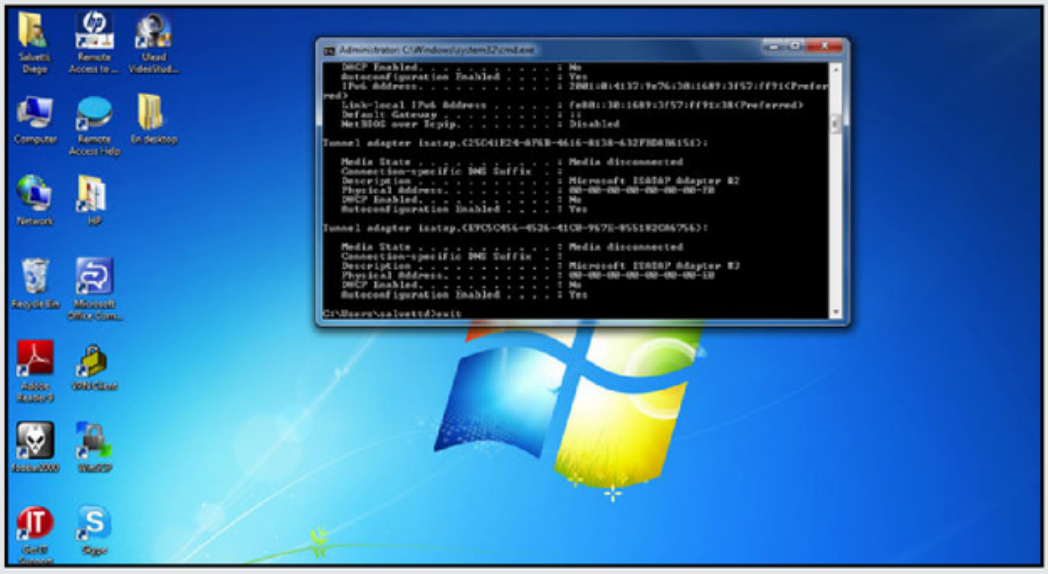
02 Si desea ver los parámetros relacionados con la placa inalámbrica, escriba el comando `ipconfig /all` y presione la tecla ENTER. Esto mostrará la configuración actual de todos los dispositivos de red.



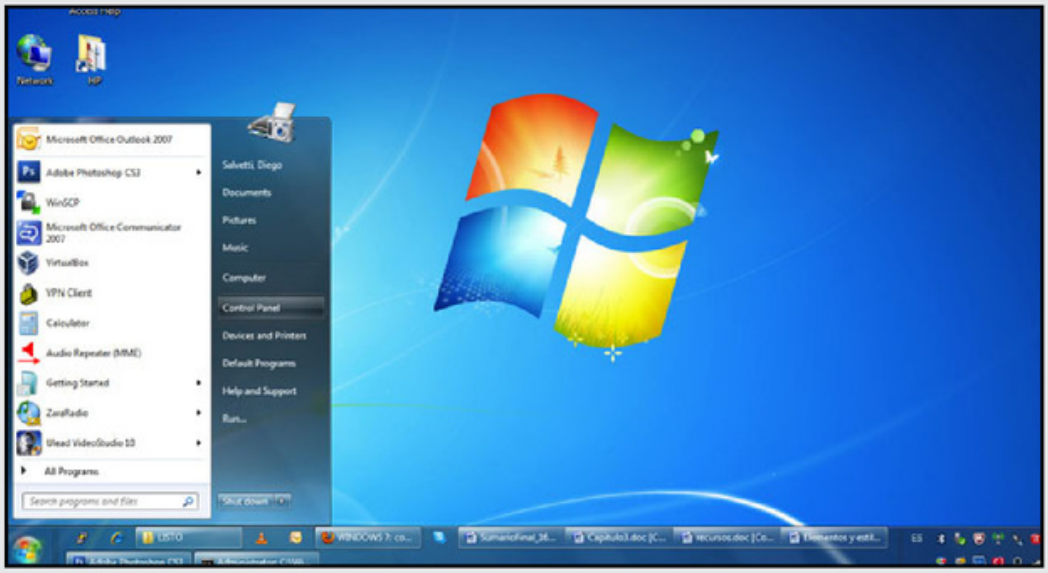
03 Identifique la información relevante correspondiente a su placa inalámbrica. Puede que tenga muchas líneas de información, pero lo importante es que vea las correspondientes a IPv4 Address, Subnet Mask, Default Gateway y DNS Servers. Todos estos parámetros pueden estar descriptos para más de un adaptador.



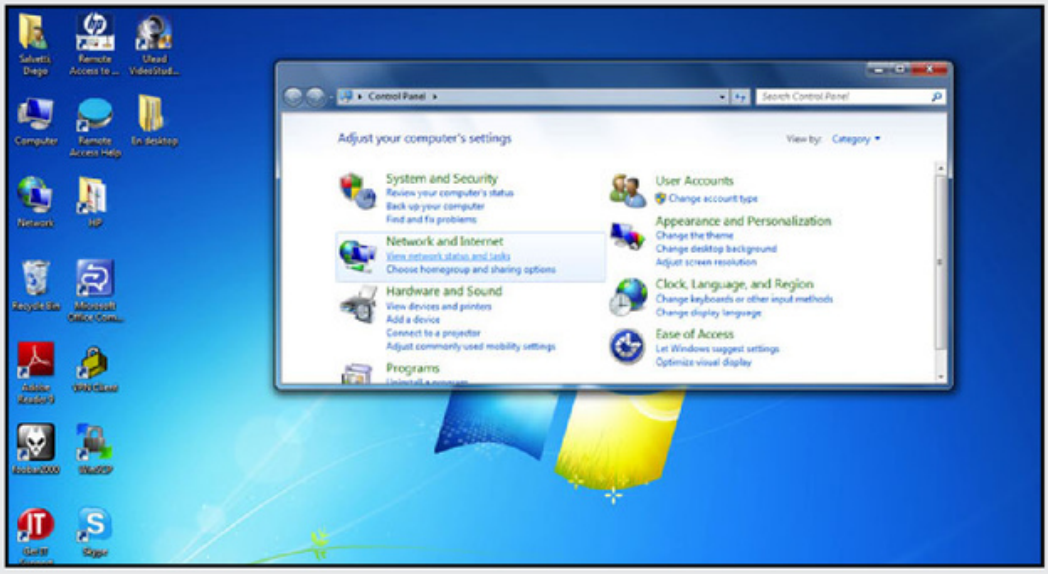
04 Tome nota de los parámetros que identificó. Tiene que anotar: Dirección IPv4 (IPv4 Address), Máscara de subred (Subnet Mask), Puerta de enlace predeterminada (Default Gateway) y Servidores DNS. Asegúrese de escribirlos correctamente. Cierre la consola cuando termine (puede escribir `exit` para hacerlo).



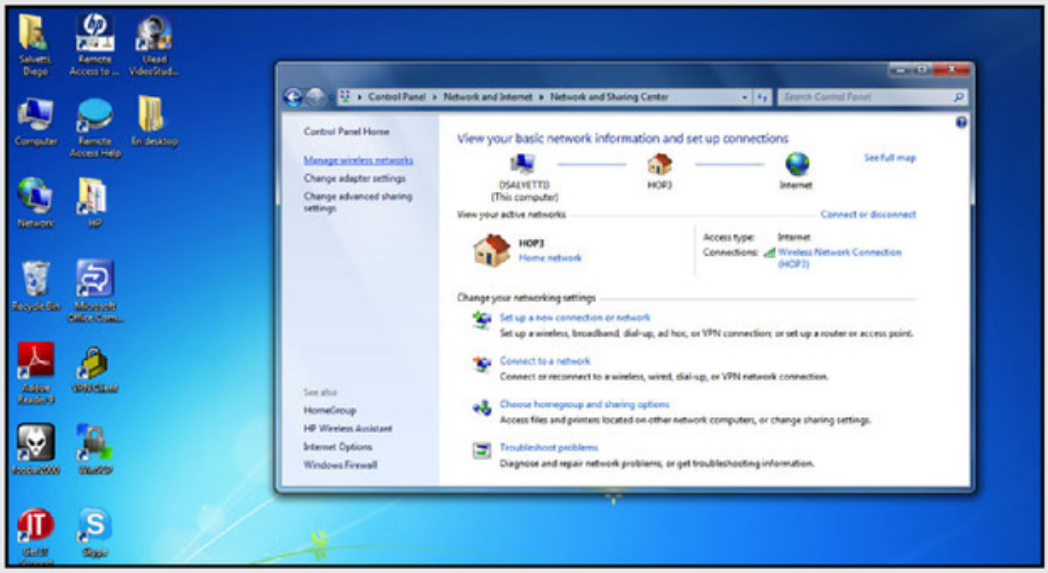
05 Para continuar, es necesario que abra el Panel de control del sistema operativo y seleccione su dispositivo de red. Para realizar esta tarea, vaya a `Inicio` y haga clic sobre `Panel de control` (`Control Panel`).



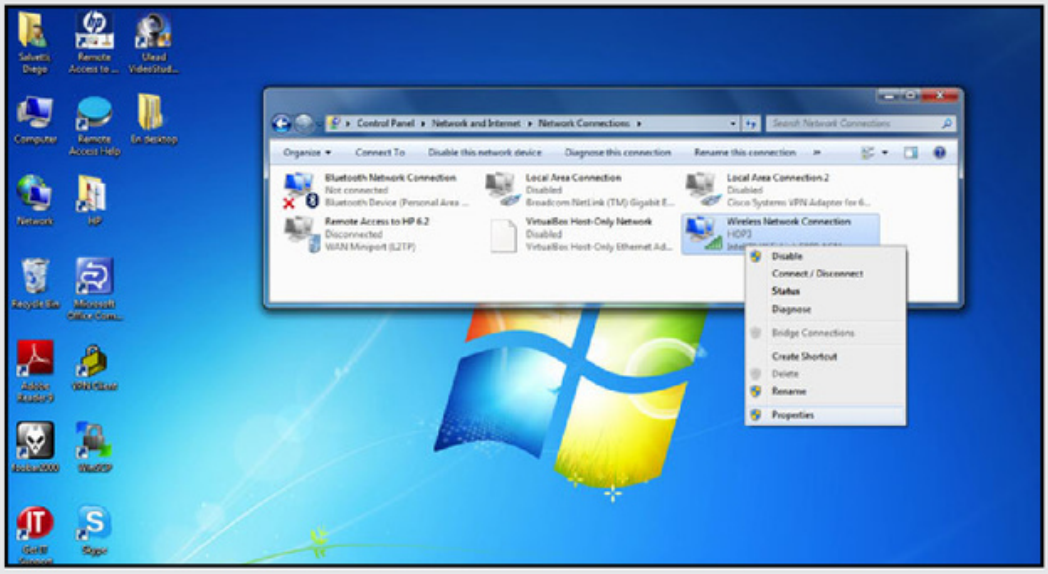
06 Haga clic en Ver el estado de la red y tareas (View network status and task) para ir a la configuración del adaptador de red inalámbrica.



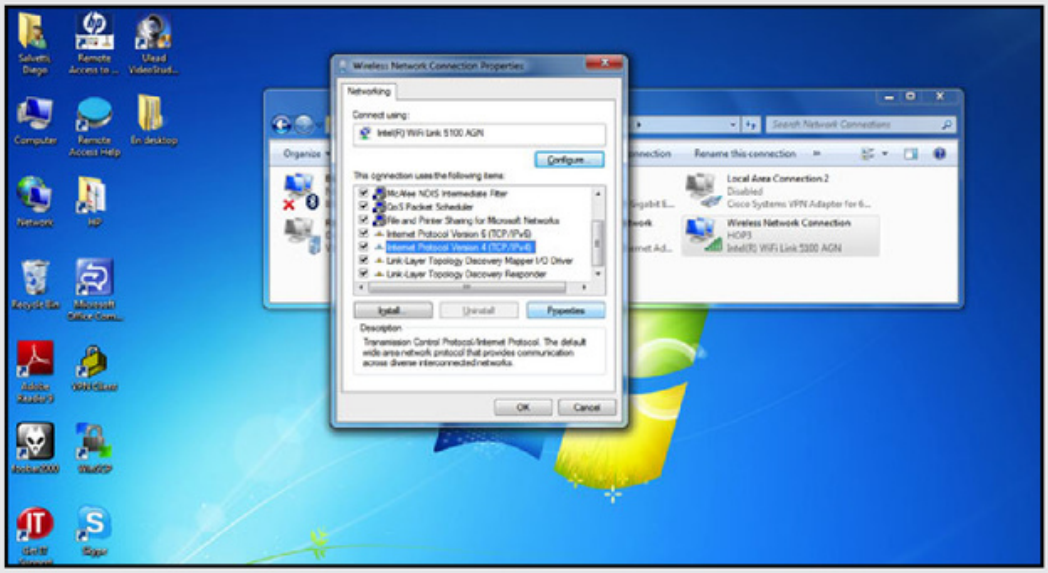
07 Identifique el menú en la parte izquierda de la pantalla y haga clic en Cambiar configuración del adaptador (Change adapter settings). De esta forma, tendrá todos los adaptadores de red de su sistema en esa pantalla.



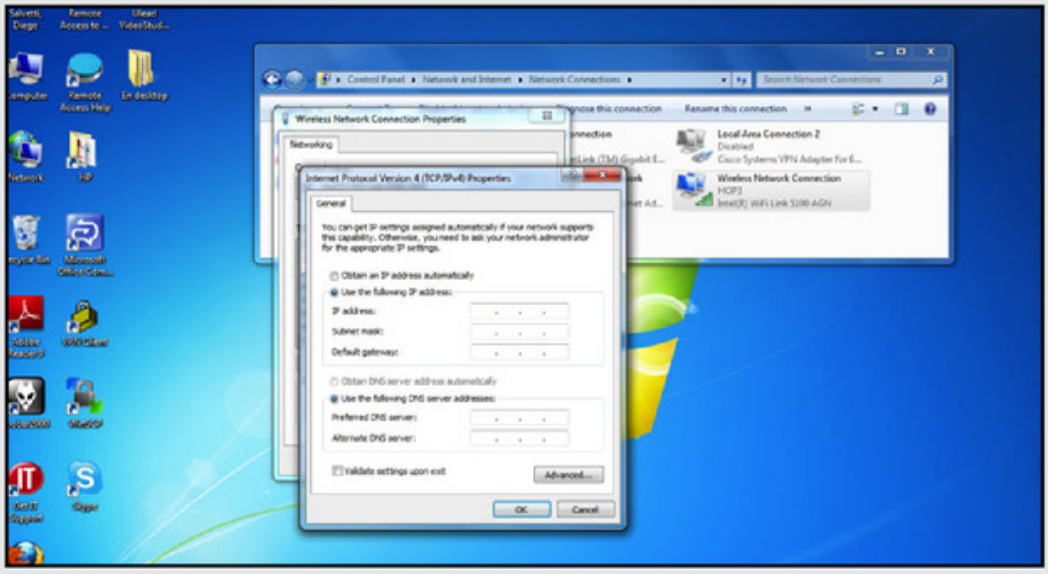
08 Haga clic con el botón derecho del mouse sobre su adaptador de red inalámbrica y luego clic en Propiedades (Properties). Note que solo los adaptadores habilitados tienen colores. Los iconos en color gris significan que el adaptador se encuentra deshabilitado.



09 Ahora tiene que hacer un clic sobre Protocolo de Internet versión 4 (Internet Protocol Version 4), que se encuentra en el cuadro central donde dice "Esta conexión usa los siguientes ítems". Luego presione en el botón Propiedades. Deslícese con la barra de desplazamiento del costado si es necesario.



10 En las propiedades del dispositivo, seleccione `Usar la siguiente dirección IP (Use the following IP address)` para asignar una IP fija. Piense en una y colóquela en Dirección IP. Luego ingrese los valores para la Máscara de subred y para la Puerta de enlace predeterminada.



Tengamos en cuenta que la dirección IP que seleccionemos debe ser similar a la IP del router (o sea, la dirección debe estar en la misma red). En general, solo deben cambiar los tres últimos dígitos. Así, si la dirección del router es 192.168.1.1, podríamos usar para nuestra placa de red la dirección 192.168.1.10.

Los tres dígitos finales pueden tener un valor entre 1 y 254, y no puede seleccionarse una dirección que sea igual a la de otro dispositivo de la red. Debemos tener en cuenta que todo dispositivo que esté conectado a la red deberá tener su propia dirección IP.

CONOCER IP PÚBLICA

Recordemos que si necesitamos consultar sitios que nos muestren cuál es nuestra IP pública y otros detalles de la conexión (como el sistema operativo usado, el navegador de Internet, entre otros), podemos dirigirnos a los siguientes sitios web: **www.my-ip.es**, **www.cualesmiip.com**, **www.cual-es-mi-ip.net**, **www.obtenerip.com.ar**, **www.vermiip.es** y **www.mi-ip.cl**.

La máscara de subred se completará automáticamente cuando ingresemos la dirección IP estática seleccionada. El valor de la puerta de enlace es el mismo que anotamos en el paso 4. Para saber qué valor de Servidor de DNS tenemos que usar, podemos consultar con nuestro proveedor de Internet. De todas formas, también podemos hacer uso de cualquier servidor de DNS. Por ejemplo, **Google** provee el servicio de DNS público de manera totalmente gratuita. Los valores de los servidores de DNS de Google son:

- Servidor **DNS1: 8.8.8.8**
- Servidor **DNS2: 8.8.4.4**

Recordemos que el servicio de DNS es el que permite a la computadora traducir los nombres legibles de dominio a dirección IP (valor de cuatro números que identifica a un dispositivo en la red). Las razones por las cuales muchas veces deseamos cambiar nuestros servidores de DNS pueden ser varias, pero en general, se refieren a un mal servicio, interrupciones, filtrado de contenido escaso y lentitud en la respuesta, entre otras. A causa de estos motivos nacieron los servidores DNS gratuitos.

Configurar la red inalámbrica

Como sabemos, muchos podemos estar acostumbrados a configurar una red inalámbrica, o tal vez nunca configuramos una y esta es la primera vez que nos enfrentamos con este tipo de tarea. Sea cual sea el caso, a continuación veremos cómo se configura una red inalámbrica en el sistema operativo Microsoft Windows 7. Debemos saber que se trata de un procedimiento que puede variar un poco si lo comparamos con versiones de Windows anteriores.



SERVIDORES DNS PÚBLICOS

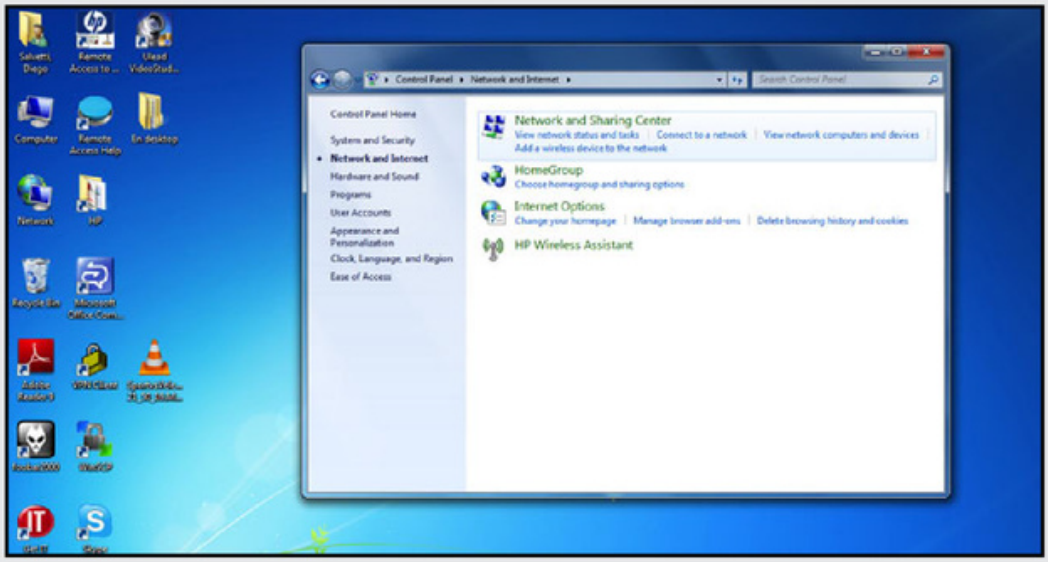
Si necesitamos hacer uso de servidores DNS gratuitos, recomendamos alguno de los siguientes sitios: **www.opendns.com** (servidores: 208.67.222.222 y 208.67.220.220), **www.scrubit.com** (servidores: 67.138.54.100 y 207.225.209.66), **www.dnsadvantage.com** (servidores: 156.154.70.1 y 156.154.71.1) y **http://nortondns.com** (servidores: 198.153.192.1 y 198.153.194.1).

CONFIGURAR LA RED ■ PASO A PASO

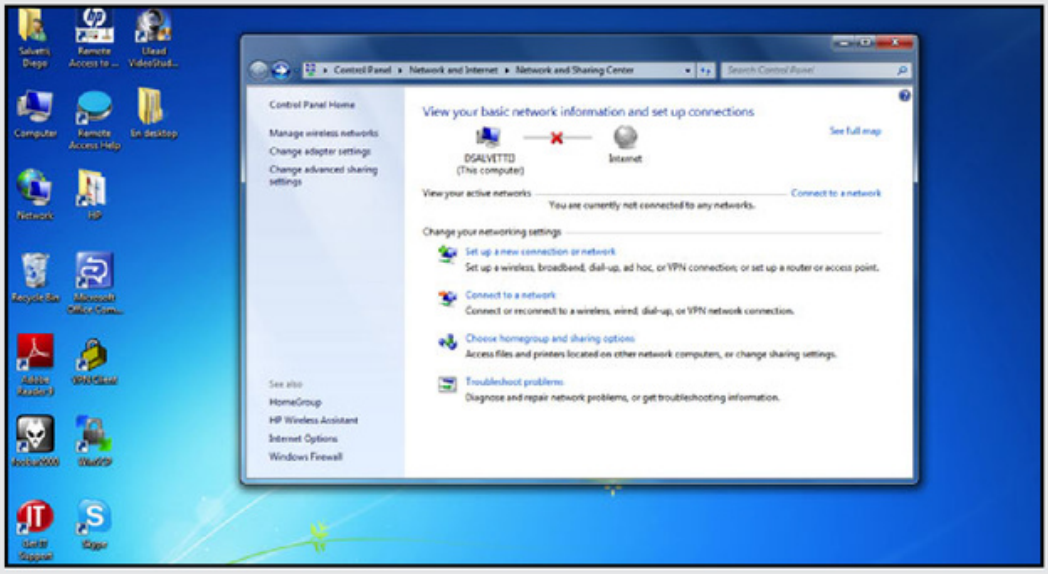
01 Lo primero que debe hacer es acceder al Centro de Redes y recursos compartidos de Windows. Haga clic en `Inicio/Panel de Control/Redes e Internet`.



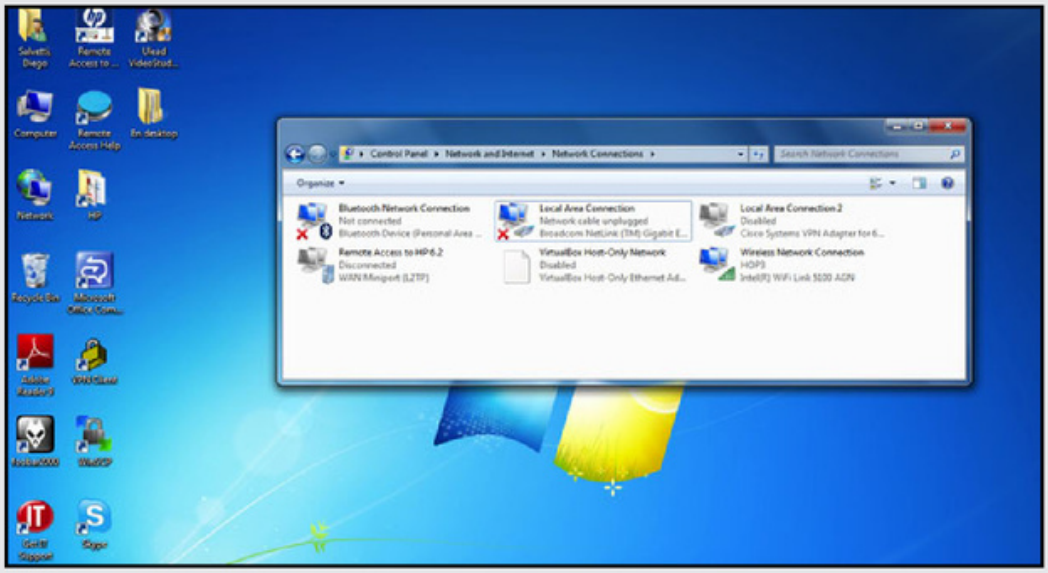
02 Ahora haga clic en `Centro de redes y recursos compartidos` (`Network and Sharing Center`) para ver la información sobre las redes y recursos disponibles.



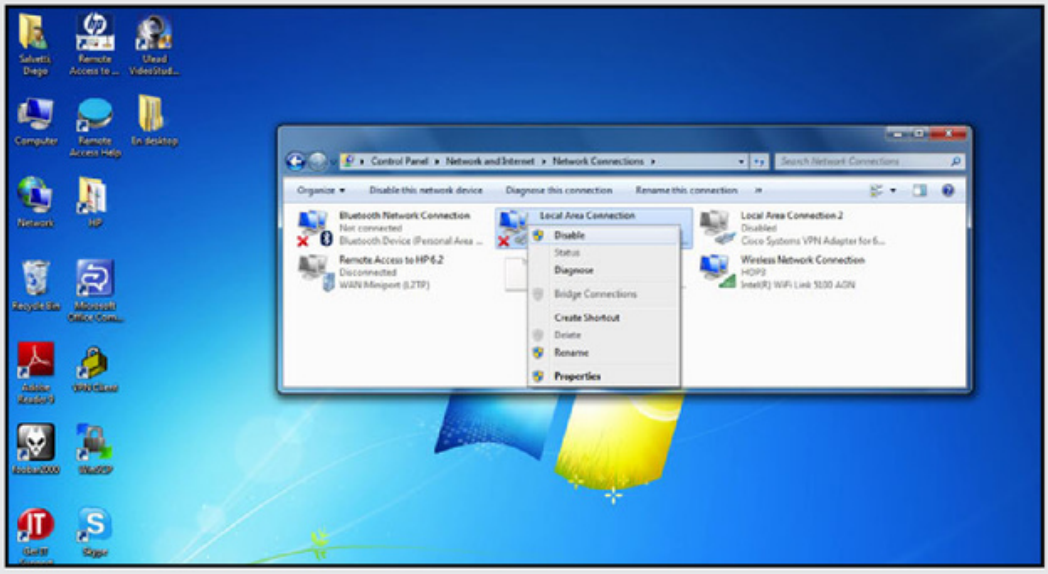
03 Dentro del Centro de redes tendrá tres opciones: Administrar redes inalámbricas (Manage wireless networks), Cambiar configuración del adaptador (Change adapter settings) y Conectarse a una red (Connect to a network).



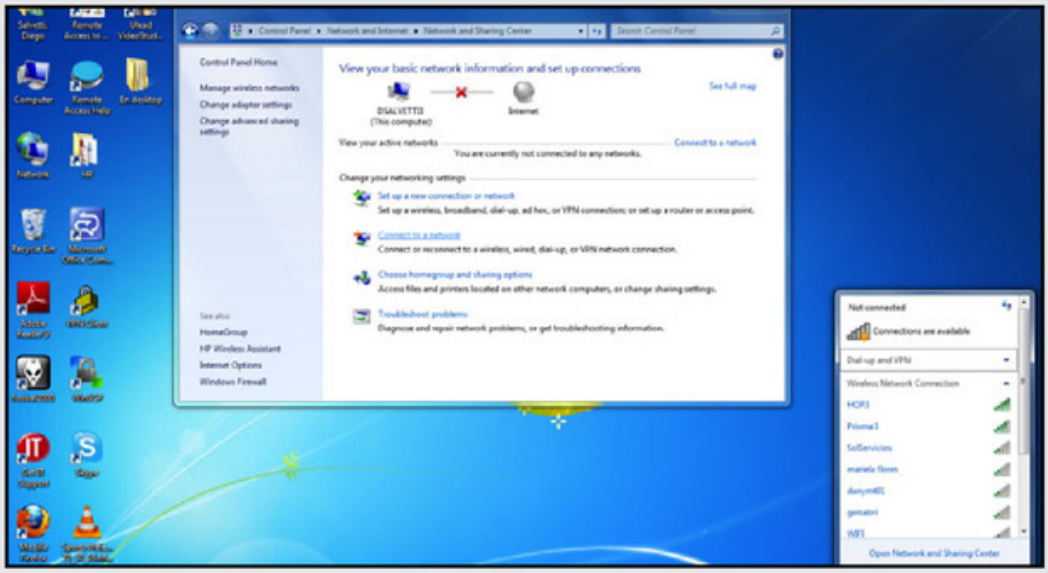
04 Ingrese a Cambiar configuración del adaptador y verá una ventana como muestra la siguiente imagen. En ella puede diferenciar entre los adaptadores habilitados y los deshabilitados. Simplemente, debe fijarse en los iconos de los adaptadores, los que están en color son los habilitados.



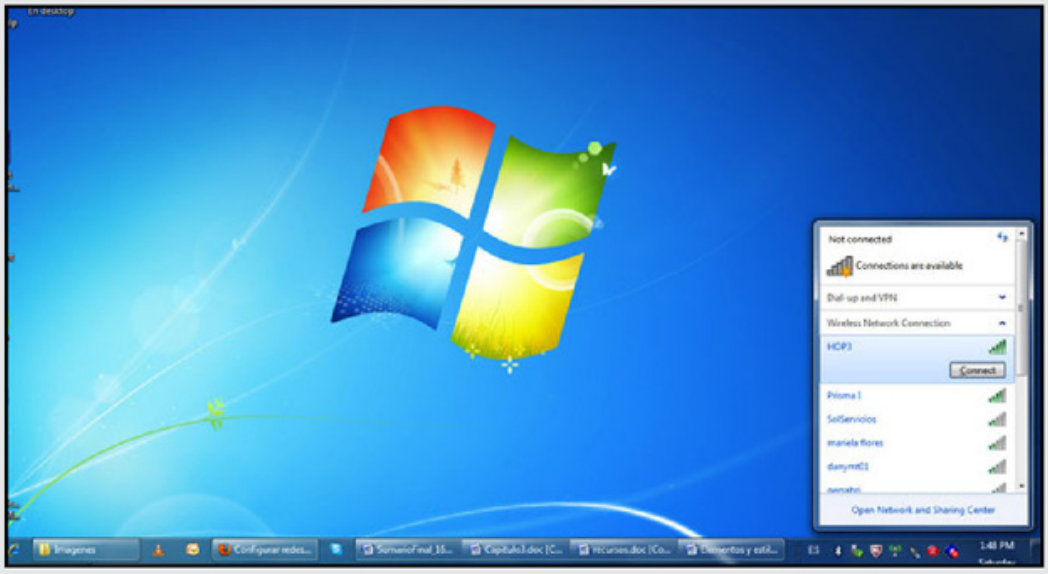
05 Si desea evitar confusiones a la hora de llevar a cabo el proceso de configurar una red inalámbrica, puede optar por desactivar las conexiones de área local u otras conexiones que no sean inalámbricas. En el menú emergente seleccione `Desactivar (Disable)`. Para activarlas, repita el clic y seleccione `Activar`.



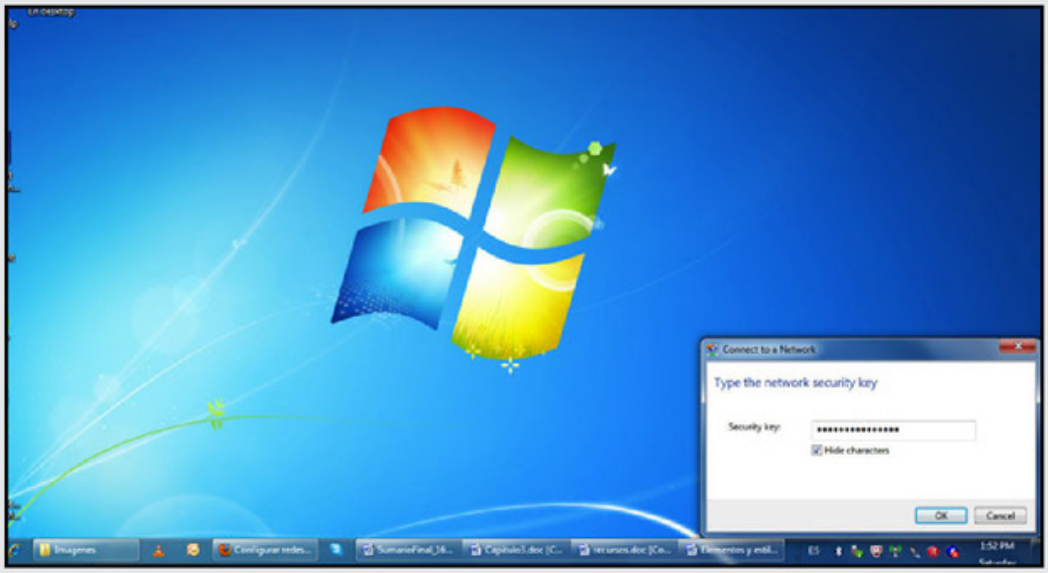
06 Llegado este punto, vuelva al Centro de redes y recursos compartidos (paso 2) y haga clic sobre la opción `Conectarse a una red`. Una vez realizado esto se abrirá el **Escáner de redes inalámbricas** en la parte inferior derecha del escritorio, tal como lo muestra la imagen.



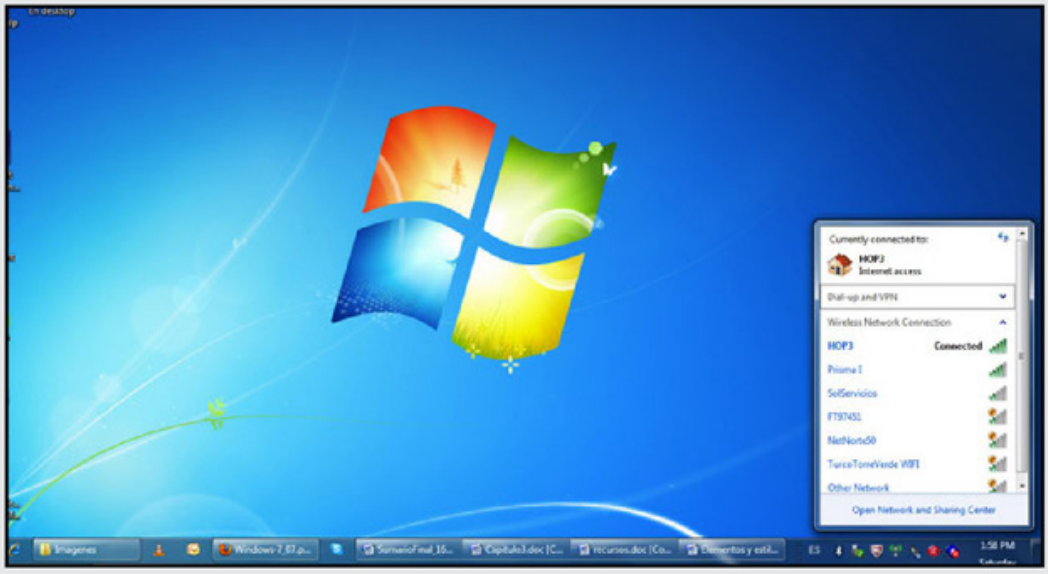
07 Ahora busque su red en el cuadro que muestra todas las redes inalámbricas que están dentro del alcance de su adaptador. Si hace clic sobre el nombre (o SSID) de la red, tendrá la opción de conectarse como lo muestra la imagen.



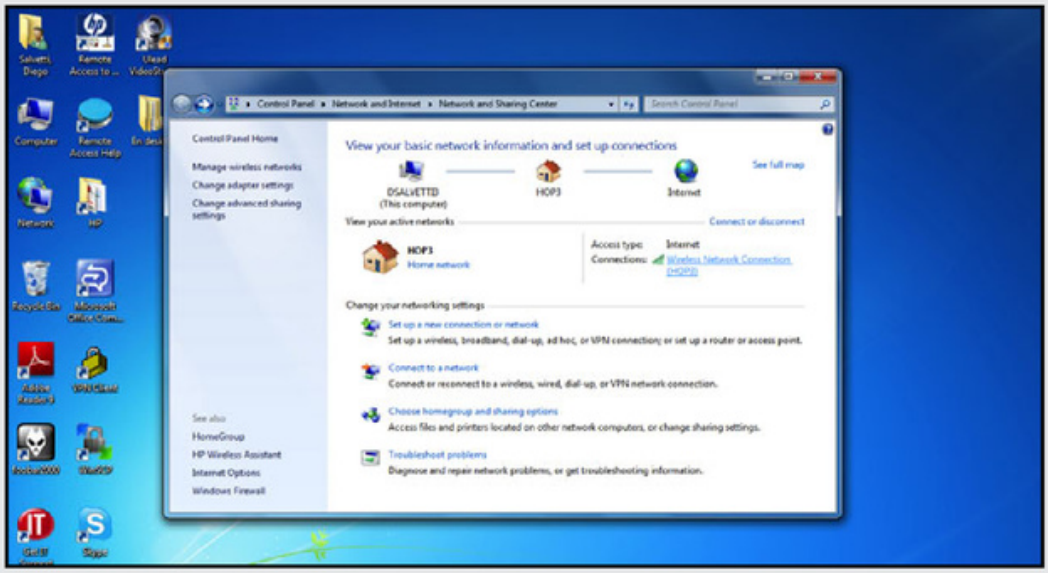
08 Si su red está protegida por contraseña, un cuadro de diálogo le solicitará que la ingrese para así autenticar y entrar a la red inalámbrica. Recuerde que puede hacer clic en la opción `Ocultar caracteres` para esconder su contraseña.



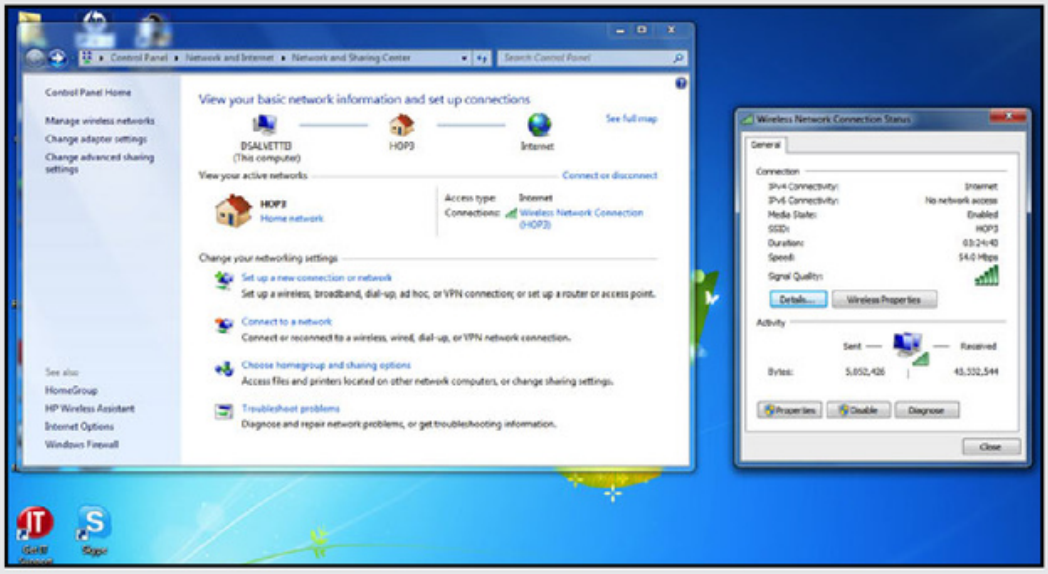
09 Si todo fue bien, estará conectado a la red inalámbrica y podrá verificar esto haciendo clic en el icono que muestra pequeñas barras en blanco en la parte inferior derecha del escritorio. El nombre de la red, en este caso HOP3, aparece resaltado y junto el estado de Conectado (Connected) confirma el éxito.



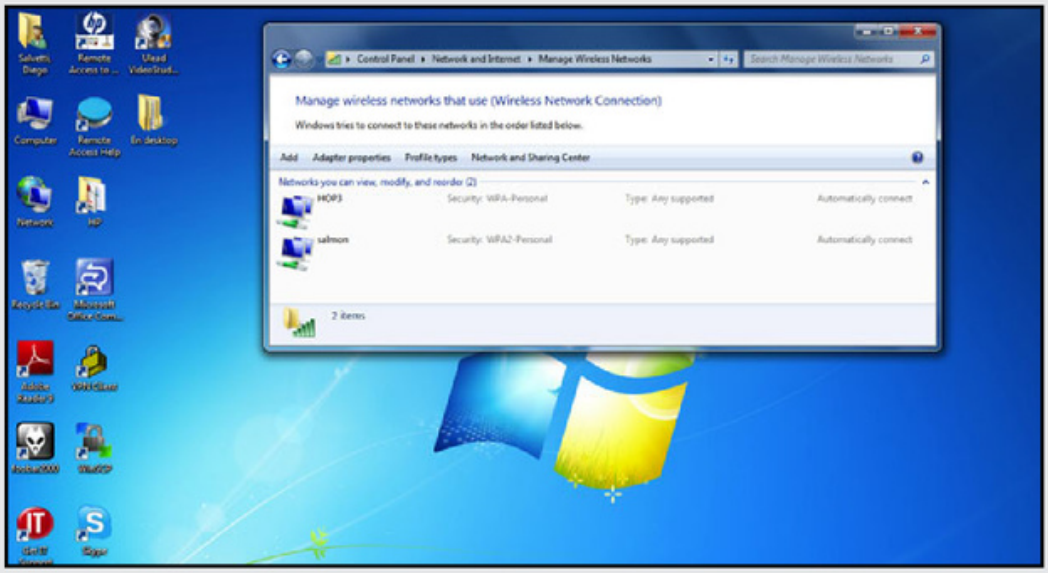
10 Vuelva al Centro de redes y recursos compartidos. Ahora puede ver en la parte central de la ventana que posee una conexión activa. Haga clic sobre el nombre de su red en la opción Conexiones, como muestra la imagen.



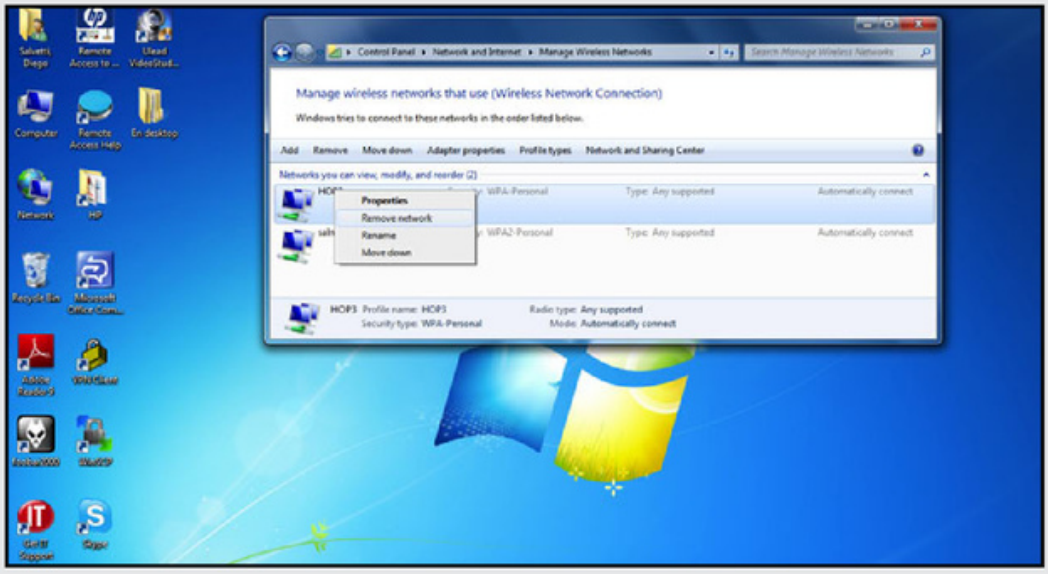
11 Se abrirá la ventana de `Estado de su conexión inalámbrica`, donde puede ver los parámetros más importantes de la red. Puede hacer clic en `Detalles` para obtener mayor información, si lo desea. El icono en Calidad de Señal le informa de manera práctica la calidad de la señal recibida.



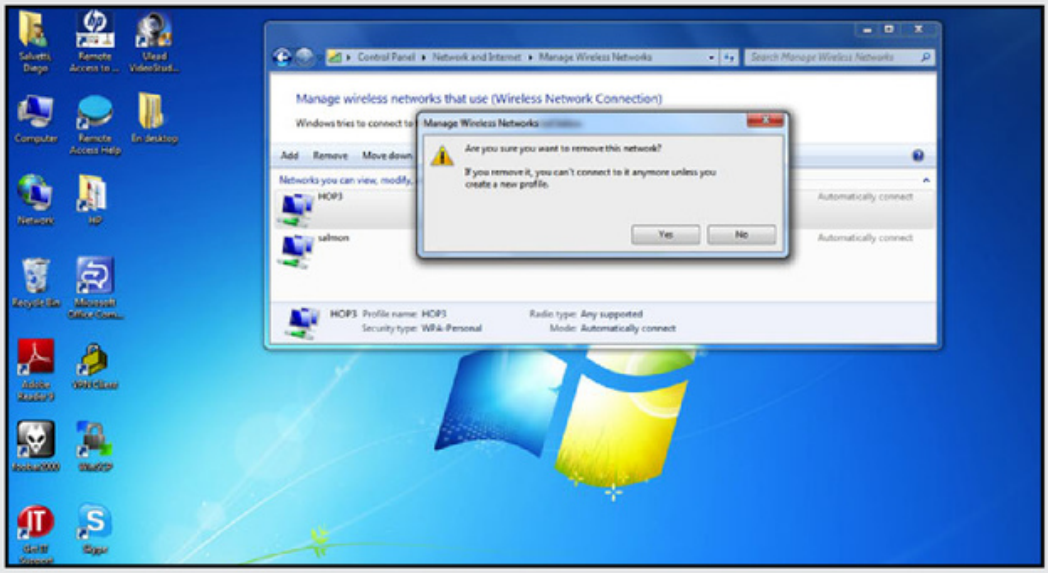
12 Cierre las ventanas anteriores y diríjase nuevamente al Centro de redes y recursos compartidos. Ahora haga clic en `Administrar redes inalámbricas` y verá la imagen siguiente. En esta ventana puede ver los Perfiles de redes, que son las configuraciones de las redes a las que se ha conectado.



13 Si Windows detecta una red de la cual tiene guardado su perfil, se puede conectar automáticamente, ya que posee los parámetros necesarios (por ejemplo, la contraseña). A veces se necesita borrar los perfiles para evitar problemas y errores en la conexión causados por configuraciones existentes que no se usan.



14 Un cuadro de diálogo se abrirá y solicitará que confirme si está seguro de borrar el perfil de red. Le informa, además, que solo podrá conectarse si crea un perfil nuevo para esa red. Seleccione Sí (Yes) para eliminar el perfil. Windows creará el perfil de forma automática la próxima vez que se conecte a esa red.



Configuración de red inalámbrica modo Infraestructura

Recordemos de lo visto anteriormente que en el modo Infraestructura, cada cliente se conecta a un punto de acceso a través de un enlace inalámbrico. Esta configuración compuesta por el punto de acceso y los usuarios ubicados dentro del área de cobertura se llama **Conjunto de servicio básico** o **BSS**; decimos que, así, se forma una célula. Cada BSS se identifica con un BSSID (identificador de BSS).

Cuando vinculamos varios puntos de acceso juntos (para ser más precisos, varios BSS) con una conexión llamada **Sistema de distribución** (o **SD**), formamos un **Conjunto de servicio extendido** o **ESS** (que posee un identificador de conjunto de servicio extendido o ESSID). Muchas veces se abrevia por SSID.

Configuración del AP

Lo primero que vamos a hacer es configurar nuestro **punto de acceso** (AP) para funcionar en el **modo Infraestructura**. En el **Capítulo 2** describimos cómo realizar esta configuración en detalle; repasaremos aquí los puntos más importantes. Asignamos una dirección IP de forma manual a la placa de red de nuestra computadora. Como vimos anteriormente, si queremos acceder a la configuración de nuestro punto de acceso, vamos a usar una dirección IP que esté en la misma subred (también llamada segmento de red). Por ejemplo, si configuramos la dirección IP **192.168.1.1** en nuestro punto de acceso, vamos a usar, para la placa de red, 192.168.1.10. En este punto tengamos en cuenta que este vínculo lo realizamos por medio del **cable UTP**, que trae el punto de acceso.

PERFIL EN MEMORIA USB

Tener el perfil de nuestra red en una memoria USB nos facilita instalar nuevas computadoras en la red. Para hacerlo, seleccionamos nuestra red y hacemos clic derecho, elegimos **Propiedades** y, en la pestaña **Conexión**, hacemos clic en **Copiar este perfil de red a una unidad Flash USB**. Seguimos los pasos del asistente que nos guiará para copiar el perfil.

Ingresamos en el **Centro de redes y recursos compartidos**, luego en **Cambiar configuración del adaptador** y ahí seleccionamos nuestra placa de red (cuidado que no tenemos que seleccionar nuestra placa de red inalámbrica). Hacemos clic con el botón derecho del mouse y seleccionamos **Propiedades** para abrir un nuevo menú desplegable. De los ítems que usa nuestra placa de red, seleccionamos el **Protocolo de Internet versión 4** (TCP/IPv4) y luego hacemos clic en **Propiedades**. Escribimos la dirección IP estática 192.168.1.10, y la máscara de subred se completará automáticamente. No necesitamos ningún otro parámetro, por lo que presionamos en **Aceptar** para grabar la configuración.

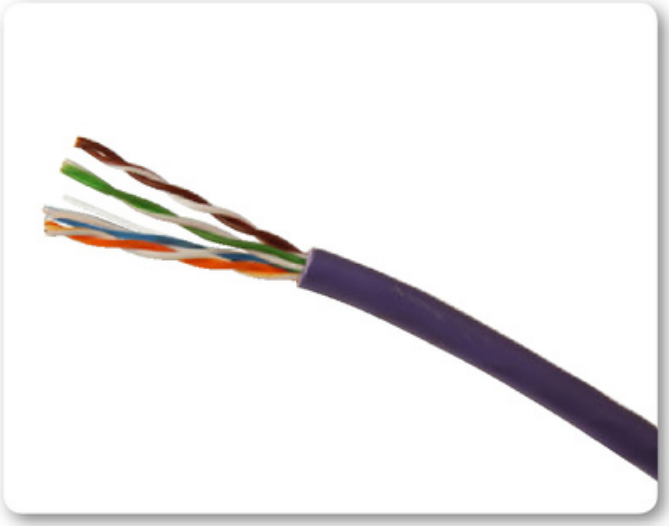


Figura 11. La figura muestra el cable UTP categoría 5 extendida, que encontramos en las redes cableadas.

Ahora abrimos el navegador web para ingresar en las configuraciones del punto de acceso. Accedemos escribiendo la dirección IP del AP, en nuestro caso, 192.168.1.1. Una ventana de acceso al AP nos solicitará ingresar el nombre de usuario y contraseña (recordemos

EN EL MISMO CANAL

Cuando un grupo de computadoras se conectan de forma inalámbrica como una red independiente (ad hoc), todos los clientes deben usar el mismo canal de radio. Aunque si nos conectamos a una red a través de un punto de acceso (modo infraestructura), entonces la placa de red inalámbrica se configurará automáticamente para usar el mismo canal que usa el punto de acceso más cercano.

que si el dispositivo nunca fue configurado, esta información viene por defecto y podemos consultar el manual para obtener estos datos). Aceptamos y vemos el entorno de configuración web del punto de acceso. Algunos dispositivos modernos tienen un asistente de configuración que facilita realizar cambios. De todas formas, nosotros haremos el proceso de configuración en forma manual, sin hacer uso de este asistente.

ALGUNOS DISPOSITIVOS MODERNOS TIENEN UN ASISTENTE DE CONFIGURACIÓN

Tomamos como ejemplo un punto de acceso Linksys. Al ingresar, vemos la pestaña **Setup**, donde tenemos el nombre del dispositivo así como la dirección IP. No modificamos ningún valor y hacemos clic en la pestaña **Wireless**.

Ahora ingresamos los parámetros para nuestro punto de acceso:

- SSID: en esta sección debemos escribir el nombre que identificará a la red. En este caso usaremos **HOP3**.
- Wireless channel: se trata de la información sobre el canal con el que vamos a trabajar; lo cambiamos a 5.
- Wireless Network mode: en este parámetro vamos a usar la opción **G-only** para trabajar a mayor velocidad.



Figura 12. Podemos emitir nuestro SSID o no seleccionando **`Enable`** o **`Disable`** en la opción **`Wireless SSID Broadcast`**.

En la pestaña **Wireless Security** de la imagen anterior podemos configurar una contraseña de seguridad. Seleccionamos **WPA** o

WEP e ingresamos la clave deseada en el campo **WPA Shared Key**. Hacemos clic en el botón **Save Settings** (guardar configuración) para aplicar los cambios. El equipo se reinicia y ya habremos finalizado la configuración de nuestro punto de acceso.

Configuración del cliente (PC)

Para configurar nuestra computadora debemos ingresar a las propiedades del adaptador de red inalámbrico y usar una dirección IP estática. Podemos consultar el paso a paso de configuración de una IP estática visto en este capítulo, para refrescar los conocimientos.

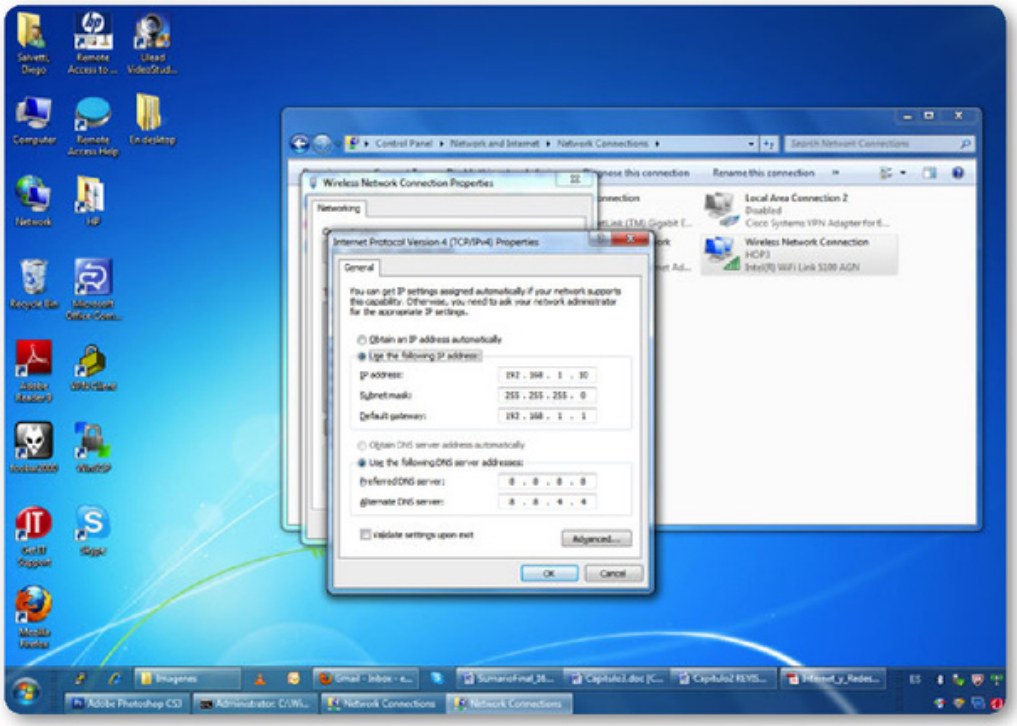


Figura 13. Recordemos que podemos usar cualquier servidor de DNS. Nuestro ISP puede facilitarnos esos datos.

Accedemos al **Centro de redes y recursos compartidos** y hacemos clic en **Cambiar configuración del adaptador**. Vamos a las propiedades de nuestra placa de red inalámbrica. Hacemos doble clic en el **Protocolo de Internet versión 4** (TCP/IPv4) para ingresar directamente a sus propiedades. Vamos a escribir la dirección IP (si es que no lo realizamos aún), y la

máscara de subred aparecerá automáticamente. En esta oportunidad es necesario ingresar la **Puerta de Enlace** (**Default Gateway**), así como los servidores de DNS (en este caso estamos usando los DNS públicos de Google). La Puerta de Enlace es la dirección IP de nuestro punto de acceso (192.168.1.1, según el ejemplo que venimos siguiendo), que es el dispositivo que conecta y encamina el tráfico de datos entre dos redes. Con esto le estamos diciendo a nuestra placa de red inalámbrica que envíe la información a nuestro punto de acceso. Para terminar, hacemos clic en la opción denominada **Aceptar**.



RESUMEN

Vimos varios temas en este capítulo. Primero hablamos del hardware necesario, y podemos concluir que el principal punto para tener en cuenta en esta instalación es determinar si el producto es soportado por el sistema operativo. Al utilizar Windows, tenemos la ventaja de que casi todos los proveedores diseñan los productos para trabajar con este sistema operativo. Detallamos la gran mayoría de las opciones del protocolo TCP/IP en lo que respecta a configuración para nuestra red. Además, realizamos configuraciones entre computadoras, implementando dos modos diferentes: Infraestructura y ad hoc. En este último, configuramos la red para compartir la conexión a Internet.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Cuáles son las dos situaciones a las que debe prestar especial atención cuando está por instalar el cliente inalámbrico?
2. ¿Cuáles son las tres formas que se describen en el texto para instalar los drivers de la placa inalámbrica?
3. ¿De qué manera práctica se identifican los zócalos de expansión en un motherboard?
4. ¿Qué se evita usando una pulsera antiestática cuando se abre el gabinete?
5. ¿De qué forma puede ver información básica de las redes inalámbricas disponibles?
6. ¿Cómo se llaman las direcciones IP que pueden cambiar cuando nos reconectamos a una red?
7. ¿Dentro de qué tipo de red se configuran las direcciones IP privadas?
8. ¿Qué información se obtiene al ejecutar el comando ipconfig en una consola?
9. ¿Por qué razón querría cambiar los servidores de DNS y usar DNS públicos y gratuitos?
10. Si quiere compartir temporalmente archivos entre dos computadoras, ¿qué tipo de red configurará, ad hoc o Infraestructura?

ACTIVIDADES PRÁCTICAS

1. Abra una consola y ejecute el comando ipconfig. Identifique los diferentes parámetros de su red inalámbrica y cableada.
2. En la misma consola ejecute ipconfig/release, luego ipconfig/renew y compare los nuevos valores con los del ejercicio 1.
3. Configure una IP estática para su placa de red inalámbrica. Cambie la opción para obtener una dirección automáticamente por DHCP.
4. Consulte algunos de los sitios que fueron recomendados para averiguar su IP pública y compare los resultados.
5. Configure una red ad hoc entre dos computadoras.

*04

Seguridad en la red

Estudiaremos los principales conceptos sobre seguridad informática; partiremos de nociones básicas y nos focalizaremos en la rama que se relaciona con la seguridad en redes inalámbricas. Analizaremos la importancia de la confidencialidad de nuestros datos. Además, aprenderemos qué significan los conceptos de autenticidad, integridad, disponibilidad y no repudio.

- Seguridad inalámbrica 94
- Seguridad de la información + WLAN 96
- Atributos de seguridad 97
- Confidencialidad en WLAN 98
- Autenticación en redes inalámbricas 105
- Integridad de datos en WLAN 109
- Disponibilidad en WLAN 111
- Las 10 amenazas más comunes 113
- Resumen 115
- Actividades 116

Seguridad inalámbrica

El uso del aire como medio para transmitir información mediante la propagación de ondas electromagnéticas deja al descubierto nuevos riesgos de seguridad. Si estas ondas de radio salen del recinto donde está instalada la red inalámbrica, nuestros datos quedarán expuestos ante cualquier persona que pase caminando. De esta forma, estos posibles **intrusos** tendrían acceso a nuestra información privada con solo poseer una notebook, netbook o, tal vez, algún teléfono celular con conexión WiFi (smartphone).

Además de esto, existen otros riesgos derivados de esta posibilidad. Por ejemplo, se podría realizar un ataque a la red por **inserción** (veremos esto luego en detalle) de un usuario no autorizado o haciendo uso de un punto de acceso ilegal más potente que capte los clientes inalámbricos en vez del punto de acceso legítimo. De este modo, se estaría interceptando la red inalámbrica.

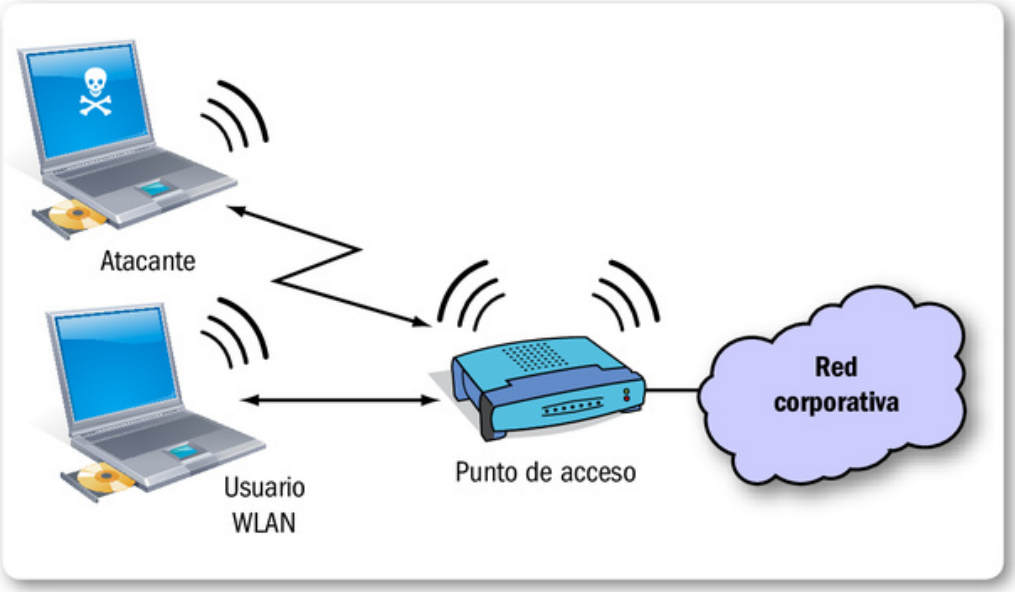


Figura 1. El atacante de una red inalámbrica tiene en sus manos información privada que no le pertenece al ingresar a nuestra red.

También es posible crear interferencias y una más que posible caída o denegación del servicio con solo introducir un dispositivo que emita ondas de radio en la misma frecuencia de trabajo de nuestra red.

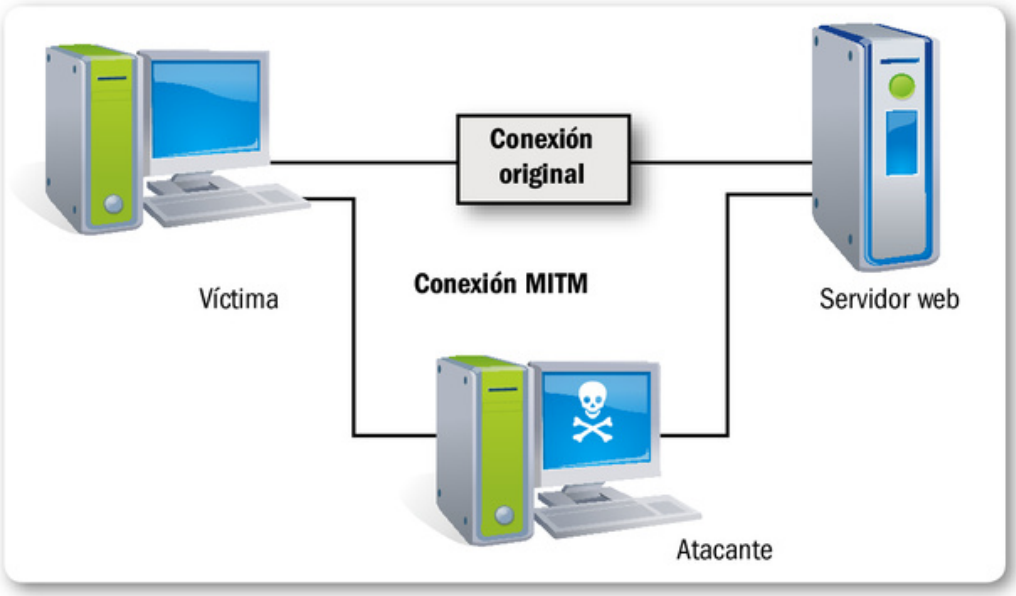


Figura 2. El esquema muestra cómo el atacante recibe la información que intercambian las víctimas sin que estas se den cuenta.

En caso de tener una red donde no se utilice el punto de acceso (como es el caso de las redes ad hoc), la posibilidad de comunicación entre clientes inalámbricos permitiría al intruso atacar directamente a un usuario de la red. Así, podríamos tener problemas si el cliente ofreciera servicios o compartiera archivos en la red. Algo muy utilizado también es la posibilidad de duplicar las direcciones IP o MAC de clientes legítimos de la red.

De esta forma, vamos a tratar la **seguridad inalámbrica** ubicándola en el contexto de la **seguridad de la información**. Entonces, cuando hablamos de seguridad inalámbrica, estamos haciendo referencia a la **seguridad de información en redes inalámbricas**.

FIRMA ELECTRÓNICA

Tengamos en cuenta que los términos **firma digital y firma electrónica** se suelen usar como sinónimos, pero esto es incorrecto. Mientras que firma digital hace referencia a una serie de métodos criptográficos, firma electrónica es un concepto de naturaleza legal y más amplia desde un punto de vista técnico. Esto es porque puede contemplar métodos no criptográficos.

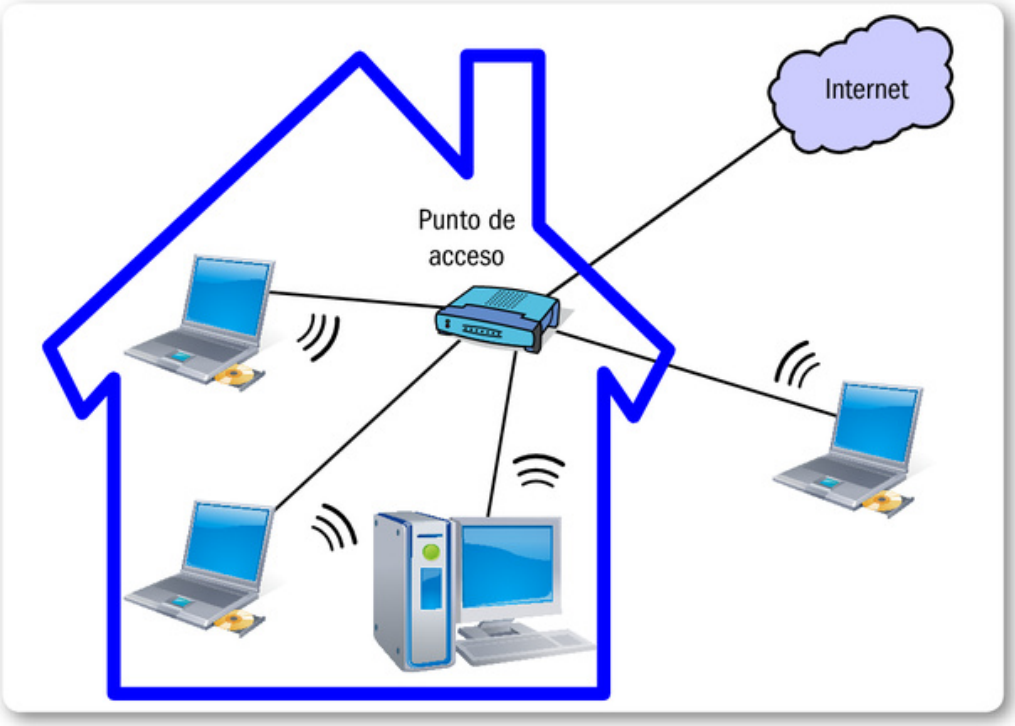


Figura 3. El enfoque de seguridad nos dará las pautas para proteger la información intercambiada sin cables y evitar a los intrusos.

Seguridad de la información + WLAN

El concepto de seguridad de sistemas de información se define como la protección de los sistemas de información contra el acceso no autorizado o la modificación de la información, ya sea que hablemos del medio donde almacenamos los datos, o de la etapa de procesamiento o tránsito. Además, se incluye la protección contra la negación de servicio a los usuarios autorizados o la provisión de servicio a usuarios no autorizados; y las medidas necesarias para detectar, documentar y contabilizar esas amenazas.

La seguridad inalámbrica se presentamos desde el punto de vista de la seguridad de los sistemas de información. Teniendo en mente

los cinco atributos de seguridad (confidencialidad, autenticación, integridad, no repudio y disponibilidad), podremos implementar y diseñar redes inalámbricas seguras.

Atributos de seguridad

De lo visto en capítulos anteriores, sabemos que el modelo de referencia OSI es una descripción abstracta para el diseño de protocolos de redes de computadoras. Este modelo divide las diferentes funciones de comunicación en siete capas que pueden funcionar de manera independiente una de otra.

Estas capas están **apiladas** e implican que cada una usa únicamente la funcionalidad de la inferior y provee funcionalidad exclusiva a la capa inmediata superior.

Tomemos un ejemplo: si consideramos la confidencialidad del tráfico de los datos entre dos puntos de acceso, podemos lograr resultados similares (proteger la información enviada) si actuamos en tres capas diferentes del modelo OSI:

- La Capa de Aplicación
- La Capa IP
- La Capa de Enlace (cifrado o encriptado de datos)

Cuando hablamos de seguridad inalámbrica, recordemos que solamente estamos examinando los mecanismos de seguridad en las capas 1 y 2, o sea, el nivel de Enlace. Otros mecanismos de seguridad de nivel 3 y superiores son parte de la seguridad implementada en las capas de Red o Aplicación.



EVADIR LA SEGURIDAD WEP

Para saltear la seguridad WEP se usan programas llamados **Packet Sniffers** y un **crackeador WEP**. El procedimiento consiste en capturar una cantidad determinada de paquetes en la red y luego, mediante el crakeador, romper el cifrado de la red. Un **key cracker** es un programa basado en matemáticas estadísticas que procesa paquetes capturados para descifrar la clave WEP.

Confidencialidad en WLAN

La confidencialidad en redes inalámbricas es asegurar que la información transmitida entre los puntos de acceso y los clientes no sea revelada a personas no autorizadas.

Nuestro objetivo es garantizar que la comunicación entre un grupo de puntos de acceso o bien entre un punto de acceso y un cliente esté protegida contra intercepciones.

¿Puedo usar WEP?

WEP (**Wired Equivalent Privacy**) y **WPA** (**WiFi Protected Access**) son los estándares usados por la mayoría de los dispositivos inalámbricos. Analizando estos dos estándares, WPA es muy superior en todos los aspectos y debemos usarlo siempre que sea posible.



Figura 4. En redes inalámbricas existen los métodos básicos de cifrado WEP y WPA, además de otras opciones.

De todas formas, todavía muchas personas o empresas utilizan la codificación WEP. Por esto, vale la pena que veamos este método de cifrado, además de sus funciones principales.

El cifrado WEP fue parte del estándar **IEEE 802.11** del año 1999. Su propósito era darles a las redes inalámbricas un nivel de seguridad comparable al de las redes cableadas tradicionales. La necesidad de un protocolo como WEP fue obvia, ya que las redes inalámbricas utilizan ondas de radio y son más susceptibles a ser interceptadas.

La vida de WEP fue demasiado corta: un diseño malo y poco transparente desencadenó ataques muy efectivos a su implantación. Algunos meses después de que WEP fuera publicado, se consideró este protocolo como obsoleto. Originalmente, usaba claves de codificación de 40 bits de longitud, que luego fueron extendidas a 104 bits por preocupación en los estándares de seguridad. Esto último, más que una solución, fue un arreglo realizado sobre la marcha, dado que las posibles combinaciones de claves eran muy pocas y los ataques de fuerza bruta no estaban previstos.

Como para tener una idea, hace unos años un grupo de investigadores logró romper una clave WEP de 104 bits en unos minutos usando una vieja computadora de escritorio con un procesador **Pentium-M** de 1.7 GHz.

Luego de WEP, nacen WPA y WPA2

WPA (Acceso Protegido WiFi) es un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias del sistema previo WEP. Luego de WEP, en el año 2003, se propone WPA como una medida intermedia para ocupar el lugar de aquel, y más tarde se certifica como parte del estándar IEEE 802.11i. Esto se realiza con el nombre de **WPA2** en el año 2004.

> WPA Y WPA2 SON PROTOCOLOS PARA TRABAJAR CON Y SIN SERVIDOR DE MANEJO DE CLAVES

WPA y WPA2 son protocolos diseñados para trabajar con y sin servidor de manejo de claves. WPA fue diseñado para utilizar un servidor de claves o autentificación (normalmente, un servidor **RADIUS**), que distribuye claves diferentes a cada usuario. Sin embargo, también se puede utilizar en un modo menos seguro de clave previamente compartida o **PSK** (**Pre-Shared Key**). Esto se destina para usuarios hogareños o de pequeña oficina. El modo PSK se conoce como WPA o **WPA2-Personal**.

Cuando se emplea un servidor de claves, a WPA2 se lo conoce como **WPA2-Corporativo** (o **WPA2-Enterprise**). La información es cifrada utilizando el algoritmo **RC4** (esto es debido a que WPA no elimina el proceso de cifrado WEP, solo lo fortalece), con una clave de **128 bits**.

Una de las mejoras sobre WEP es la implementación del Protocolo de Integridad de Clave Temporal o **TKIP** (**Temporal Key Integrity**

Protocol). Debemos tener en cuenta que este protocolo cambia claves dinámicamente a medida que el sistema es utilizado.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. La comprobación de redundancia cíclica o **CRC** (**Cyclic Redundancy Check**) utilizada en WEP es insegura, dado que se puede alterar la información CRC del mensaje sin conocer la clave WEP. En cambio, WPA implementa un código de integridad del mensaje **MIC** (**Message Integrity Code**), también conocido como **Michael**. Sumado a esto, WPA incluye protección contra **ataques de repetición** (**Replay Attacks**).

Al incrementar el tamaño de las claves y el número de claves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que el ingreso no autorizado a redes inalámbricas sea mucho más difícil.

Modos de funcionamiento de WPA

Repasaremos los modos de funcionamiento del protocolo WPA:

- **WPA-RADIUS** (acrónimo de **Remote Access Dial-In User Server**) es un protocolo de autenticación, autorización y administración (AAA) para aplicaciones de acceso a la red o movilidad IP.
  Un ejemplo común de uso de este tipo de servicio es cuando realizamos una conexión a un ISP con un módem DSL, cablemódem, Ethernet o WiFi. En este caso, se envía información (que generalmente es un nombre de usuario y contraseña) que, luego, llegará hasta un servidor de RADIUS sobre el protocolo **RADIUS**. Ahí se comprueba que la información sea correcta, si usamos esquemas de autenticación. Si es aceptado, el servidor autoriza el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros para que podamos navegar sin problemas.



DIFICIL SÍ, PERO NO IMPOSIBLE

Si pensamos que por tener una contraseña **WPA-PSK** en la red vamos a estar a salvo de terceras personas que quieran infiltrarse, estamos equivocados. Utilizando **diccionarios de palabras** y tiempo, podemos descubrir la clave al usar un ataque de fuerza bruta. Los diccionarios incluyen palabras que son comúnmente usadas como claves.

Recordemos que con este tipo de servicio estamos permitiendo que las organizaciones puedan centralizar su autentificación, autorización y administración.

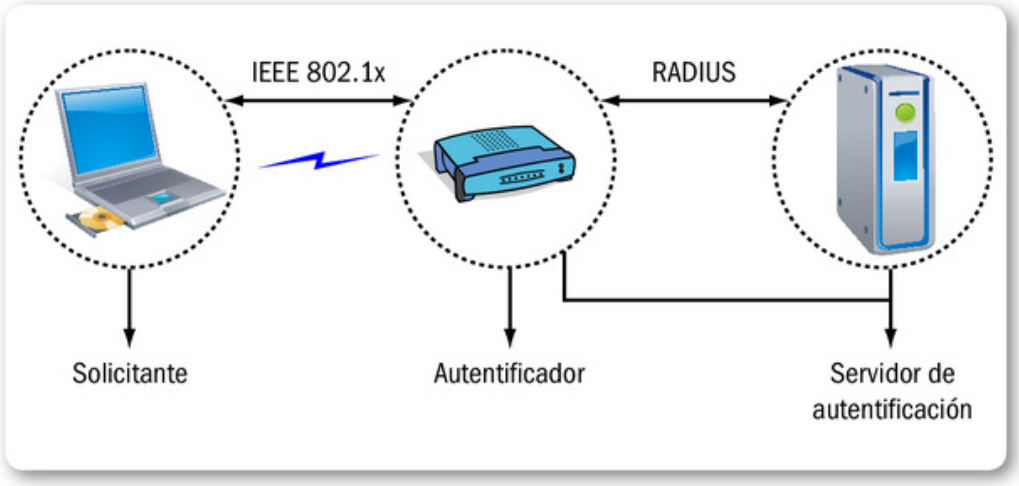


Figura 5. Ejemplo de una red inalámbrica donde hacemos uso de WPA-Radius. Podemos identificar las entidades que actúan.

Vamos a ver un poco más en detalle todo esto. Para continuar, definimos tres tipos de entidades:

- **Solicitante**: es el cliente inalámbrico.
- **Autentificador**: es el intermediario entre el cliente inalámbrico y el servidor de autentificación.
- **Servidor de autenticación**: es un sistema que guarda la información relacionada con los usuarios y con las autenticaciones.

EL SERVIDOR DE AUTENTICACIÓN GUARDA DATOS SOBRE USUARIOS Y AUTENTICACIONES

Describamos el proceso de autenticación para este modo de funcionamiento de WPA. Veamos en un gráfico cómo se realiza este proceso; además, mostremos a modo informativo los mensajes que se intercambian para concretar la autenticación.

Debemos tener en cuenta que los protocolos que aparecen y no tratamos en este texto no los consideramos como fundamentales para el objetivo de este libro y por esa razón no los desarrollamos en profundidad.

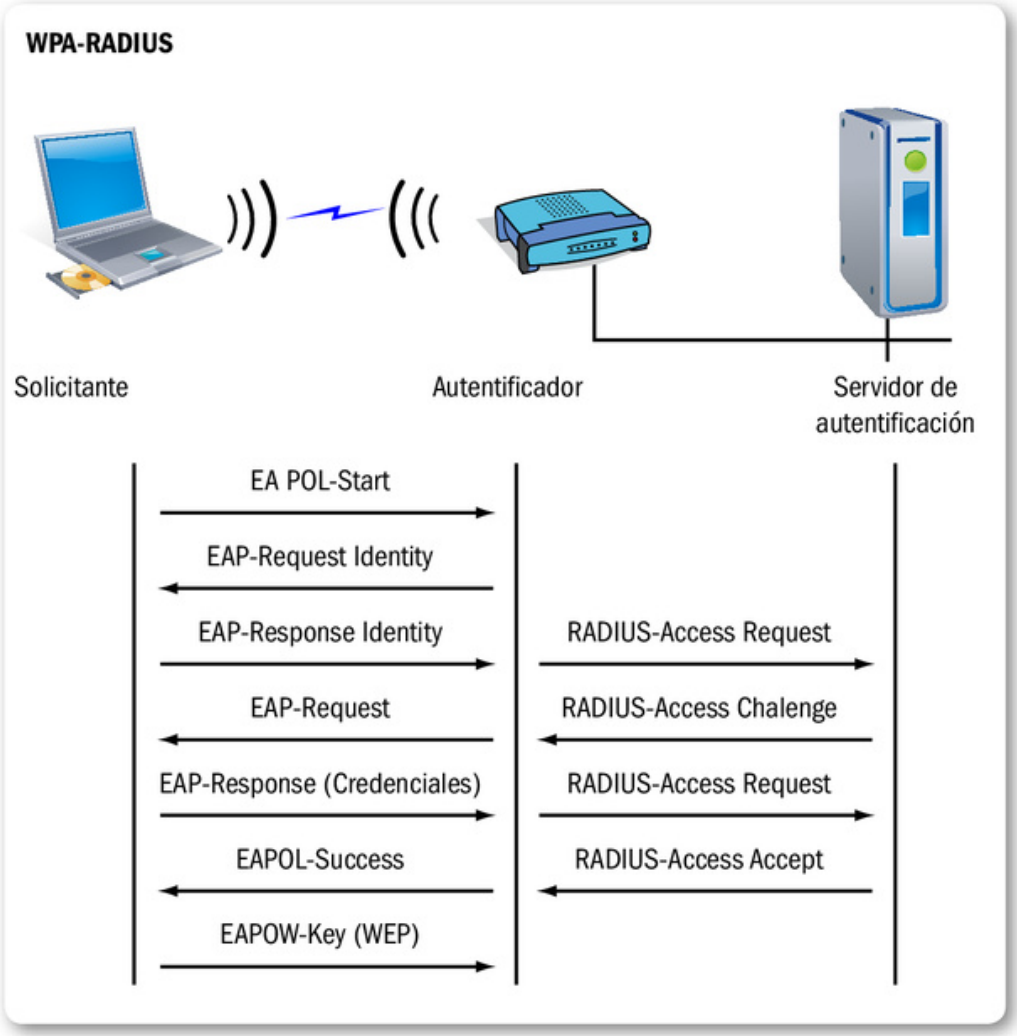


Figura 6. Ejemplo de una red inalámbrica donde hacemos uso de WPA-Radius. Podemos identificar los protocolos que actúan.

1) El solicitante, un cliente inalámbrico de nuestra red que quiere ser autenticado, envía una petición al autentificador.
2) El autentificador, punto de acceso, habilita un puerto de comunicación para el solicitante.
3) Por este puerto solo pueden viajar mensajes de autenticación en tramas de gestión (paquetes de información que se envían para realizar tareas específicas). El resto del tráfico no se tiene en cuenta.
4) El autentificador pide la identidad encapsulada al solicitante mediante el protocolo **EAPOL** (EAP **Encapsulation over LANs**).
5) El solicitante envía su identidad al autentificador.

6) El punto de acceso manda la identidad del cliente al servidor de autenticación mediante **EAP** (Extensible Authentication Protocol).
7) El cliente y el servidor de autenticación establecen un diálogo mediante el protocolo EAP.
8) Finalizado este diálogo, el solicitante y el servidor de autenticación comparten una clave de sesión que nunca ha viajado por la red.
9) El servidor de autenticación envía la clave de sesión al autentificador mediante el protocolo RADIUS.
10) El punto de acceso habilita el puerto para la dirección MAC del dispositivo solicitante y, adicionalmente, establece una clave de encriptación con el solicitante.

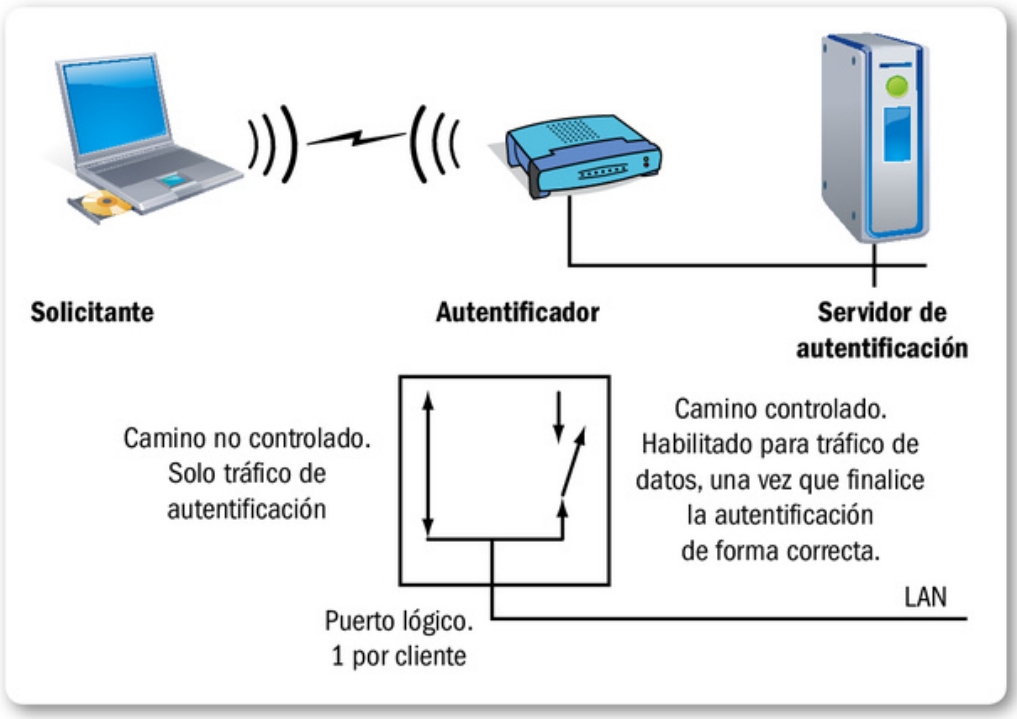


Figura 7. Esquema equivalente en el proceso de autenticación si usamos WPA-Radius; se ve el acceso o no acceso con una llave.

- **WPA-PSK** (Pre Shared Key)
  Destinado para entornos en los que no hay disponible un servidor de autenticación y en los cuales no es necesario llegar al mismo nivel de seguridad que el usado en las comunicaciones corporativas. En este punto podemos hacer uso de este modo en nuestros

hogares, oficinas pequeñas o en lugares donde la seguridad no es un tema demasiado importante.

El principio de funcionamiento se basa en una clave compartida por todos los dispositivos involucrados en la comunicación (por ejemplo, clientes inalámbricos y AP) llamada **Pre Shared Key**, **password** o **master key**. La gestión de esta clave es manual en todos los equipos, y no hay un mecanismo estándar para modificar esta clave secreta compartida.

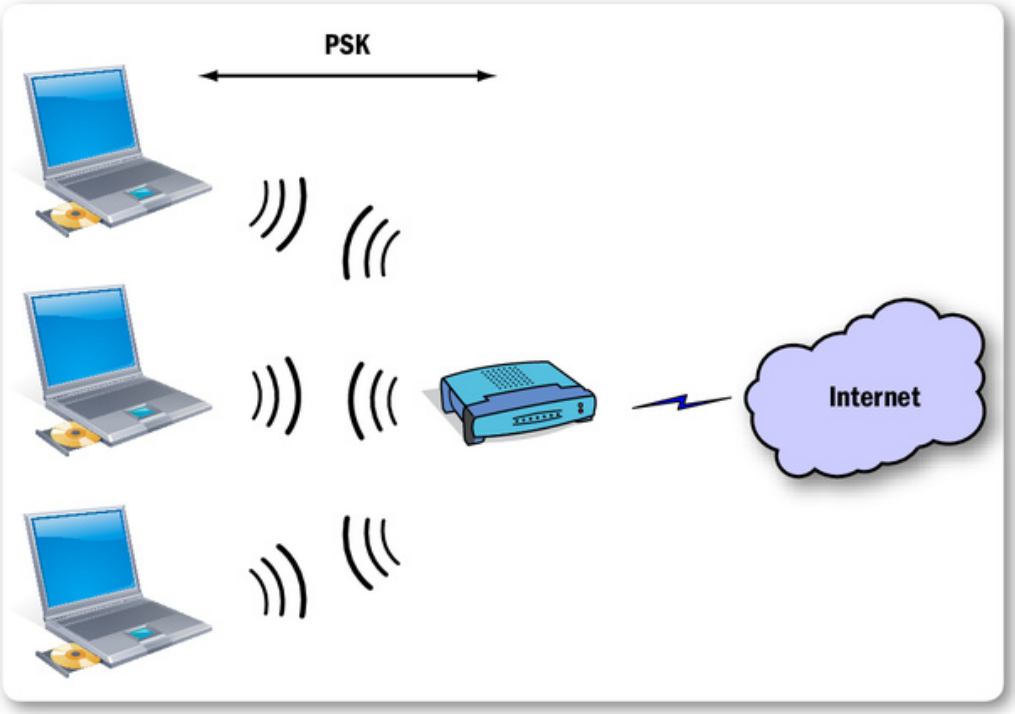


Figura 8. Pasar de WEP a WPA-PSK en una red supone, simplemente, actualizar el firmware correspondiente.

Modos de funcionamiento de WPA2

El protocolo WPA2 está basado en el estándar 802.11i. WPA. Por ser una versión previa, que se podría considerar de migración, no incluye todas las características del **IEEE 802.11i**. Así, recordemos que podemos afirmar que **WPA2** es la versión certificada del estándar 802.11i. La Alianza WiFi llama a la versión de clave precompartida **WPA-Personal** y **WPA2-Personal**, y a la versión con autenticación

RADIUS (también la podemos encontrar como autenticación **802.1x/EAP**), como **WPA-Enterprise** y **WPA2-Enterprise**.

Los fabricantes manufacturan productos basados en el protocolo WPA2 que utiliza el algoritmo de cifrado **AES**.

Con este algoritmo es posible cumplir con los requerimientos de seguridad impuestos por algunos gobiernos.



Autenticación en redes inalámbricas

En nuestras redes inalámbricas la autenticación es la medida diseñada para establecer la validez de una transmisión entre puntos de acceso de la red y/o clientes inalámbricos. Dicho de otra forma, la autenticación inalámbrica significa tener el derecho de enviar hacia y mediante el punto de acceso.

Para facilitar la comprensión del concepto de **autenticación** en redes inalámbricas, vamos a explicar qué es lo que sucede en el inicio de la sesión de comunicación entre un AP y un cliente inalámbrico. El inicio de una comunicación empieza por un proceso llamado **asociación**.

Existen dos mecanismos de asociación que fueron agregados al estándar IEEE 802.11b al momento de diseñarlo:

- Autenticación abierta
- Autenticación con llave compartida

Tengamos en cuenta que la **autenticación abierta** significa no tener seguridad; entonces, cualquier cliente inalámbrico puede hablarle al punto de acceso sin necesidad de identificarse durante el proceso. De



esta forma, cualquier cliente, independientemente de su clave WEP, puede verificarse en el punto de acceso y luego intentar conectarse (esto es, por ejemplo, ingresando la contraseña cuando se solicita identificarse).

En cambio, en la **autenticación de llave compartida**, se comparte una contraseña entre el punto de acceso y el cliente de la red inalámbrica. Un mecanismo de confirmación/denegación le permite al punto de acceso verificar que el cliente conoce la llave compartida y, entonces, le concede el acceso.

La autenticación con llave compartida implementada en el protocolo **WEP** también es obsoleta. Existen varios ataques de tipo texto plano versus texto cifrado con los cuales se puede vulnerar la autenticación basada en WEP. Esto es porque la llave de cifrado y autenticación son el mismo secreto compartido; entonces, una vez que una resulta comprometida, la otra también.

Evitar difundir la SSID

Existe una variación del esquema de autenticación abierta llamada **Red cerrada** o **CNAC** (**Closed Network Access Control**), desarrollada por **Lucent Technologies** en el año 2000. Las redes cerradas se diferencian del estándar 802.11b en que el punto de acceso no difunde periódicamente las llamadas **Tramas Baliza** (**Beacom Frames**). De esta forma, evitamos la publicación de la SSID. Esto implica que los clientes de la red inalámbrica necesitarán saber de manera previa qué SSID tienen que asociar con un punto de acceso. Esto fue considerado por muchos fabricantes de equipo como una mejora de seguridad. Mientras que detener la difusión del **SSID** previene a los clientes de enterarse del SSID por medio de una trama baliza, nada nos asegura que otro cliente con un programa de intercepción detecte la asociación que provenga de otro punto de la red.



CIFRADO PESADO

Cuando realizamos **cifrado** o **encriptado** a nivel de enlace, estamos usando mayor cantidad de recursos de **hardware** en los puntos de acceso de la red por donde pasa la información. Además, se requieren medidas especiales de seguridad en la administración y la distribución de claves.

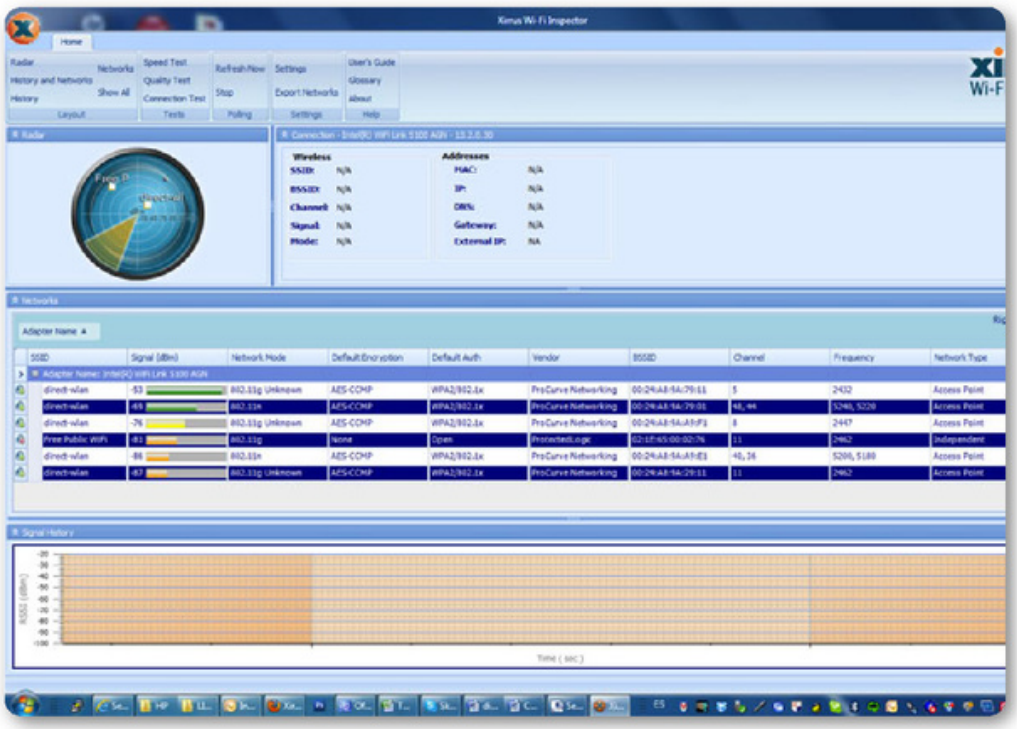


Figura 9. El programa Wi-Fi Inspector nos permite monitorear las redes cercanas aunque la SSID no sea visible a simple vista.

Filtrar direcciones MAC

Conocido como **Filtrado por MAC** o **Lista de control de acceso ACL** (**Access Control List**), es un método mediante el cual solo se permite unirse a la red a aquellas direcciones físicas (MAC) que estén dadas de alta en una lista de direcciones permitidas. Como sabemos, este filtrado permite hacer una lista de equipos que tienen acceso al AP, o bien denegar ciertas direcciones **MAC**.

Se ha convertido en una práctica común usar la dirección MAC de la interfaz inalámbrica como un mecanismo de seguridad. Existen dos realidades: una para el usuario común con pocos conocimientos, que piensa que las direcciones MAC son únicas y no pueden ser modificadas por cualquiera; debemos saber que la otra realidad más fuerte es que las direcciones MAC en casi cualquier red inalámbrica pueden ser fácilmente modificadas o **clonadas** por usuarios que posean un nivel de conocimientos algo avanzaod, de modo de obtener una MAC de una entrada válida en el punto de acceso.

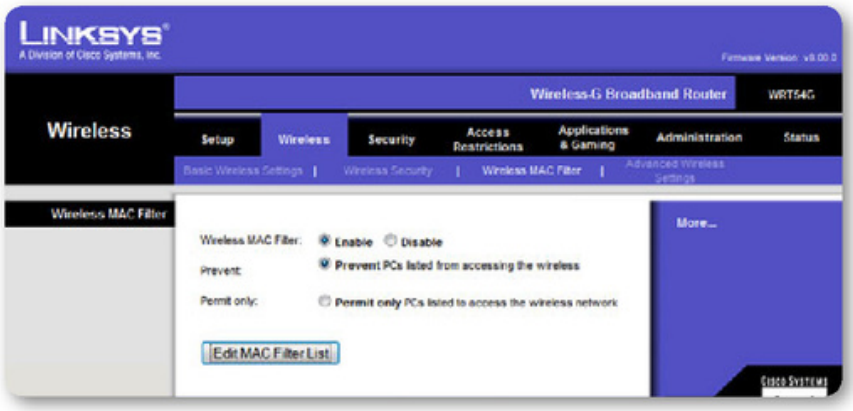


Figura 10. En las opciones del punto de acceso podemos habilitar el filtrado MAC y editar la lista de usuarios permitidos.

Portal cautivo

También llamado **portal captivo**, es un software o hardware en una red que tiene como objetivo vigilar el tráfico **HTTP** (protocolo usado en Internet). Además, obliga a los usuarios de la red a pasar por una página web especial si es que quieren navegar por Internet.

Solo haremos una pequeña introducción a este tema, ya que necesitaríamos varias páginas para desarrollar los portales cautivos. Veamos cómo es el funcionamiento.

En una red donde la autenticación se realiza mediante este sistema, a los clientes se les permite asociarse a un punto de acceso (sin autenticación inalámbrica) y obtener una dirección IP con DHCP (no hace falta autenticación para obtener esta dirección). Cuando el cliente tiene la IP, todas las solicitudes HTTP se capturan y se envían al portal cautivo. Así, el cliente es forzado a identificarse en una página web.

Los portales cautivos son responsables de verificar la validez de la contraseña y luego modificar el acceso del cliente.

En el primer paso (1), se solicita una asociación del cliente a la red inalámbrica, se anuncia la SSID en general y no se requiere autenticación (WEP o WPA). En el segundo paso (2), el cliente obtiene una dirección IP mediante el protocolo DHCP. En el paso final (3), el tráfico HTTP del cliente se redirecciona al servidor del portal cautivo. El cliente se identifica con usuario y contraseña, y si los datos son válidos, se permite el tráfico hacia Internet.



Figura 11. Esquema de funcionamiento de un **`portal captivo`** con la autenticación correspondiente en tres pasos.

Integridad de datos en WLAN

Si un protocolo inalámbrico puede asegurarnos que la información transmitida no ha sido alterada por personas no autorizadas, entonces el protocolo cumple con la integridad de datos.

Es interesante tener en cuenta que en los primeros años, WEP intentaba cumplir con esta premisa a rajatabla. Desafortunadamente, el mecanismo de integridad implementado, llamado **CRC** (cuya sigla significa **código de redundancia cíclica**), resultó completamente inseguro. Utilizar un mecanismo inseguro permite que el tráfico de información sea alterado sin que se note.

PORTALES CAUTIVOS EN LA PC

Los portales cautivos se usan, sobre todo, en lugares con redes públicas (plazas, hospitales, etc.). El objetivo es mostrar un mensaje de bienvenida y, además, informar las condiciones de acceso. Podemos montar nuestro propio portal cautivo para Windows en nuestra PC. Una solución es FirstSpot: **http://patronsoft.com/firstspot**.

Luego, los protocolos WPA y WPA2 resolvieron el problema de la integridad de datos que poseía WEP agregando un mensaje de código de autenticación más seguro. Además de un contador de segmentos, que previene los **ataques por repetición** (**replay attack**, o también llamados ataques de reinyección).

En estos **ataques de repetición**, el atacante registra la conversación entre un cliente y el AP para así obtener un acceso no autorizado. La información capturada por el atacante es luego reenviada con el objetivo de falsificar la identidad del usuario que posee acceso a la red.

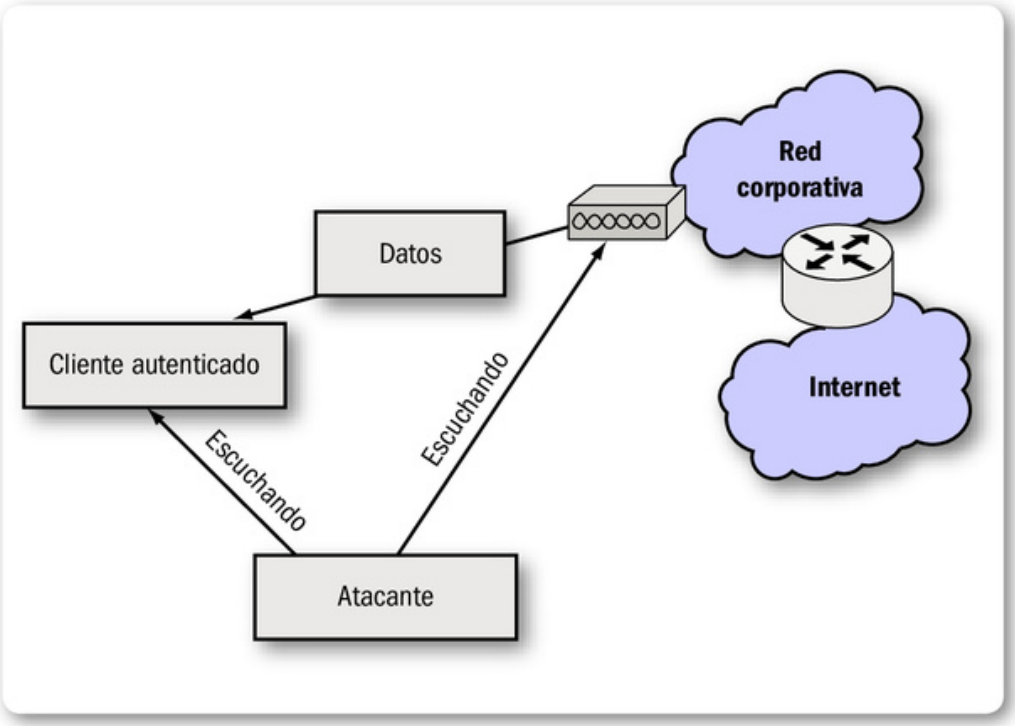


Figura 12. En un ataque de reinyección, el atacante espera de forma silenciosa hasta obtener información útil.

CLUSTER DE ALTA DISPONIBILIDAD

Un cluster de alta disponibilidad es un conjunto de dos o más computadoras que se caracterizan por mantener una serie de servicios compartidos y constantemente monitorizándose entre sí. En general, se dividen en dos clases: alta disponibilidad de infraestructura o alta disponibilidad de aplicación.

Debemos recordar que la integridad de datos mediante WEP es obsoleta. Recomendamos implementar WPA o WPA2 para lograr integridad de datos en una red inalámbrica.

WPA Y WPA2

MODO / CIFRADO		WPA	WPA2
Modo corporativo	**Autenticación**	IEEE 802.1X /EAP	IEEE 802.1X /EAP
	Cifrado	TKIP/MIC	18 Mp
Modo personal	**Autenticación**	PSK	PSK
	Cifrado	TKIP/MIC	AES-CCMP

Tabla 1. Resumen de autenticación y cifrado en WPA y WPA2, en los modos denominados corporativo y personal.

Disponibilidad en WLAN

Tener una red donde se asegure un acceso confiable a servicios de datos e información para usuarios que están autorizados es poseer **disponibilidad** en ella.

Debemos considerar que las redes inalámbricas trabajan en canales predefinidos, que cualquiera puede usar para enviar información. No es simple detener a alguien que busca interferir con su señal de radio nuestra red. Lo único que podemos hacer es **monitorear** cuidadosamente la red para identificar fuentes potenciales de interferencia (por ejemplo,

WEP Y SU ALGORITMO

WEP está basado en el algoritmo de cifrado llamado **RC4**. Las implementaciones de este algoritmo en el estándar IEEE 802.11 se consideran inadecuadas, ya que existen ataques para romper el cifrado WEP. Algunos ataques se basan en la limitación numérica de los **vectores de inicialización** del algoritmo RC4.

una red de un vecino que opera en el mismo canal que nosotros).

La negación de servicio mediante interferencia de radio es algo común en redes inalámbricas. Por ejemplo, imaginemos si el vecino, además de tener su red configurada en el mismo canal que la nuestra, decide usar el mismo SSID. Para evitar esta clase de ataques, intencionales o no, debemos realizar un rastreo diario de frecuencias de radio. Si deseamos evitar interferencias con otras redes, no usemos demasiada potencia en el punto de acceso.

Otras razones por las cuales nuestra red se puede desempeñar de manera deficiente o no estar disponible son los clientes con **virus**, **programas de intercambio de archivos** (P2P), **spam**, etc. Todo esto puede inundar nuestra red con tráfico y dejar menos ancho de banda disponible para los usuarios.

Debemos tener en cuenta que la disponibilidad en redes inalámbricas necesita de buenas prácticas de monitoreo.

No repudio en redes inalámbricas

Los protocolos inalámbricos existentes carecen de un mecanismo para asegurar que el emisor de la información tenga una prueba de envío de esta y que el receptor obtenga una prueba de la identidad del emisor. Los estándares 802.11 no se hacen responsables de la rendición de cuentas en el tráfico de datos. Esta rendición de cuentas debe ser implementada por protocolos de capas superiores en el modelo OSI.



WPA VS. WPA2

WPA2 es la versión certificada de WPA y es parte del estándar IEEE 802.11i. Al referirnos a esta versión, es importante destacar que hay dos cambios principales: por un lado, el reemplazo del algoritmo **Michael** por un código de autenticación conocido como **CCMP** (Counter mode/CBC mode), que es criptográficamente seguro; y por otra parte, el reemplazo del algoritmo RC4 por el AES (Advanced Ecryption Standard), también conocido como **Rijndael**.

Las 10 amenazas más comunes

Repasemos los tipos de ataque más relevantes que existen:

- **Ataque de intromisión**: es cuando alguien abre archivos en nuestra computadora hasta encontrar algo que sea de su interés. Esta persona puede o no tener acceso autorizado, y no necesariamente tiene que ser alguien externo (puede ser alguien que convive todos los días con nosotros). En las empresas es muy común que el ataque se realice desde adentro por parte de un empleado.
- **Ataque de espionaje en líneas**: se da cuando alguien escucha la conversación y no está invitado a ella. Es muy común este ataque en redes inalámbricas. Prácticas como el **Wardriving** (método de detección de una red inalámbrica) hacen uso de este ataque.
- **Ataque de intercepción**: se desvía la información a otro punto que no sea el destinatario. De esta manera, se puede revisar la información y el contenido de cualquier flujo de red.
- **Ataque de modificación**: en este ataque se altera la información que se encuentra en computadoras o bases de datos. Es muy común este tipo de ataque en bancos.
- **Ataque de denegación de servicio**: como ya dijimos, en este tipo de ataques se procede a negar el uso de los recursos de la red a los usuarios que se conectan de modo legítimo.
- **Ataque de suplantación**: este tipo de ataque se dedica a dar información falsa, a negar transacciones y/o hacerse pasar por otro usuario conocido. Un ejemplo es el uso de portales falsos en sitios de bancos donde las personas ingresan, por ejemplo, los datos de tarjetas de crédito que luego serán vaciadas por los atacantes.

Remarquemos que estos ataques, así como se realizan en medios electrónicos, también pueden ejecutarse en medios físicos (como expedientes, archivos, papeles con información confidencial, etc.). En general, los ataques a computadoras se inician con información que ha sido obtenida de una fuente física.

En la tabla siguiente veremos las diez **amenazas de seguridad** más relevantes en redes inalámbricas y plantearemos de forma sintética recomendaciones a seguir para cada una de ellas.

AMENAZAS			
N°	PARÁMETRO	DESCRIPCIÓN DE AMENAZA	POSIBLE SOLUCIÓN
1	**Confidencialidad**	Riesgo de interferencia, usuarios no autorizados pueden obtener acceso al tráfico de datos en su red.	Usar cifrado WPA2. Recomendar a los usuarios el uso de cifrado en protocolos de nivel superior.
2	**Confidencialidad**	Riesgo de robo de tráfico y riesgo de un ataque tipo intercepción.	Usar cifrado WPA2. Monitorear la señal inalámbrica, la SSID y la MAC de conexión.
3	**Autenticación**	Riesgo de acceso no autorizado a su red inalámbrica.	Implementar WPA2. No depender solo de un esquema de autenticación basado en MAC. No publicar la SSID.
4	**Autenticación**	Riesgo de acceso no autorizado a su red inalámbrica y a Internet.	Implementar IEEE 802.1X. Implementar un portal cautivo.
5	**Integridad**	Riesgo de alteración de tráfico en la red inalámbrica.	Recomendar a los clientes el uso de cifrado en capas superiores. Usar WPA2.
6	**Disponibilidad**	Riesgo de interferencia. Negación de servicio (congestionamiento).	Monitorear diariamente el espectro de radio. No sobrecargar de potencia los enlaces.
7	**Disponibilidad**	Riesgo de no disponibilidad de ancho de banda debido a retransmisiones de radio.	Buscar fuentes de interferencia ocultas que pueden estar cerca.
8	**Disponibilidad**	Riesgo de no disponibilidad de ancho de banda debido a software malicioso.	Monitorear el tráfico IP, especialmente el ICMP e IP. Incluir detectores de intrusión IDS.
9	**Autenticación Rendición de cuentas**	Riesgo de acceso no autorizado a su red interna.	Implementar la red inalámbrica fuera del firewall.
10	**(Acceso a la red) Rendición de cuentas**	Riesgo de uso no autorizado de recursos de la red.	Implementar un portal cautivo basado en firmas digitales.

Tabla 2. Las 10 amenazas de seguridad más importantes.

- **IDS**: se trata de un sistema detector de intrusos (**Intrusion Detection System**) cuya función es detectar tráfico sospechoso y reaccionar enviando alarmas o reconfigurando dispositivos para tratar de finalizar conexiones.
- **Firewall**: dispositivo (hardware o software) que se sitúa entre dos redes de distinto nivel de seguridad (normalmente una red interna y una externa como Internet). Analiza todos los datos que transitan entre ambas redes y filtra (bloquea) los que no deben ser reenviados según reglas preestablecidas.



RESUMEN

En este capítulo presentamos la seguridad inalámbrica desde el punto de vista de la seguridad de los sistemas de información. Esto nos llevó a ver los cinco atributos de seguridad existentes: confidencialidad, autenticación, integridad, disponibilidad y no repudio. Además, dado que la formulación de los estándares inalámbricos (como el IEEE 802.11) solo hace referencia a las capas 1 y 2 del modelo OSI, algunos atributos de seguridad pueden ser implementados por protocolos de capas superiores. En la parte final, resumimos los diferentes tipos de ataques que existen y las 10 amenazas a las que podemos estar expuestos en nuestra red.

Actividades

TEST DE AUTOEVALUACIÓN

1. Si se carece de medidas de seguridad en una red, ¿de qué forma puede quedar expuesta la información frente a intrusos?
2. ¿Cuáles son las tres formas que se describen en el texto para instalar los drivers de una placa inalámbrica?
3. ¿Cómo es posible mejorar las políticas de seguridad planteadas?
4. ¿Qué garantiza la autenticación?
5. ¿Qué se entiende por cifrado o codificación a nivel de enlace?
6. ¿Cuáles fueron las fallas o errores que provocaron la obsolescencia del protocolo WEP?
7. ¿Cuáles son los modos en que puede usarse el protocolo WPA/WPA2?
8. ¿Es conveniente dejar de difundir el SSID para incrementar la seguridad de la red?
9. ¿Cuál es el nombre del mecanismo de integridad implementado en WEP que resultó totalmente inseguro?
10. ¿En qué consiste el ataque por repetición?

ACTIVIDADES PRÁCTICAS

1. Verifique el nivel de seguridad en una red inalámbrica.
2. Identifique el algoritmo de protección que utiliza la red.
3. Cambie el SSID de la red inalámbrica.
4. Reemplace el cifrado WEP por WPA2.
5. Verifique las amenazas más comunes en su red de datos.

*05

Resolver problemas

En este capítulo nos adentraremos en la resolución de los problemas de nuestra flamante red inalámbrica. Si bien puede existir una variedad de dificultades, trataremos de enfocarnos en un método que nos ayudará a identificar qué ocurre cuando se presenta un problema en la red.

- **Enfoque metodológico 118**
- **Pasos fundamentales para verificar 120**
  - Actualizaciones 124
- **Nuestro método 124**
  - Delimitar el problema 125
  - Encerrar la causa del problema 126
  - Planear la solución 127
  - Corroborar los resultados 134
  - Documentar los resultados 135
  - Caso práctico 136
- **¿Qué herramientas usar para resolver problemas? 138**
  - Escenarios prácticos 140
- **Resumen 143**
- **Actividades 144**



↗↗↗

Enfoque metodológico

Basándonos en el modelo OSI, que venimos estudiando desde el primer capítulo, analizaremos capa por capa en busca de la causa de un problema. Recordemos que el modelo OSI divide las funciones necesarias para realizar la comunicación en siete capas que pueden ejecutar sus funciones de manera independiente una de otras. Al tener los servicios **segmentados** en capas, la resolución del problema será más fácil y rápida que si utilizamos otro método.

También necesitaremos conocer de qué forma es posible controlar las potenciales dificultades de la red; por este motivo, presentaremos algunas herramientas para **monitorear y diagnosticar** inconvenientes. Si enfrentamos una complicación en nuestra red con un plan, la causa y la posible solución van a ser más simples de detectar e implementar.

Capa	OSI	TCP/IP
7	Aplicación	Aplicación
6	Presentación	
5	Sesión	**Transporte (TCP)**
4	Transporte	
3	Red	**Red (IP)**
2	Enlace de datos	Control de acceso al medio
1	Física	

Figura 1. Recordemos con esta imagen los protocolos del modelo OSI versus TCP/IP, separados por capas.

Hacer un diagnóstico y resolver problemas de red tal vez sea una tarea enredada. Muchos técnicos o conocedores de redes pueden llegar a decir que es la actividad más difícil de su trabajo. De todas formas, no tenemos que temerles a los problemas que se presentan día a día en las redes. Si poseemos un **método** práctico y una buena dosis de paciencia, vamos a lograr resultados óptimos.

Una vez que hayamos realizado el diagnóstico del problema, la identificación de los recursos afectados y el camino que vamos a seguir para llegar a esos recursos, la corrección del problema será un paso

directo y sencillo. Debemos tener presente que, antes de dar el diagnóstico, debemos aislar la verdadera causa que originó el problema, de factores irrelevantes.



Figura 2. El navegador web Firefox de Mozilla nos brinda información en caso de un problema.

De la experiencia, podemos decir que resolver problemas de redes (tanto cableadas como inalámbricas) es más un arte que una ciencia exacta. Por este motivo. hay que atacar el conflicto de forma organizada y metódica, recordando que estamos buscando la causa, no síntomas.



Figura 3. Aplicaciones como Windows Live Messenger no dan información específica al momento de resolver un problema.

Pasos fundamentales para verificar

Antes de describir el método para resolver problemas, vamos a desarrollar un par de conceptos para tener en cuenta. Así, nos aseguraremos de que todos los dispositivos estén correctamente conectadas y funcionando, y de tener la última versión de firmware.

Tensión eléctrica estable

En los nuevos aparatos electrónicos que conforman nuestro equipamiento inalámbrico (puntos de acceso, placas inalámbricas y cámaras inalámbricas, entre otros), el hardware es exageradamente sensible a las oscilaciones que sufre la tensión eléctrica. Es decir, una interrupción o fluctuación de **tensión**, causada por un corte en el servicio eléctrico, una caída en la corriente o por alguna desconexión del equipo, puede producir daños a las partes del aparato inalámbrico.

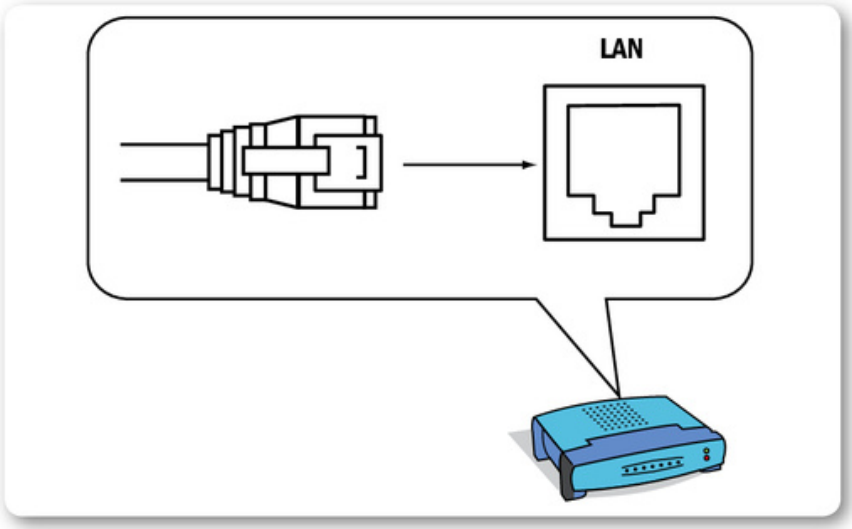


Figura 4. Recordemos que en el puerto Ethernet de nuestro AP conectamos el cable UTP con una ficha RJ-45.

Si nuestro punto de acceso sufre una interrupción de la energía en el momento en que se realiza la secuencia de arranque del equipo, la

memoria **Flash** interna (donde se carga el firmware) puede verse dañada. De este modo, el dispositivo puede quedar inutilizado.



Figura 5. Como sabemos, muchos dispositivos inalámbricos identifican el puerto a la red cableada con un color y la inscripción Ethernet.

Los **puertos Ethernet** (donde conectamos la red cableada con el punto de acceso) son otro punto sensible a daños si se producen anomalías en el servicio eléctrico.

Si bien la parte inalámbrica podría no verse afectada, el dispositivo quedaría inutilizado para vincular la red cableada o la salida a Internet (en caso de que tengamos solo un puerto Ethernet).

SIEMPRE POR CAPAS

Cuando nuestra red tiene problemas e identificamos que algo va mal, lo primero que necesitamos hacer es averiguar en qué capa está la dificultad. Además, si logramos confirmar la capa que es causante del inconveniente, entonces tendremos mayores chances de solucionarlo en menor tiempo.



Figura 6. Algunos fabricantes copian la parte estética de fuentes originales, pero debemos tener cuidado porque usan diferentes valores de tensión y corriente.

Es necesario tener en cuenta que es posible sufrir deterioros similares en la parte electrónica de nuestro equipo si usamos un transformador que no es el original o está defectuoso. Por esta razón, es importante conseguir repuestos originales, aunque para esto debamos invertir un monto de dinero más elevado.

Si alimentamos el punto de acceso, por ejemplo, con muy bajo y/o alto voltaje, corremos el riesgo de dañar el dispositivo. Recordemos que cada fabricante tiene su propio diseño.

USAR UPS O ESTABILIZADOR

Los equipos de una red inalámbrica son muy sensibles a los cambios en el sistema eléctrico; tengamos siempre en cuenta esto para no dañar los dispositivos. Evitaremos estar afectados por la inestabilidad del sistema eléctrico usando un **estabilizador de tensión** o un **sistema de alimentación ininterrumpida** (UPS, Uninterruptible Power Supply, en inglés).



Figura 7. Las fuentes de alimentación originales son las que proveen las tensiones y corrientes adecuadas.

En general, las fuentes de alimentación (**transformadores**) varían muy poco. Por eso, es muy fácil confundirse con otros dispositivos y usar un transformador inadecuado para el nuestro.

Si tenemos muchos equipos en la red y corremos el riesgo de confundir las fuentes de alimentación, recomendamos marcar todas las fuentes usando cinta o etiquetas. Así, etiquetaremos cada fuente con su marca y modelo, agregando también el voltaje y la corriente de salida que ofrecen a nuestro dispositivo.



Figura 8. Es muy común confundir la fuente de alimentación del punto de acceso con la alimentación para la notebook.



Figura 9. Es una buena práctica etiquetar todos los cables en nuestra red; en esta imagen vemos como ejemplo un cable UTP.

Actualizaciones

Al hablar de **actualizaciones** siempre nos referimos a los equipos que traen software incorporado (microcódigo) y que llamamos **firmware** (explicamos este tema en el **Capítulo 2**). Es sabido que cada fabricante instala una versión de **firmware** en el dispositivo a la hora de ponerlo a disposición de los usuarios en el mercado. Sin embargo, el firmware es constantemente actualizado por el fabricante y suelen existir nuevas versiones para usar (se puede consultar el sitio web del fabricante del equipo para comprobar la disponibilidad de una nueva versión).

Nuestro método

Para proseguir, en esta sección basaremos nuestro **método** para resolver problemas en la red inalámbrica en cinco pasos fundamentales, los cuales mencionamos a continuación:

1) Delimitar el problema
2) Encerrar la causa del problema
3) Planear la solución
4) Corroborar los resultados
5) Documentar los resultados

Delimitar el problema

Aunque muchas veces se ignora este primer paso, nosotros consideramos que es el más **importante** de todos. Tenemos que iniciar el método haciendo un análisis del problema completo. De no realizarlo, estaríamos perdiendo mucho tiempo al tratar de arreglar síntomas y no, la verdadera causa del problema.

Tal vez nos preguntemos: ¿qué necesitamos para realizar semejante paso importante? No mucho, bastará con una **lapicera**, una **libreta u hojas** y prestar mucha **atención**.

> LA DELIMITACIÓN DEL PROBLEMA ES UNO DE LOS PASOS MÁS IMPORTANTES PARA SOLUCIONARLO

La mejor fuente de información es prestar atención a lo que dicen los usuarios de la red y, así, recopilar datos útiles. Tengamos presente que escuchar el problema desde un ángulo diferente al nuestro puede mostrarnos información que nos ayude a resolver el inconveniente. Las personas que hacen uso de la red a diario estaban allí cuando el problema no existía y, luego, cuando apareció; y seguramente recordarán cuáles fueron los sucesos que llevaron al inconveniente.

Para ayudar a identificar el conflicto, **anotemos** en una lista la secuencia de hechos que describen los usuarios. En caso de que nosotros mismos seamos los usuarios, tratemos de recordar qué ocurrió antes de la falla.

Si hacemos preguntas, lograremos acotar el problema. El éxito de estas preguntas depende de la habilidad de cada uno para obtener información. Las siguientes preguntas y sus posibles respuestas nos muestran nuevos ejemplos por seguir para delimitar el conflicto:

- ¿Los problemas ocurren todo el tiempo o en ciertos lapsos? Cuando el hardware comienza a fallar se hace visible con síntomas que se presentan en forma intermitente.
- ¿El problema afecta a todos los clientes inalámbricos o solamente a uno? En caso de verse afectado solo un cliente inalámbrico, es muy probable que la falla esté en su computadora.
- ¿Se hicieron actualizaciones automáticas del sistema operativo? Ciertos cambios en el sistema pueden causar problemas.
- Cuándo el problema ocurre, ¿es en todas las aplicaciones (**MSN, Skype**, etc.) o solamente en una en particular? En caso de aparecer en una sola, deberemos centrarnos en investigar sobre ella.

- ¿Anteriormente ocurrió algún problema similar? En caso de que la respuesta ses afirmativa, debemos revisar la documentación en busca de la posible solución. Si no existe documentación, preguntemos si alguien recuerda cómo se solucionó el error.
- ¿Se agregaron nuevos usuarios a la red inalámbrica o cableada? Al incrementar el tráfico de la red, todos los usuarios pueden sufrir retrasos en la conexión y la transferencia de datos.
- ¿Se han instalado nuevos dispositivos en la red? En caso de ser afirmativa la respuesta, debemos verificar que los nuevos dispositivos estén configurados correctamente.
- ¿Existen diferentes marcas de fabricantes en los equipos implementados en la red? Es posible que exista alguna incompatibilidad entre fabricantes de equipos. ¿Alguien instaló nuevo **software** en la PC que tiene problemas antes de que ocurra el error? Muchas veces, la instalación de programas puede ocasionar errores. Revisemos cualquier aplicación instalada antes de que ocurra el problema.
- ¿Alguna persona movió un dispositivo de la red? Es común que el equipo que se haya movido no esté conectado correctamente.
- ¿Han intentado solucionar el problema antes? De ser así, tratemos de hablar con la persona que intentó hacerlo.

Encerrar la causa del problema

El objetivo de este segundo paso es aislar o identificar la causa original del problema. Comenzaremos separando de nuestra lista (realizada en el paso anterior) todos los problemas sencillos, y seguiremos con los que consideremos más difíciles de resolver. Decimos que un problema es sencillo de resolver cuando, por ejemplo,



AYUDA EN LÍNEA

Cuando un problema en la red inalámbrica escapa del conocimiento que poseemos, es momento de buscar ayuda. Podemos consultar a compañeros o amigos que tengan experiencia en el tema. Un recurso práctico, fácil y que todos tenemos a mano es buscar en Internet sobre el problema específico. El buscador de Google (**www.google.com**) es muy recomendado.

se repite el inconveniente de forma continua en todo momento. Esto depende de la experiencia propia de cada persona. Separando problemas o errores, estaremos acotando toda la lista a una o dos categorías que incluyan solo lo más importante.

En ciertas ocasiones es útil que alguien nos muestre cómo se produce el error; de esta forma, podremos ver realmente cuál es el inconveniente. Por ejemplo, si el problema aparece cuando una persona intenta ingresar a su cuenta de correo electrónico, entonces reproduzcamos el error ingresando al sitio web del correo, y anotemos cómo se produce y los mensajes de errores que obtenemos.

> LOS PROBLEMAS MÁS DIFÍCILES SON AQUELLOS QUE SE PRODUCEN EN FORMA INTERMITENTE

Los problemas más difíciles de aislar son los que se producen de forma **intermitente** y que pocas veces se manifiestan cuando uno está presente. Una de las maneras más usadas para resolver estos problemas es realizar nuevamente los eventos que los ocasionaron. Como ayuda extra, podemos solicitar al usuario que nos detalle lo que estaba realizando antes y en el momento en que ocurrió el error. Si este se presenta de modo intermitente, podemos solicitar que nos llamen cuando aparezca el inconveniente en la red y, mientras tanto, pedir que nadie toque nada (nos referimos a no instalar nuevas aplicaciones, por ejemplo). Así, podremos ver el error cuando se manifiesta.

Planear la solución

Una vez que tenemos varias categorías de posibles causas que originan el problema en la red, comenzaremos a planear la solución.

Pensaremos un plan para identificar y resolver los conflictos basándonos en el conocimiento actual. Empezaremos siempre con las soluciones más sencillas y obvias, para ir descartándolas de la lista hasta llegar a las más difíciles y complejas. Algo muy importante para tener en cuenta es **anotar** lo que hacemos en cada paso; así estaremos **documentando** cada acción efectuada y su resultado. Cuando en un futuro se nos presente un problema y nosotros identifiquemos algún síntoma similar, podremos consultar la documentación correspondiente para resolverlo con mayor facilidad y rapidez.

Recomendamos seguir dos enfoques para tener éxito al momento de resolver los problemas concretos de la red:

- Resolver problemas de arriba-abajo
- Resolver problemas del centro-arriba, o del centro-abajo

Resolver problemas de arriba-abajo

Si tenemos presente la pila de protocolos del modelo OSI o TCP/IP, podremos recorrerla en busca de soluciones para el inconveniente.

Tomemos uno de los problemas de nuestra lista, por ejemplo, la falla al tratar de conectarnos a **MSN**. Comenzaremos verificando, en este caso, la aplicación en donde tenemos el error (MSN, que trabaja en la Capa de Aplicación del modelo TCP/IP). Intentaremos resolver el conflicto verificando el nombre de usuario y la contraseña ingresados.

PARA SOLUCIONAR UN PROBLEMA DEBEMOS TENER PRESENTE LA PILA OSI O TCP/IP

Un usuario que ingresa de manera errónea su dirección de e-mail o contraseña puede ser la causa del supuesto error. De ser así, daríamos por solucionado el tema comprobando que, si ingresamos correctamente los datos, el proceso de autenticación funciona.

Si el problema no se resuelve, seguiremos descendiendo imaginariamente en la pila de protocolos hasta llegar, por ejemplo, a las capas inferiores. Tal vez un problema de **interferencia** en la señal inalámbrica o un bajo nivel de señal en la notebook causa la falla y, de esta forma, lo estaríamos identificando.

Este método requiere paciencia y dedicación. Si consultamos en Internet acerca de problemas específicos y formulamos preguntas puntuales, podremos obtener resultados muy satisfactorios.

Resolver problemas del centro-arriba, o del centro-abajo

Resolver el problema utilizando este enfoque es la manera más popular. Es aplicado, en general, de modo intuitivo por personas que ya poseen experiencia en redes, y es la forma más fácil para empezar a lidiar con este tipo de errores para los que no poseen experiencia

alguna. Iniciamos el método posicionándonos, nuevamente de manera imaginaria, en la capa central de la pila de protocolos TCP/IP (esto sería entre la Capa de Transporte y la Capa de Red).

Si miramos para arriba (centro-arriba) tenemos:

- La Capa de Transporte y, más arriba, la Capa de Aplicación.

En cambio, si miramos desde nuestra posición imaginaria hacia abajo (centro-abajo) tendremos:

- La Capa de Red y, por último, la Capa de Acceso a la red.

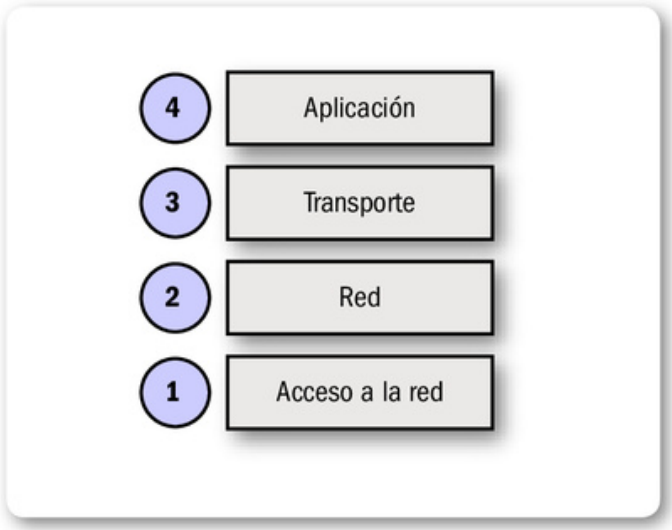


Figura 10. Tener una visión del problema desde un ángulo diferente nos proporciona posibles nuevas soluciones.

Cuando exista un supuesto problema y apliquemos este método, iniciaremos verificando, en la mayoría de los casos, si existe **conectividad a nivel de Red** (IP) entre diferentes dispositivos que integran la red o con el servicio que estamos solicitando (MSN en el ejemplo que estamos siguiendo).

Debemos tener en cuenta que la conectividad IP se comprueba fácilmente con un comando llamado **ping**. Podemos decir que el comando **ping** es una de las herramientas más útiles empleadas en diagnóstico de redes. Este comando existe en todos los sistemas operativos, y podemos utilizarlo para realizar el envío de información binaria (ceros y unos) entre dispositivos que se encuentren en la red. Así, la persona que realiza el ping a otro puede saber si existe una conexión entre su computadora y el destino en función de si los paquetes de información llegan o no.

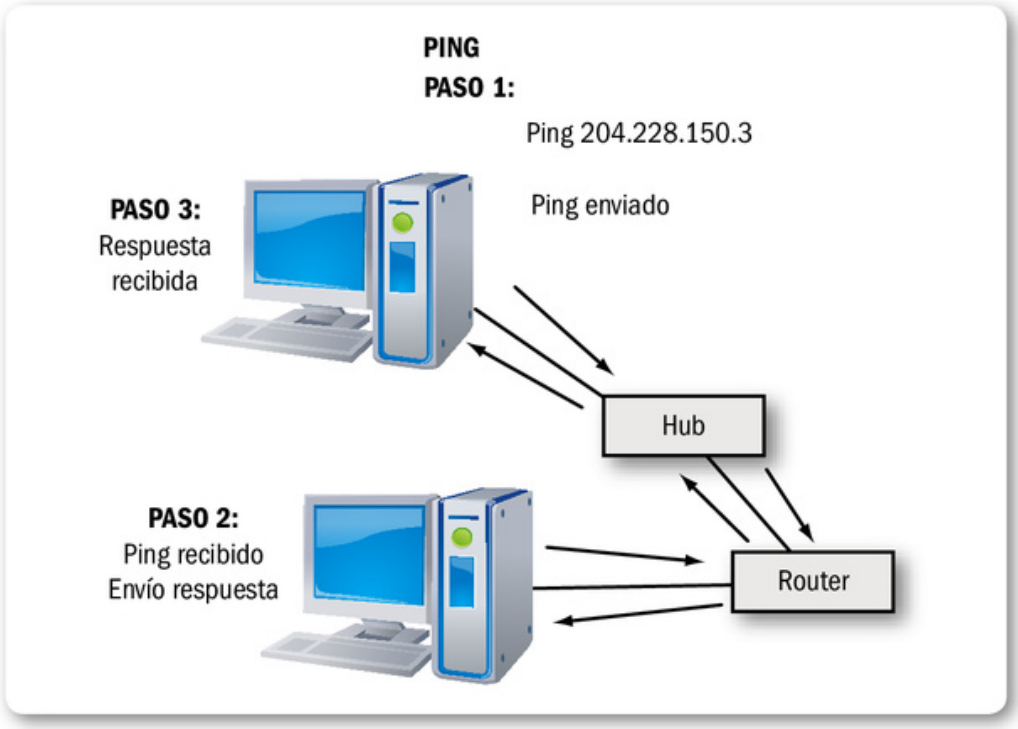


Figura 11. Este ejemplo nos muestra el camino de los datos enviados por el comando ping.

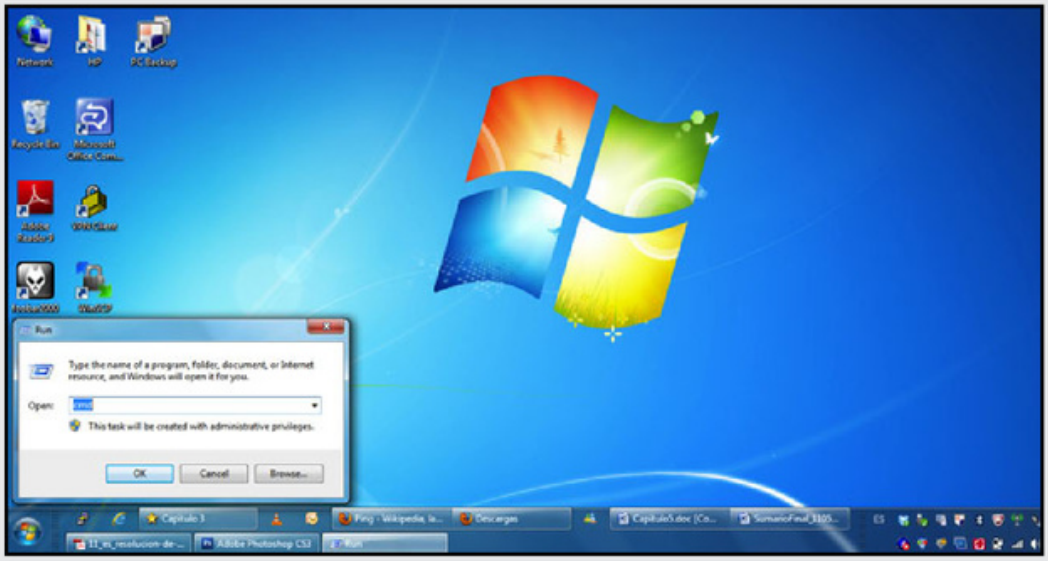
En este punto vale aclarar que estos paquetes de información enviados por el comando **ping** no tienen información alguna, tan solo se trata de señales inertes para cualquier dispositivo de la red. Consideremos también que no importa el sistema operativo que utiliza el dispositivo destino, al cual enviamos los paquetes, ya que el ping se realizará de todas formas. A continuación, veamos con un ejemplo detallado cómo funciona este comando.

MONITOR DE RED EN WINDOWS 7

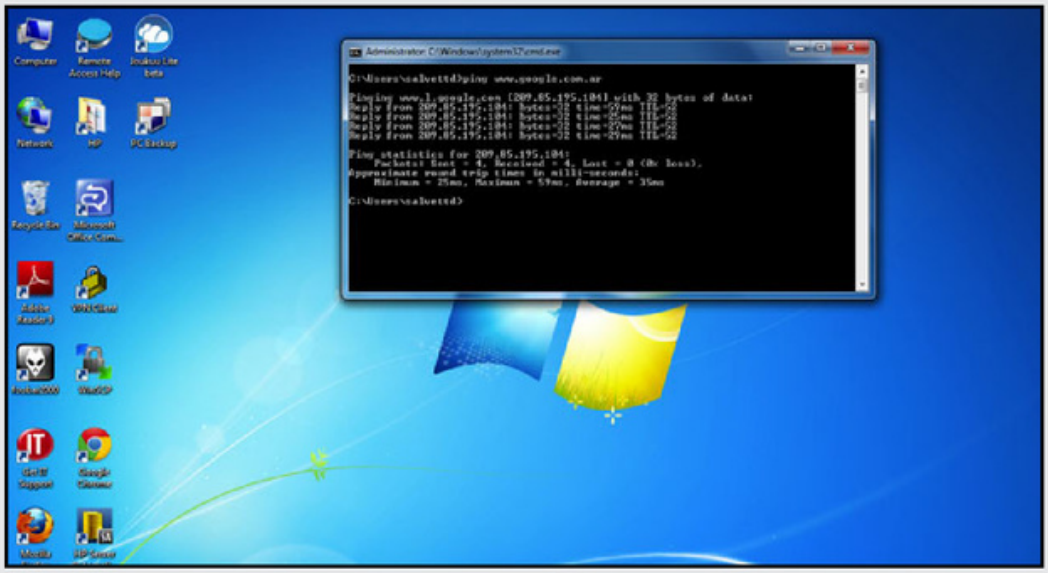
Es interesante tener en cuenta que existe un **gadget** (pequeño programa diseñado con una función específica) para sistemas Microsoft Windows 7 muy útil a la hora de monitorear una red de datos. Se trata de **Network Meter**, que nos permitirá ver el SSID, calidad de la señal en porcentajes, direcciones IP asignadas, localización de la IP usando el servicio de **GoogleMaps** y velocidad de subida/bajada, entre otros datos. Podemos bajarlo desde la dirección **http://addgadget.com**.

EJEMPLO DE COMANDO PING ■ PASO A PASO

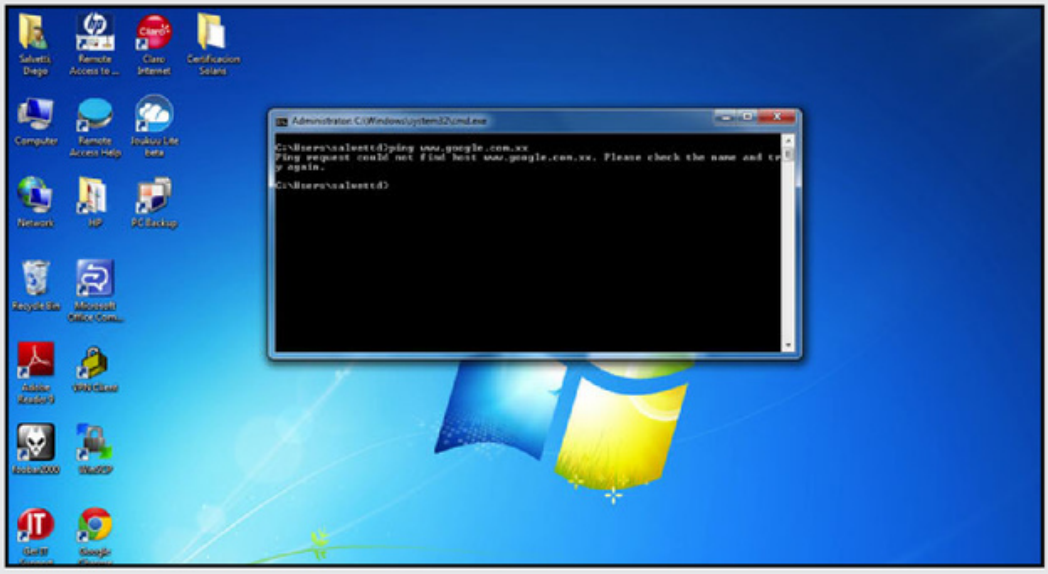
01 Ejecute `ping` desde el símbolo del sistema que correrá de forma automática el archivo ping.exe alojado en la carpeta system32. Haga clic en `inicio` y luego en `Ejecutar` (o Run), y luego escriba `cmd`.



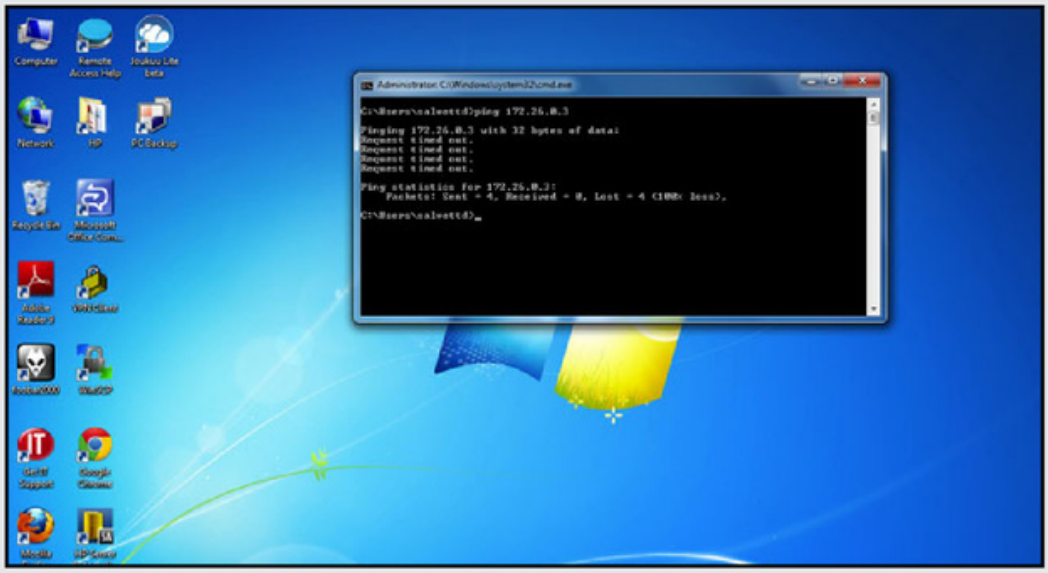
02 La sintaxis de este comando es la misma que para el resto de los comandos en Windows. Se forma: `ping <ip> -parámetro valor -parametro2 valor`. Ahora, reemplace `<ip>` por la dirección IP destino (esta variable es obligatoria). Escriba `ping www.google.com.ar` y presionr ENTER.



03 Vea la salida que obtiene luego de presionar ENTER. Se informa la dirección IP del sitio web y cuatro confirmaciones de respuesta desde ese destino. Además, se muestra la demora en realizar el camino entre el servidor consultado y la computadora. Escriba `ping www.google.com.xx` y luego pulse ENTER.



04 Como el destino no existe se muestra un mensaje de error diciendo que debe verificar la ruta destino. Ingrese una dirección IP que no pertenezca a ningún usuario en la red. Escriba `ping 172.26.0.3` y presione ENTER. Verá que no obtendrá respuesta. En cambio, tendrá un mensaje de tiempo agotado (Time out).



Algunos de los parámetros más comunes que podemos utilizar con este comando son:

- **-t**: realiza ping al destino hasta que se fuerza la salida (presionando las teclas **CTRL+C**)
- **-n <numero>**: se especifica el número de solicitudes que deseamos enviar. Por ejemplo: **ping –n 15**

Siempre que no especifiquemos otra cosa, se enviarán cuatro mensajes al destino (por lo tanto. recibiremos esa misma cantidad en el origen). Si queremos modificar esto y enviar paquetes de forma ininterrumpida, usamos el parámetro **–t** como vimos. Como dato útil consideremos que, en caso de existir algún inconveniente en la red (falta de señal, corte en el servicio, entre otros), podríamos darnos cuenta del posible problema mirando el porcentaje de datos perdidos que refleja este comando.

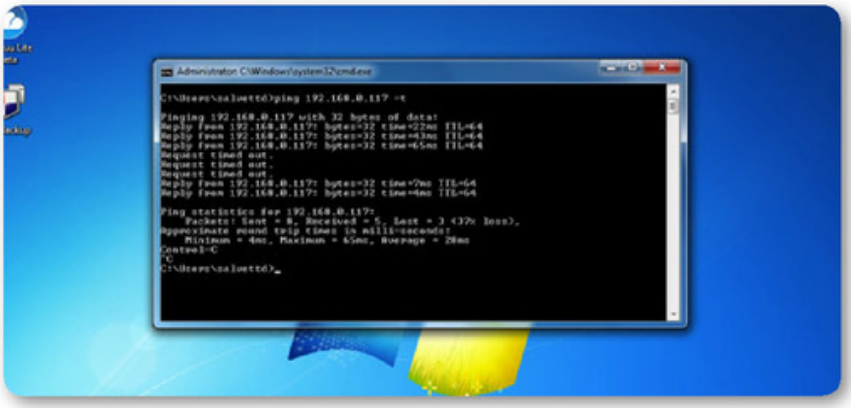


Figura 12. Si con **ping** los paquetes enviados difieren de los recibidos, podemos tener un indicio de problemas en la red.

Usaremos el comando **ping** para evaluar la conectividad entre diferentes elementos de la red. Principalmente, recomendamos hacerlo entre la estación inalámbrica que presenta problemas y otra computadora o estación inalámbrica con nuestro punto de acceso.
Si alguno de estos tests falla, podremos movernos y atacar el problema poniendo el énfasis en donde ocurre el corte. En caso de que ninguno falle, nos centraremos en las aplicaciones del usuario con problemas o en sus configuraciones del sistema operativo.

Sea cual sea la forma que adoptemos para resolver el problema en nuestra red, es importante que nos familiaricemos con las herramientas (como ping) utilizadas para analizar las funciones de cada capa (según el modelo TCP/IP).

El objetivo principal que perseguimos al describir una metodología es que podamos detallar procedimientos de resolución de fallas y, además, identificar problemas de manera efectiva y simple.

SE RECOMIENDA CREAR UN PLAN Y SEGUIR CADA UNO DE SUS PROCEDIMIENTOS

Se recomienda crear un **plan** y seguir los procedimientos tal como lo hayamos pensado. Evitemos improvisar y saltar de un lado a otro de forma aleatoria, porque eso puede provocarnos problemas y consumirnos tiempo. Siempre existe la posibilidad de crear un nuevo plan en caso de no tener éxito (tratemos de basarnos en la experiencia adquirida del plan anterior).

Finalmente, cuando encontremos el problema, lo solucionaremos según nuestro criterio. Por ejemplo, si es necesario cambiar la placa de red inalámbrica, compraremos una y reemplazaremos el componente de la computadora. Sea cual sea el conflicto, documentemos en un cuaderno los cambios realizados (antes y después) para tener futuras referencias,veamos en detalle estos pasos finales.

Corroborar los resultados

No podemos considerar finalizada la reparación del inconveniente sin tener una **confirmación** de que todos los componentes de la red trabajan satisfactoriamente. Es fundamental asegurarnos de que el problema ya no existe. Para esto, vamos a solicitar a los usuarios de la red inalámbrica que prueben la solución (básicamente, esto es que usen la red de forma normal). Ellos serán los que confirmarán los resultados.

Una parte importante es fijarnos que la solución encontrada no signifique nuevos problemas en la red. Por ejemplo, si existía un conflicto en una dirección IP de un usuario y se tomó como solución modificar a mano esa IP y asignarle otra, tenemos que verificar que la IP asignada no sea la misma que tiene otro usuario (que la recibe por DHCP). Esto generaría un conflicto de **direcciones IP duplicadas** y tendríamos un impacto negativo en la red, lo que originaría un nuevo conflicto.

Documentar los resultados

Por último, pero no menos importante, necesitamos **documentar el problema** encontrado y la solución planteada (todas, las que no fueron exitosas y las que sí). No existe nadie que nos enseñe efectivamente cómo resolver problemas más que la experiencia propia adquirida. Esto nos proporciona información de gran valor que debemos aprovechar. Cada problema que se presenta es una oportunidad para incrementar la experiencia y ganar nuevos conocimientos.



Figura 13. Volcar nuestra experiencia en un blog online para compartir información con otras personas es una muy buena idea.

Tener un **cuaderno** (o blog en Internet) con el procedimiento que utilizamos para reparar el problema puede ser muy útil cuando el mismo conflicto (o uno similar) se vuelva a presentar. **Documentar** la resolución de problemas es una forma didáctica de crear, retener y compartir nuestra experiencia.

Tengamos presentes ciertas consideraciones:

- En caso de tener una red grande, y si la primera revisión en busca de síntomas que nos lleven al problema falla, recomendamos dividir

la red en partes más pequeñas. De esta forma, **atacaremos** cada una de esas partes de modo independiente, analizando toda la información relevante para lograr aislar la causa.

- Muchas veces, preguntarnos si el problema es originado en el **hardware** o **software** de la red nos ahorrará mucho tiempo. Por ejemplo, si consideramos que es un problema de software, intentemos utilizar la misma aplicación pero en otra computadora de la red, para así verificar que la falla existe en un solo usuario de la red inalámbrica y no afecte a otras conexiones.
- Debemos recordar que si el problema se relaciona con el hardware, es recomendable verificar: placas de red, cables y conectores de la red cableada y alimentación de los dispositivos, puntos de acceso y dispositivos similares, etc.
- Aislar una parte de la red en busca del problema puede resultar una solución para las otras partes. Si esto ocurre, no consideremos resuelto el problema y concentrémonos en la parte que no está operativa y, posiblemente, sea la causa del conflicto.
- Definamos **prioridades** a la hora de resolver problemas. Muchos problemas pueden ser críticos y necesitarán ser resueltos rápidamente. Evaluemos cómo impacta el problema en la red y los servicios que prestamos. En este sentido, no es lo mismo dejar a un usuario sin Internet para que consulte un e-mail de su novia, que dejar sin acceso a la red a una persona que necesita realizar una transacción bancaria con suma urgencia.

Caso práctico

Para tratar de resumir todo lo visto hasta el momento, veremos un ejemplo de la vida real. De esta forma, podremos mostrar cómo funciona el método planteado como adecuado.

Es lunes por la mañana, y cuando las personas que comúnmente usan la red encienden sus computadoras para tratar de revisar sus correos electrónicos, obtienen un error. Al unísono podemos escuchar "No puedo entrar a mi **Gmail** para leer los correos".

Para continuar, veamos cómo resolveríamos este simple pero interesante conflicto. Basándonos en la resolución de problemas arriba-abajo, formularemos las siguientes preguntas para recopilar información sobre la causa de la falla que nos aqueja:

- Qué programa utiliza para chequear su correo? (en este punto, debemos verificar cada uno de los posibles problemas que puedan estar en la Capa de Aplicación).
- ¿Puede verificar la configuración de conexión de su programa?
- ¿Puede ingresar en otras **páginas web**? (en este paso es necesario que realicemos la verificación de problemas de DNS).
- Por cuestiones de seguridad, ¿tiene su aplicación un tiempo que vence y se desconecta? (verificamos problemas de sesión en la Capa de Transporte TCP).
- ¿El punto de acceso u otro dispositivo le solicitan nombre de usuario y contraseña para autenticarse? (aquí debemos verificar los posibles problemas de autenticación para el usuario correspondiente).
- ¿Su computadora tiene una dirección IP asignada? (nos encargamos de verificar problemas que se presenten a nivel IP).

> ES IMPORTANTE SEGUIR CADA UNO DE LOS PASOS PARA SOLUCIONAR UN PROBLEMA DE RED

- Si aplicamos la otra resolución de problemas (centro-arriba o centro-abajo), podríamos preguntar lo siguiente:
  - ¿Puede hacer **ping** a la dirección **www.gmail.com**?
  - ¿Puede hacer **ping** al punto de acceso de la red?

  En caso de que ambas respuesta sean negativas:
  - ¿Verificó si tiene una dirección IP asignada?
  - ¿Ingresó sus datos en el servidor de autenticación?

Los problemas pueden ser diferentes según las redes que tengamos, pero la metodología adecuada que debemos utilizar para encontrar y resolver los problemas es siempre la misma.



DOCUMENTAR LA RED

Antes de emitir el diagnóstico de un problema, necesitamos averiguar el tipo de problema de que se trata. Para esto, recopilaremos la mayor cantidad de información posible sobre la red. Si está documentada, consultaremos al respecto; de no ser así, deberemos elaborarla nosotros. Incluiremos datos como topología de red, resumen de dispositivos con sus nombres y direcciones (MAC e IP), y otros.

Qué herramientas usar para resolver problemas?

Necesitamos tener en claro qué **herramientas** tenemos disponibles para ejecutar nuestro método y así resolver los posibles errores de la red inalámbrica.

Básicamente, decimos que usaremos dos tipos de **herramientas**. por un lado las que vienen con cada producto (según el fabricante, aunque esto puede variar) y las que trabajan con cualquier producto soportado por la norma IEEE 802.11.

Enumeremos algunas herramientas y su aplicación básica. Es posible consultar más información en Internet.

HERRAMIENTAS

N°	NOMBRE	USO	EJEMPLO DE USO
1	**Nslookup**	Se usa para determinar si el DNS está resolviendo correctamente los nombres y las IP.	En una consola escribimos: nslookup [-option] [hostname] [server]
2	**Ntop**	Permite monitorear una red en tiempo real.	Hay que bajar e instalar la herramienta para Windows.
3	**Tracert**	Hoy en día se utiliza Visualroute. Permite seguir la pista de los paquetes que vienen desde un host en la red.	Debe bajarse la herramienta VisualRoute para Windows.
4	**Nmap**	Efectúa el rastreo de puertos en un host de la red.	Debe bajarse e instalarse Nmap para Windows.
5	**Wireshark**	Analizador de protocolos usado para analizar y solucionar problemas.	Debe bajarse e instalarse para Windows.

Tabla 1. Las cinco principales herramientas para utilizar al momento de resolver problemas en la red.

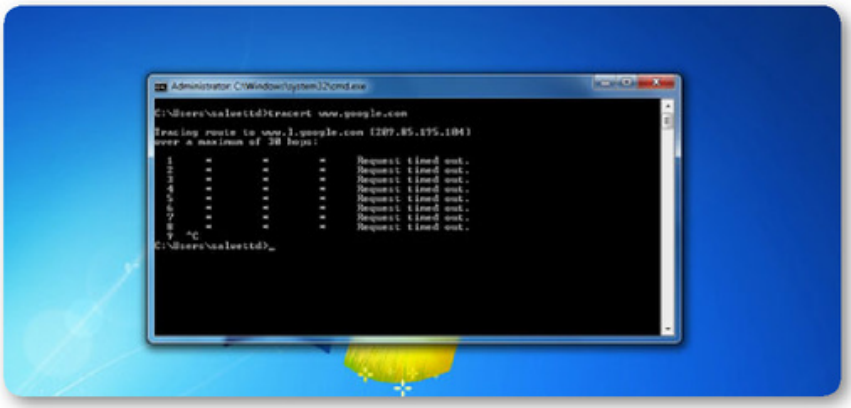


Figura 14. Ejemplo de aplicación de la herramienta **`tracert`** sobre la dirección **`www.google.com`**.

Como sabemos, existen muchas herramientas que nos pueden ayudar en la resolución de problemas de red; una de ellas es **VisualRoute**, que vemos en la **Figura 15**.

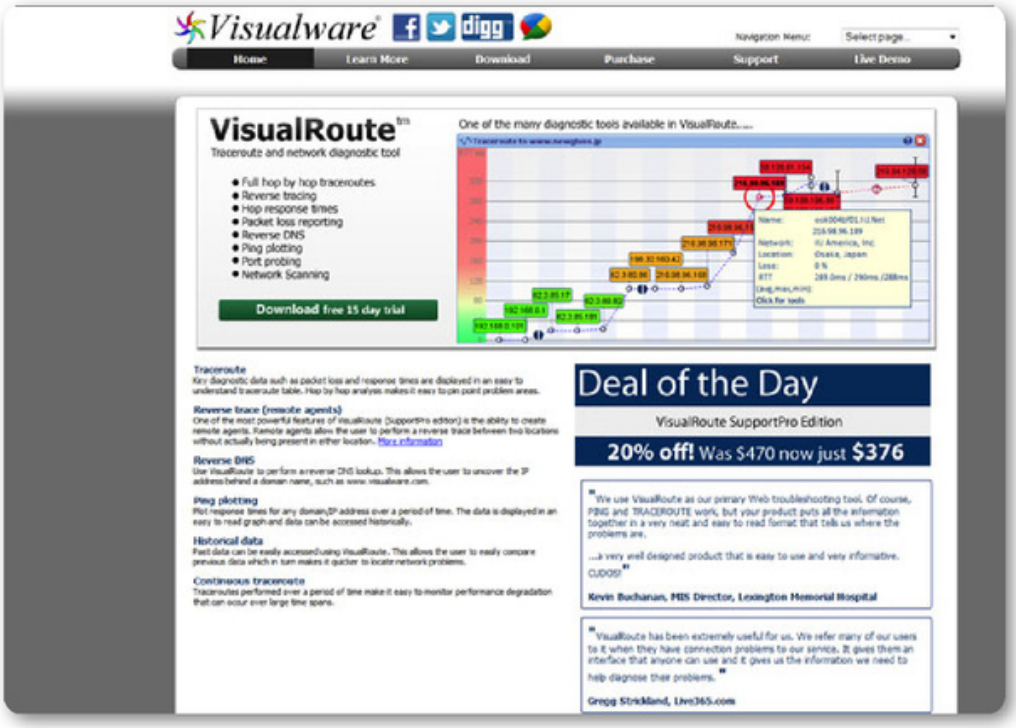


Figura 15. La empresa **`VisualWare`** nos presenta el producto **`VisualRoute`** para realizar diagnósticos en nuestra red.

Escenarios prácticos

Determinemos un problema y busquemos las herramientas apropiadas para utilizar según sea el caso.

1) Red congestionada.

Cuando se plantea este tipo de problemas, lo recomendado es tener una visión general de las comunicaciones IP que figuran activas en la red inalámbrica. Para conseguirlo en Windows podemos usar la herramienta **WireShark** o **IPSniffer**.

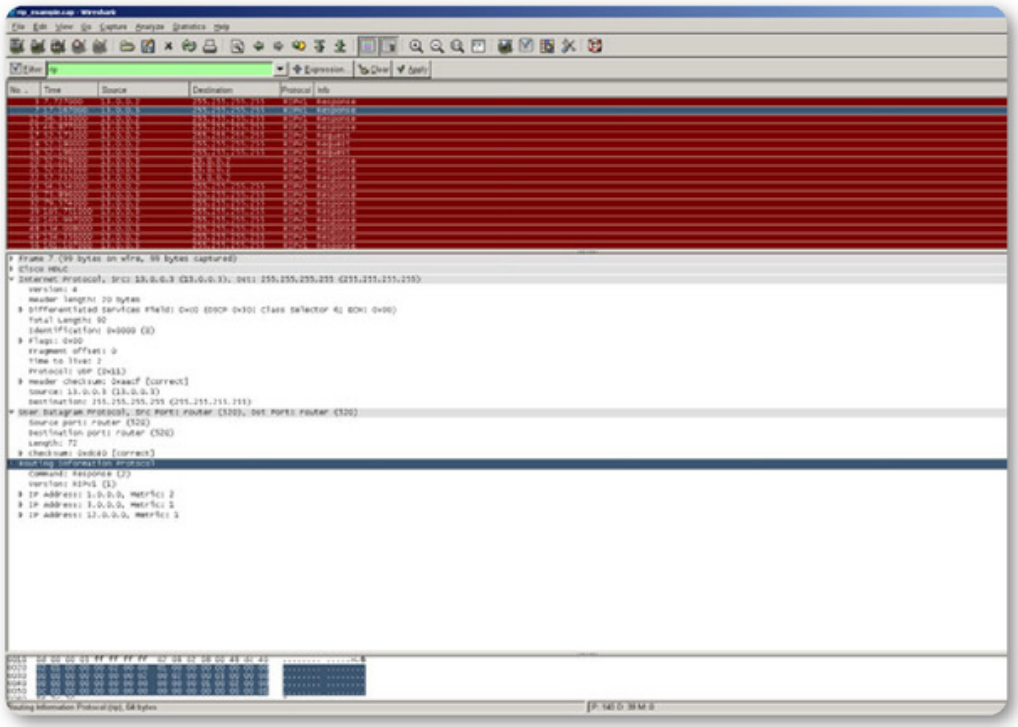


Figura 16. WireShark nos presenta los diferentes protocolos en tiempo real y discriminados con etiquetes y colores.

ETHEREAL, LUEGO WIRESHARK

Para los que no lo saben, primero fue **Ethereal** y, luego, **WireShark**. Así se sucedieron estos analizadores de protocolos multiplataforma. La funcionalidad que ofrecen es similar al famoso **tcpdump** (un analizador de protocolos que se ejecuta desde consola) de ambientes UNIX. La diferencia básica con tcpdump es que **WireShark** tiene interfaz gráfica.

Con esta herramienta estamos tratando de identificar conexiones entrantes y salientes hacia la red inalámbrica. De esta forma, podremos identificar el tipo de tráfico IP y la manera en que se distribuye el tráfico entre los clientes de la red. En este punto podríamos observar que entre dos usuarios de la red inalámbrica existe gran cantidad de tráfico web seguro (HTTPS) y varias conexiones **Telnet**, mientras que otros dos nodos tienen excesivo tráfico DNS y eso puede provocar un problema.

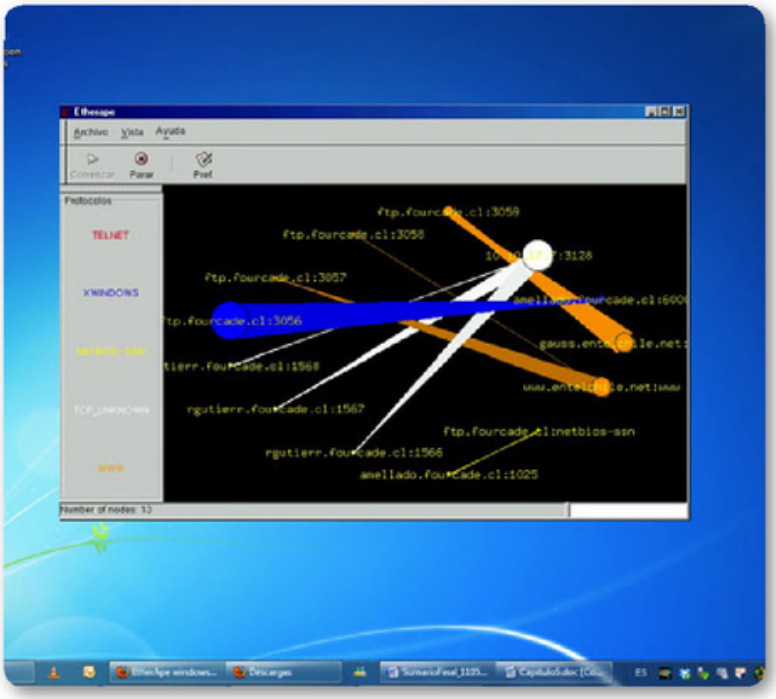


Figura 17. Otra herramienta útil es EtherApe, la cual nos entrega una visión global del tráfico que ocurre en la red y cada uno de los protocolos asociados.

PING GRAFICADO

Si nuestro **troubleshooting** (solución de problemas) requiere información detallada y con el comando **ping** no alcanza, podemos usar **Ping Plotter** (**www.pingplotter.com**). Esta herramienta no solo hace ping a un destino, sino que también realiza el trazado de la ruta y las gráficas de las respuestas. Toda esta valiosa información puede guardarse para luego ser analizada.

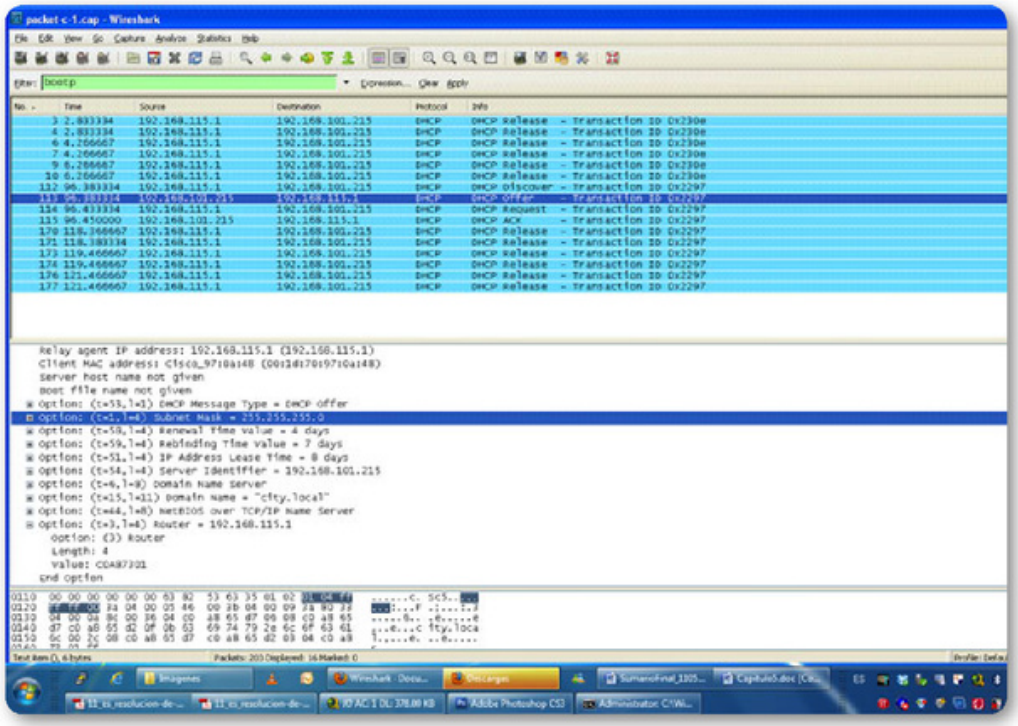


Figura 18. El programa **WireShark** realmente nos permite ver lo profundo de las comunicaciones.

2) ¿Conexiones rechazadas o **red fuera de servicio**?

En el momento en que nosotros consideremos que necesitamos tener una visión más cercana de lo que ocurre en la red, y específicamente con un tipo de tráfico, no dudemos en instalar **WireShark**. Como describimos antes, es una herramienta muy versátil; en este caso podemos capturar todo el tráfico que pase por nuestra placa de red inalámbrica y nos permitirá analizar esos datos.

Se trata de una alternativa para realizar las siguientes tareas:

ETIQUETADOR DE RED

Si necesitamos etiquetar cables en la red y queremos hacerlo de manera prolija, recurrimos a la empresa **Sharpmark Solutions**. En el sitio de la **Network Connections Group USA** tenemos disponible un programa gratuito para realizar el etiquetado. Ingresamos a **www.ncusa.com/labeling/downloads.htm** para bajar el software etiquetador de cables y dispositivos.

- Monitorear pérdida de paquetes en conexiones TCP. Esto ocurre cuando la red está congestionada, **saturada de tráfico**, etc.
- Monitorear el tiempo de retorno. Se trata de un indicador que informa sobre el **retardo en la red**.
- Monitorear errores de protocolo. Es muy difícil ver estos errores sin una herramienta de este tipo. Cuando tenemos direcciones IP duplicadas, vamos a detectarlo usando WireShark.



RESUMEN

En este capítulo presentamos un enfoque propio para resolver problemas que aparecen en las redes. Antes de entrar en el detalle del procedimiento, recomendamos ciertos puntos a tener en cuenta para evitar causar daños y/o problemas a los dispositivos en la red. Definimos los pasos de nuestro método y presentamos, con ejemplos prácticos, la forma de ejecutarlos. Para finalizar el capítulo, presentamos herramientas muy útiles a la hora de analizar, diagnosticar y arreglar una red junto con ejemplos cotidianos sufridos en redes.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿En qué dos modelos se basa el método para resolver problemas de red?
2. ¿Cuál es un punto sensible a daños en un punto de acceso si hay anomalías en el servicio eléctrico?
3. ¿Por qué motivo es importante tener el firmware del equipo actualizado?
4. Enumere los cinco pasos fundamentales del método.
5. ¿Para qué sirve realizar preguntas a los usuarios de la red cuando reportan un problema?
6. ¿Cuáles son los dos enfoques que se describen para resolver los problemas planteados?
7. ¿Cuál de los dos enfoques es el más popular y se realiza de manera intuitiva?
8. ¿Con qué comando se comprueba que hay conectividad IP?
9. ¿Por qué es importante documentar el procedimiento?
10. Enumere algunas herramientas que se recomienda usar para la resolución de problemas de red.

ACTIVIDADES PRÁCTICAS

1. Abra una consola y ejecute el comando ping. Use como dirección de destino la IP del punto de acceso de su red.
2. Ejecute nuevamente el comando ping usando la dirección 127.0.0.1 y la opción –t. Evalúe los resultados.
3. Pruebe la herramienta nslookup desde la consola del sistema operativo.
4. Instale WireShark y capture tráfico de su red.
5. Analice y trate de identificar el tráfico de su red.

*06

Enlaces

Los enlaces son redes inalámbricas implementadas en un área que abarca pequeñas o grandes dimensiones. Anteriormente definimos una red inalámbrica como un vínculo entre dos o más terminales que se comunican sin necesidad de utilizar cables. En este capítulo veremos los enlaces de larga y corta distancia.

- **Enlaces de larga distancia..... 146**
- **¿Qué es un radioenlace? 149**
  - Tipos de enlaces..... 152
- **Alineación de antenas..... 160**
  - Con extremos visibles..... 160
  - Con extremos no visibles..... 162
- **Enlaces de corta distancia..... 162**
- **Bluetooth: ¿qué es y cómo funciona? 167**
  - Topología de red 168
- **Resumen..... 169**
- **Actividades..... 170**

Enlaces de larga distancia

Con lo visto hasta el momento en este libro, podríamos decir que la tecnología inalámbrica es solamente para aplicar en redes LAN o redes locales pequeñas. Sin embargo, si investigamos el impacto que tiene esta tecnología a nivel mundial, nos daremos cuenta de que, en ciertos países, el uso de las redes inalámbricas es mucho más intenso, y se aplica para situaciones en las que es necesario enlazar computadoras o equipos a larga distancia.

Recordemos que en países europeos, es muy común que las empresas instalen cables de fibra óptica y, así, ofrezcan excelentes conexiones (muy buen ancho de banda) a Internet para lograr que las ciudades y su población puedan comunicarse.

Si comparamos esto último con la situación que vemos en nuestro país y en casi toda Latinoamérica, notamos que la inversión por parte de empresas relacionadas a las **telecomunicaciones** en infraestructura para el usuario final son mínimas. En este sentido, las **fibras ópticas** instaladas no llegan hasta el usuario final y, por lo tanto, no se provee un ancho de banda comparable al que podemos encontrar en los países europeos o al propio Estados Unidos.

> UN RADIOENLACE ES UNA CONEXIÓN ENTRE DISPOSITIVOS POR ONDAS ELECTROMAGNÉTICAS

Por este motivo (sumado a otras ventajas que vimos anteriormente), la tecnología inalámbrica es exitosa en países que están desarrollándose. Cuando en una red no se necesita realizar una instalación cableada (esto implica cables UTP, conectores, herramientas específicas para armar los cables y bandejas, entre otros), los costos son menores, y la viabilidad de la red es alta.

Un **radioenlace** es cualquier conexión entre dispositivos de telecomunicaciones (computadoras, puntos de acceso, entre otros) realizada por medio de ondas electromagnéticas. Cuando las distancias son extensas entre ambos puntos por unir, se denomina **radioenlace de larga distancia** (o **enlace de larga distancia**).

Si nos encargamos de desglosar la tecnología inalámbrica utilizada en los radioenlaces, vamos a darnos cuenta de que existen algunas variantes. Analizando cada variante, vemos cuáles pueden ser útiles dependiendo de la necesidad que debamos cubrir.

Por ejemplo, muchos de nosotros podemos haber escuchado hablar de los **radioenlaces de microondas** que instalan las empresas dedicadas a las telecomunicaciones. Como sabemos, se trata de enlaces que trabajan con **ondas electromagnéticas** cuyas frecuencias van desde los 500 MHz hasta los 300 GHz.

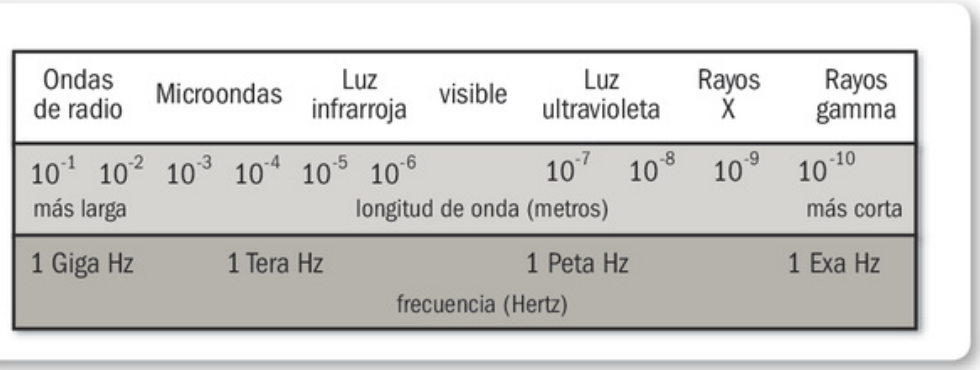


Figura 1. Recordamos la clasificación de las diferentes frecuencias y sus usos en el espectro electromagnético.

Los **enlaces de larga distancia por microondas** ofrecen mucha confiabilidad y estabilidad del servicio, dado que son una tecnología realmente madura. En este sentido, el problema con el que podemos encontrarnos es el elevado costo y la mano de obra calificada que necesitamos para instalar el equipamiento.

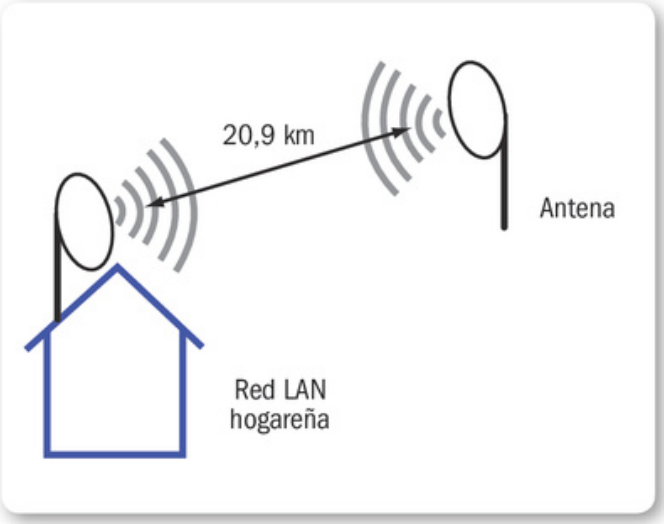


Figura 2. Los radioenlaces con microondas pueden unir puntos distantes y, así, compartir nuestra red hogareña.

Otro sistema que es muy utilizado es el **satelital**. Comúnmente, lo podemos encontrar en lugares donde el acceso con otra tecnología es casi imposible (por ejemplo, en pueblos o ciudades de montaña). También es una solución costosa para concretar una comunicación donde se intercambia información en ambos sentidos.

De manera diferente, la tecnología empleada en redes inalámbricas (**espectro esparcido**), al ser usada en frecuencias en el rango de las microondas, permite crear enlaces de alta velocidad con un bajo costo.

Por consiguiente, podemos decir que usar la tecnología inalámbrica para enviar información a gran velocidad en largas distancias y con un bajo costo hace que sea una vía rentable para tener en cuenta a la hora de evaluar la unión de puntos distantes.

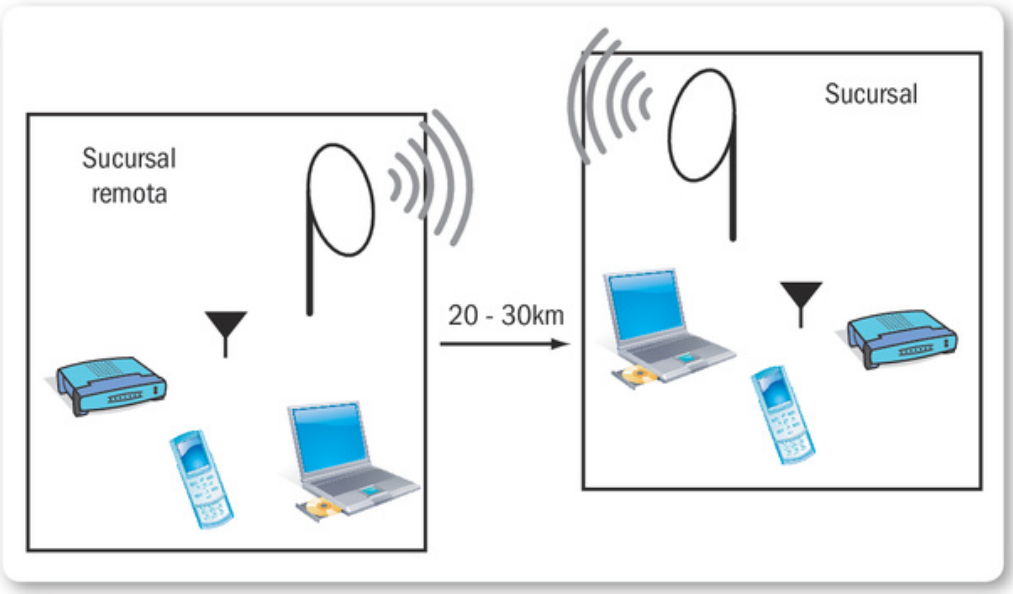


Figura 3. El objetivo del radioenlace es extender una red LAN que utiliza tecnología inalámbrica para vincular un destino aislado.

RADIOPAQUETE

Radiopaquete son técnicas para transmitir datos sobre enlaces de bajo costo. Desarrolladas por radioaficionados en los ochenta, se utilizaron con éxito para dar acceso a Internet a zonas remotas inaccesibles. Consiste en enviar señales digitales mediante pequeños paquetes que forman un mensaje.

¿Qué es un radioenlace?

Un enlace de larga distancia (también conocido como **enlace remoto**) es una conexión que usa tecnología inalámbrica (puntos de acceso, ruteadores y computadoras, entre otros) para enlazar equipos que se encuentran distantes. La separación de estos puntos por unir puede ir desde los cientos de metros hasta kilómetros. Por ejemplo, un enlace nos permitirá conectar una red LAN de nuestra oficina con otro edificio o lugar de la ciudad o área geográfica.

Si los equipos que se van a vincular son fijos, entonces el servicio se denomina **enlace remoto fijo**. Ahora, si algún equipo es móvil (nos referimos a que el dispositivo posee la capacidad de moverse dentro de un determinado rango o área de cobertura), entonces el servicio se conoce como **enlace remoto móvil**.

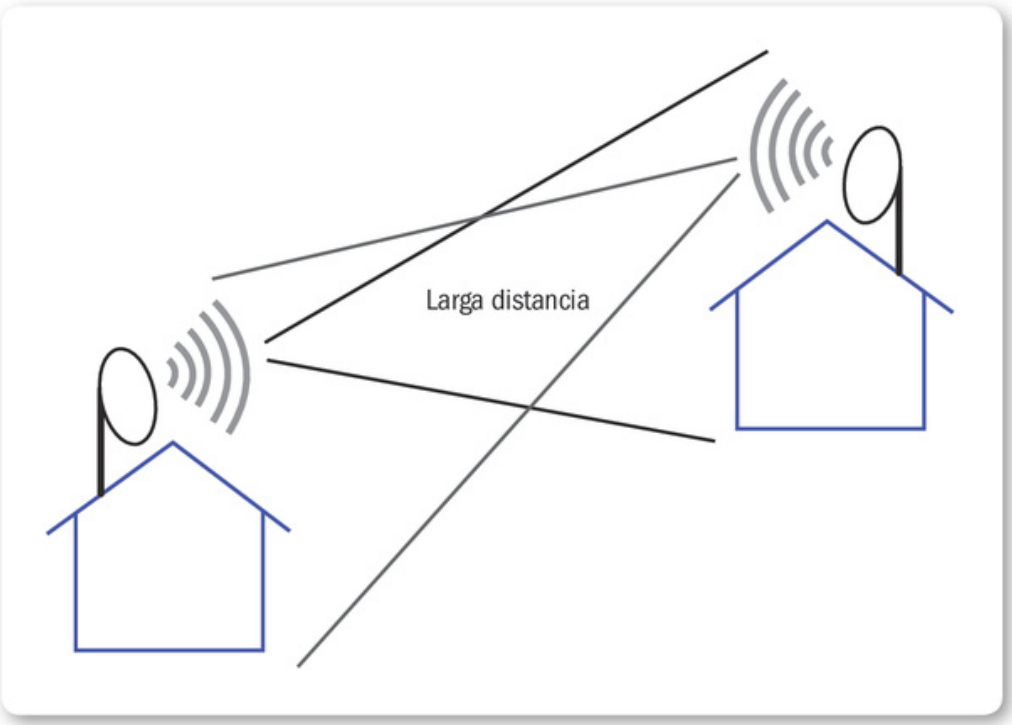


Figura 4. Ejemplo de un radioenlace fijo para unir dos hogares separados por un río. Las antenas permanecen fijas en un lugar.

Los radioenlaces establecen un concepto de comunicación del tipo **dúplex**. Para aclarar este último término, digamos que la palabra

dúplex es utilizada para definir a un sistema que puede mantener una comunicación bidireccional. O sea, que el sistema **dúplex** enviará y recibirá mensajes de forma simultánea.

De modo informativo, vamos a definir las tres categorías de comunicaciones o sistemas según la capacidad de transmitir de forma total o parcial en modo dúplex.

1. **Dúplex** (**Full duplex**): casi todos los sistemas modernos de comunicaciones funcionan en modo dúplex. De esta manera permiten tener canales de envío y recepción simultáneos.

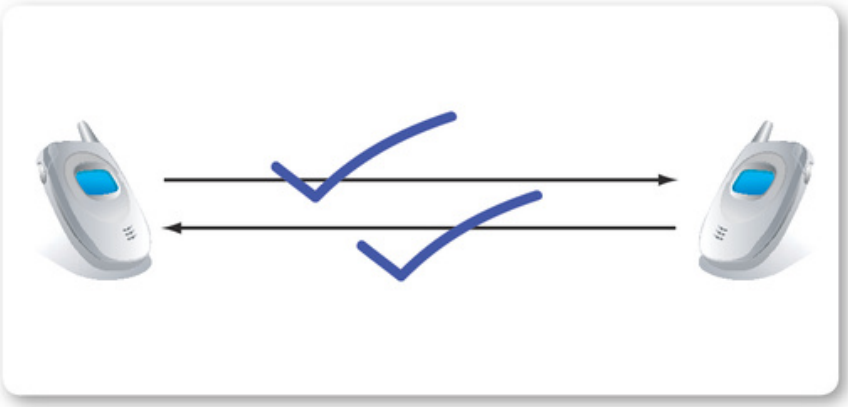


Figura 5. Ejemplo de comunicación dúplex donde ambos extremos pueden enviar y recibir mensajes simultáneos.

2. **Semidúplex** (**Half duplex**): existen sistemas que pueden transmitir en los dos sentidos, pero no lo hacen de forma simultánea. Así, puede ocurrir que en una comunicación con equipos de radio, uno no pueda hablar (transmitir un mensaje) si la otra persona está también hablando (transmitiendo). Esto es debido a que su equipo está recibiendo (en modo escucha) un mensaje en ese momento.

RADIOPAQUETE DESDE LOS AÑOS 60

Packet radio existe desde mediados de los 60. La Universidad de Hawai se basó en Packet radio para construir la red **ALOHA** en 1970. Llamaba la atención el uso de un medio compartido para la transmisión. Su objetivo era facilitar las comunicaciones entre la PC central y las PCs de la universidad dispersas.

3. **Símplex**: en este caso, debemos tener en cuenta que únicamente es posible realizar la transmisión en un solo sentido.

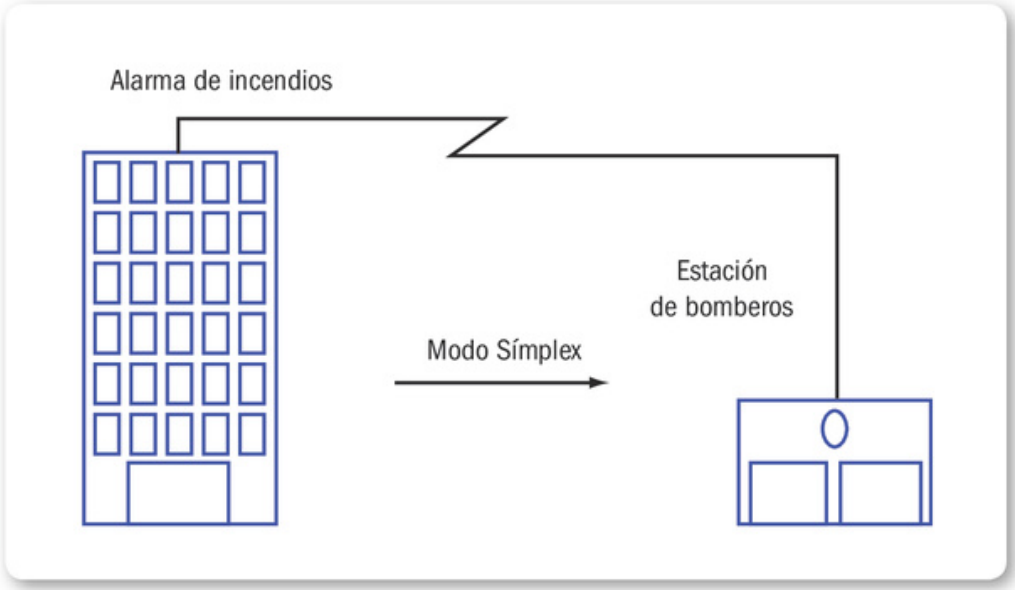


Figura 6. Un claro ejemplo de un modo símplex es cuando se acciona la alarma de incendios en un edificio para dar aviso a los bomberos.

En nuestro radioenlace dúplex de larga distancia tendremos asignadas un par de frecuencias para la transmisión y recepción de señales. A esto se lo denomina **radio canal**.

Un punto importante a destacar es que todos los enlaces se realizan, básicamente, entre puntos distantes visibles. Con esto queremos decir que ambos extremos del enlace deben ser puntos altos en la topografía (recordemos que topografía es la ciencia que estudia los procedimientos para representar gráficamente la superficie de la tierra).

No importa cuán grande o pequeño sea nuestro enlace, para que funcione correctamente debemos asegurarnos de que exista la altura adecuada en los extremos. Además, vamos a tener en cuenta otros parámetros que estudiaremos más adelante en este capítulo y que se relacionan con las variaciones de las condiciones atmosféricas de cada región. Hay que tener presente que para calcular las alturas adecuadas, debemos conocer la **topografía** del terreno. Además, es importante tener en cuenta la ubicación y altura de obstáculos que puedan existir en el trayecto de nuestro radioenlace, como árboles y edificios.

Tipos de enlaces

En los sistemas de telecomunicaciones donde se emplean los radioenlaces para transportar la información podemos definir varios tipos de radioenlaces según ciertos parámetros. Por ejemplo, según las frecuencias utilizadas podemos decir que existen:

- **Radioenlace infrarrojo**
- **Radioenlace UHF**
- **Radioenlace de onda corta**
- **Radioenlace de microondas**
- **Radioenlace satelital**

Vamos a centrarnos en los radioenlaces por microondas, que comprenden una escala de frecuencias entre 2 y 40 GHz. De modo informativo, decimos que los equipos que utilizan frecuencias cercanas a los 12 GHz, 18 GHz o 23 GHz pueden enlazar dos puntos separados por 1 a 25 kilómetros, aproximadamente. Los equipos que trabajan con frecuencias entre 2 GHz y 6 GHz logran transmitir información entre distancias de 30 a 50 kilómetros.

Dada esta gama de frecuencias a utilizar, es necesario que las antenas que intervienen en el enlace de larga distancia (mediante una antena emisora y una antena receptora) no tengan obstáculos entre ellas. Cuando se logra que no existan obstáculos en el medio, se dice que existe **línea visual libre** (**Line of Sight**).

En este sentido también es común que, para enlaces de muy largas distancias, se utilicen repetidores. De esta manera, un radioenlace se encuentra formado por equipos terminales y repetidores intermedios (en caso de ser necesarios por la distancia).

Los repetidores tienen una función simple, conseguir que la señal recibida sea enviada nuevamente a mayor distancia. De esta forma



ENLACE SATELITAL

Los satélites artificiales revolucionaron a las telecomunicaciones. Con ellos se difunden imágenes en directo y datos a larga distancia. En general, los satélites en órbitas a unos 35.000 km (órbita geoestacionaria) están conformados por uno o más receptores y transmisores que cumplen la función de un enorme repetidor de microondas.

estarían salvando la falta de visibilidad que puede existir por obstáculos o por la curvatura de la Tierra.

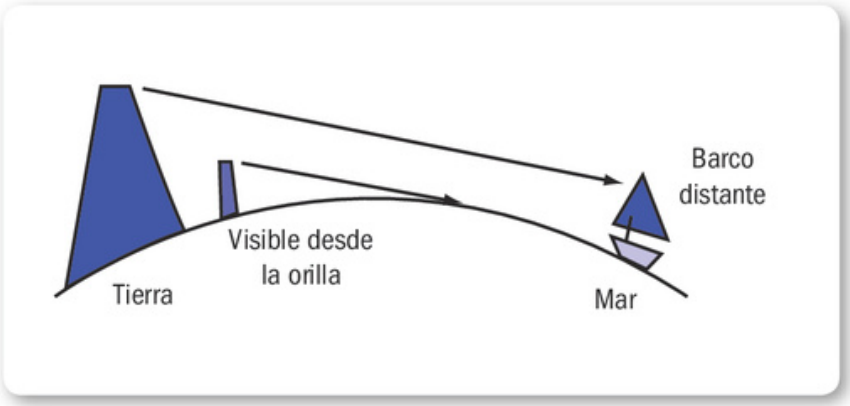


Figura 7. La curvatura de la Tierra es un factor determinante en puntos que necesitan unirse con línea visual directa.

Podemos clasificar a los **repetidores** usados en un radioenlace como:

- **Repetidores activos**
- **Repetidores pasivos**

Decimos que los **repetidores activos** son aquellos que reciben la señal, la amplifican en una etapa (en algunos casos se regenera la señal si es necesario) y luego la retransmiten.

En cambio, los repetidores pasivos se encargan de repetir la señal sin cambiar nada. Simplemente realizan la tarea de hacer rebotar la señal recibida en una superficie espejo o también acoplando dos antenas espalda con espalda (procedimiento también llamado **Back to Back**).

> LOS REPETIDORES ACTIVOS SON AQUELLOS QUE AMPLIFICAN LA SEÑAL RECIBIDA

De esta forma, los **repetidores pasivos** suelen utilizarse cuando se necesita cambiar de dirección una señal y no es posible (o es muy costoso) instalar un repetidor activo.

Debemos tener en cuenta que la forma general de diferenciar a los radioenlaces es por la cantidad de nodos que intervienen en el vínculo. Así, podemos tener un enlace **punto a punto** (PaP) o **punto a multipunto** (PaM).

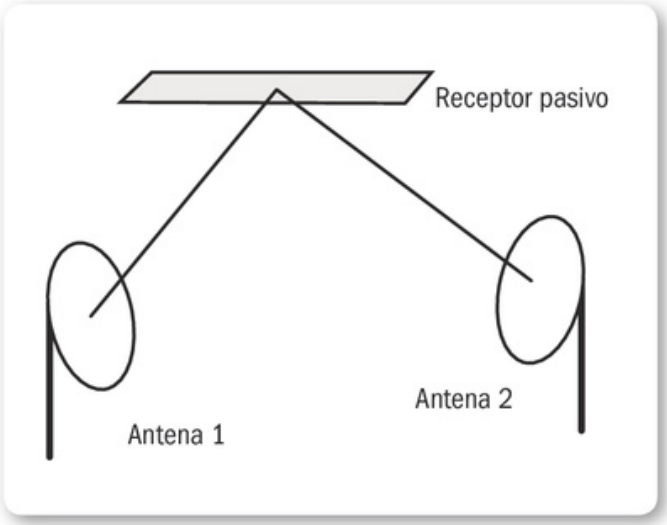


Figura 8. Vemos en la imagen una de las formas de implementar un radioenlace utilizando un repetidor pasivo.

Punto a punto

En este tipo de enlaces, solamente intervienen dos nodos. Estos nodos pueden ser de transmisión o de recepción, donde se interconectan dos computadoras o dos redes.

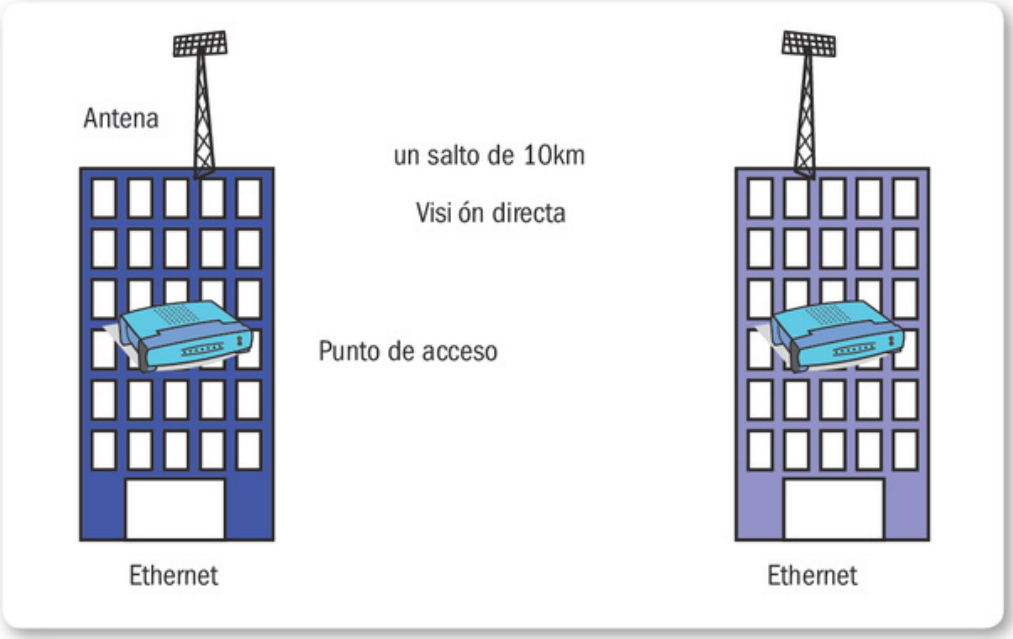


Figura 9. Un enlace punto a punto es simple cuando consta de un solo salto; esto es, la cantidad de sistemas para lograr el destino.

Para este tipo de enlaces punto a punto, se utilizan **antenas direccionales**. Para continuar, nos encargaremos de realizar la descripción de cada una de las características presentes en las antenas conocidas como direccionales.

Podemos encontrar las antenas direccionales con el nombre de **unidireccional** o **directiva**. Son antenas capaces de concentrar la energía radiada de forma localizada. En otras palabras, orientan la señal inalámbrica en una dirección con un haz estrecho pero de largo alcance. Así, se envía información a una cierta **zona de cobertura**, a un **ángulo determinado**, por lo cual su alcance es mayor. Sin embargo, fuera de esa zona de cobertura no se obtiene señal (dado su direccionalidad) y no se establece la comunicación entre los puntos.



Figura 10. Ejemplo de antena parabólica. Estas antenas tienen mejor rendimiento cuando necesitamos concentrar la información en una dirección deseada.

Las antenas se conectan al punto de acceso donde la potencia y otros factores determinarán el alcance del radioenlace. La potencia del punto de acceso (o puede ser otro elemento, como una placa de red inalámbrica) es un factor importante en los radioenlaces. Se define como

la potencia (medida en decibeles o milivatio) que entrega el dispositivo emisor a la salida de antena. Esta potencia es configurable en la mayoría de los equipos inalámbricos por medio del **software de gestión**.

Hay una gran variedad de **antenas direccionales** en el mercado, pero si se usan **antenas parabólicas** (son las de mayor direccionalidad), podremos alcanzar grandes distancias (desde metros hasta 50 o más kilómetros); todo dependiendo de los equipos utilizados y la información que vayamos a transmitir.

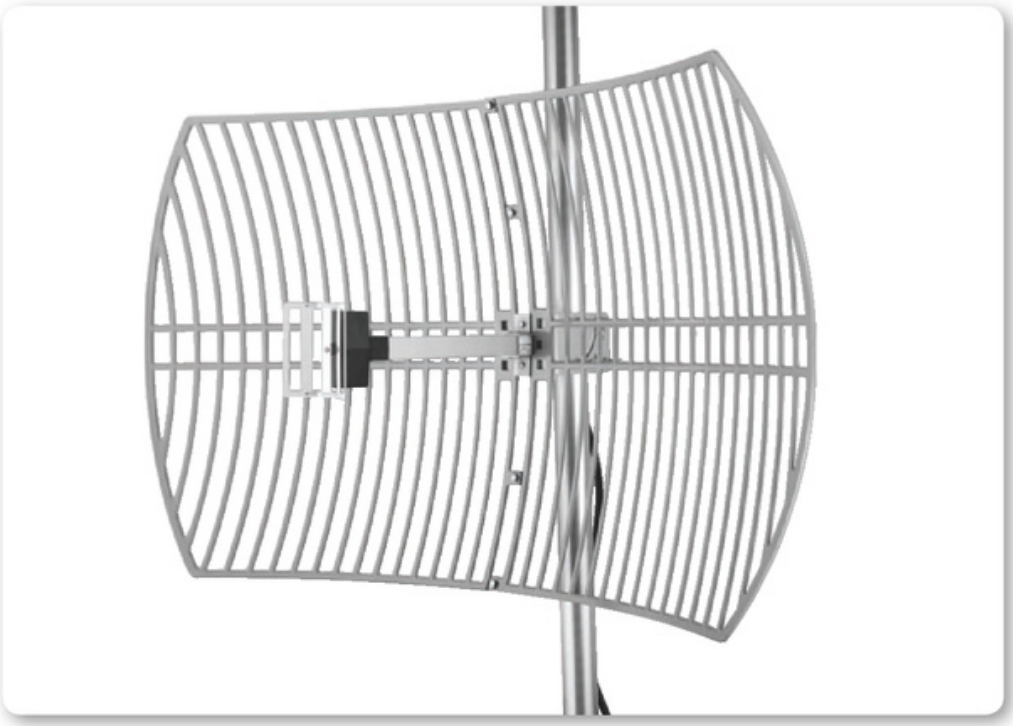


Figura 11. Antena direccional (**grid** o **parrilla**). Es similar a la **parabólica convencional**, y se utiliza en zonas de fuertes vientos.

CAOS EN EL CIELO

Existen acuerdos internacionales para prevenir un posible **caos en el espacio** con respecto a las frecuencias utilizables en las transmisiones con satélites. Las bandas de 3.7 a 4.2 GHz y de 5.925 a 6.425 GHz se utilizan para flujos de información provenientes del satélite o hacia el satélite, respectivamente. Se suele llamar a estas frecuencias **bandas 4/6 GHz**.

Punto a multipunto

En este caso, el enlace se llama **punto a multipunto** y sirve para enlazar diferentes puntos remotos hacia un punto central. Consta de un nodo realizando funciones de transmisor y más de un receptor como destino. Así, se interconectan varias redes o computadoras distantes. También se puede utilizar para conformar zonas de cobertura de señal donde podremos distribuir, por ejemplo, Internet, voz (telefonía) y datos.

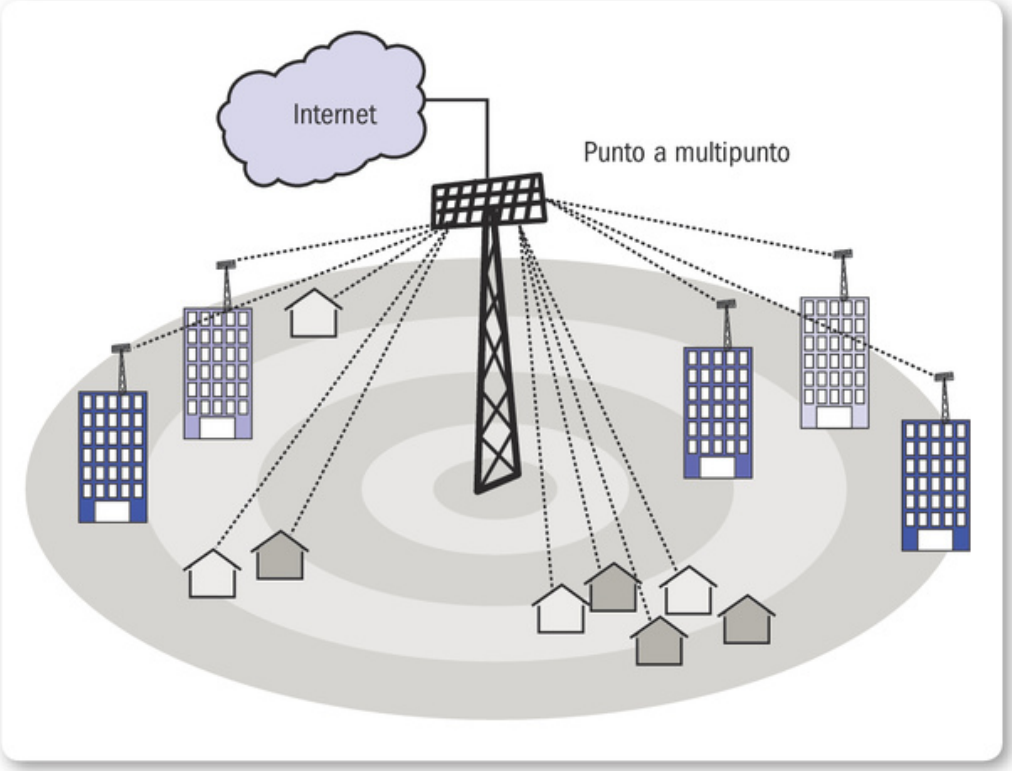


Figura 12. En un enlace punto a multipunto logramos zonas de cobertura para enlazar varios puntos.

¿ANTENA PARABÓLICA O PANEL?

En general se prefiere utilizar antenas panel cuando no existen grandes distancias u obstáculos en el medio del enlace. Cuando se necesita un sistema con mayor rendimiento, debemos usar antenas parabólicas. Así, podemos empezar un enlace punto a punto con antena panel y luego, si las circunstancias lo requieren, cambiarla por una parabólica.

Las antenas que podemos usar en el nodo transmisor son las que **irradian energía** en todas las direcciones (conocidas como omnidireccionales) o varias antenas sectoriales (las cuales solamente irradian para un sector determinado) conectadas a un punto de acceso que tenga muy buena potencia.

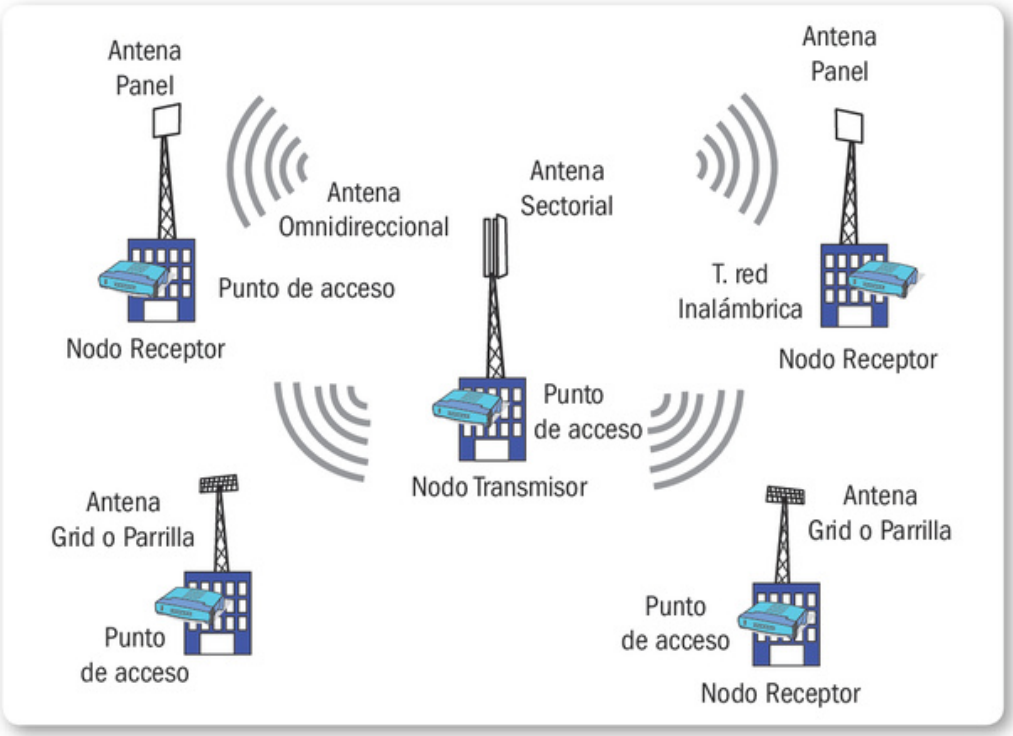


Figura 13. El enlace punto a multipunto es ideal para implementarlo en edificios esparcidos sobre un área local extensa.

Si vemos el lado del receptor, destacamos el uso de antenas de diferentes tipos y ganancias. Recordemos que la ganancia de antena es la potencia de amplificación de una señal. En general, cuanto mayor es la ganancia, mejores son la antena y la recepción de la señal. Estas características dependen de la distancia existente desde el nodo transmisor. Las antenas pueden ser las llamadas antenas panel (**panel antenna**) o las antenas grid, que vimos anteriormente. Se conecta la antena a un punto de acceso en el lado receptor, aunque si la distancia es muy corta, es posible conectar directamente la antena a la placa de red inalámbrica de la computadora. También depende de lo que estemos transmitiendo; en este ejemplo, al conectar la antena a la

placa inalámbrica, suponemos que se transmite la señal de Internet. En esta configuración se prescinde del uso de un punto de acceso, lo que resulta en una configuración más económica.



Figura 14. Las antenas sectoriales son de fácil fabricación y montaje, lo que las transforma en antenas de bajo costo y gran rendimiento.

El enlace punto a multipunto nos permite reducir costos, dado que es un sistema que consta de un nodo central donde está el transmisor a donde apuntan las antenas direccionales de los receptores (otras oficinas distantes). La capacidad obtenida es igual al enlace punto a punto, pero más extensible a varios puntos destino, en una menor distancia.

VENTAJAS SATELITALES

En las comunicaciones que usan satélites la mayor ventaja es la gran capacidad de transmisión de datos. Además, proporcionan una cobertura muy amplia con un costo independiente de la distancia de los puntos por unir. Recordemos que la televisión satelital es otra área fuerte donde se usan satélites.

Alineación de antenas

Veremos cómo realizar, de forma general, la alineación de las antenas cuando estamos por efectuar un enlace inalámbrico de gran distancia. Al trabajar con antenas muy directivas (concentran el haz de la señal de forma eficaz) a grandes distancias, necesitamos emplear algún método para alinearlas correctamente y así enviar y recibir la información con las menores pérdidas posibles. Ahora supongamos que existe línea visual y adecuada zona de Fresnel en la trayectoria que estamos tratando de unir con un radioenlace. Podemos consultar en Internet cómo alcanzar el objetivo de la zona de Fresnel; no lo explicamos aquí dado que escapa al objetivo de este libro.

Con extremos visibles

Cuando la situación de nuestro enlace nos permita ver el otro extremo (distancias cortas, por ejemplo), realizar la alineación de las antenas es una tarea sencilla. En este caso, simplemente deberemos **alinear visualmente** ambas antenas y, de esta forma, procedemos a efectuar la constatación de los resultados con alguna herramienta especialmente diseñada para este propósito.

Vimos herramientas como **NetStumbler** anteriormente, y en este caso también podemos utilizarla. Con esta aplicación vamos a medir la **intensidad de la señal** en el receptor, para así realizar un ajuste fino de la orientación de la antena. De este modo, siempre buscamos obtener el máximo punto de recepción.

Por otra parte, si trabajamos en equipo junto con otra persona, podremos comunicarnos por medio de un **celular** para hacer las correcciones que consideremos necesarias.

BANDAS SIN LICENCIAS

Los enlaces inalámbricos trabajan en bandas de frecuencia que no requieren licencia. Esto implica que no se tiene protección alguna del ente regulador de cada país. Recomendamos analizar el estado del espectro donde queramos implementar el enlace y la banda que vamos a utilizar. En zonas rurales no hay mucha congestión en la banda de 2.4 GHz, como en las ciudades.

Algunas herramientas que podemos usar para orientar las antenas son:

- Teléfono celular o similar para poder comunicarnos con el otro extremo del enlace.
- Computadora con el programa NetStumbler o similar para medir la intensidad de la señal recibida.
- **Binoculares**.

El procedimiento es bastante sencillo. Una vez instaladas las antenas y los equipos en sus respectivos extremos del enlace, conectamos la alimentación e iniciamos los dispositivos. Por ejemplo, en el extremo 1 tenemos el punto de acceso configurado, y en el extremo 2, una computadora que actúa como **cliente inalámbrico**. Una vez que la señal es recibida en el extremo 2, vamos a medir la intensidad recibida con **NetStumbler** u otro programa que cumpla las mismas funciones. Debemos tener presente que la señal que nos llega al cliente figura en dBm y es **negativa**; por lo tanto, mientras más grande es el número, más chica es la señal (tengamos en cuenta que algunos programas pueden indicar el nivel de señal recibida como un porcentaje; entonces, cuanto mayor sea el porcentaje, mayor será la señal).

> NETSTUMBLER ES UN PROGRAMA QUE SIRVE PARA MEDIR LA INTENSIDAD DE LA SEÑAL RECIBIDA

Realizamos los siguientes pasos:

1. En el extremo 1 dejamos la antena fija y movemos la antena del extremo 2 muy lentamente para un solo lado, mientras observamos la intensidad de la señal que nos llega. Cuando encontramos el **máximo**, dejamos fija la antena del extremo 2 asegurándola con alguna **abrazadera** o similar.
2. Realizamos lo mismo pero moviendo lentamente la antena del extremo 2 hacia arriba o abajo (esto es para buscar el **ángulo de elevación óptimo** dadas las diferencias en las alturas de las antenas).

Una vez terminado el procedimiento en esta antena, realizamos lo mismo en el extremo 1. Muchas veces es necesario repetir el procedimiento para lograr el punto óptimo.

Ahora podemos realizar pruebas de transmisión haciendo uso del comando **ping**, y de esta forma, ver las pérdidas de **paquetes** y el tiempo de transmisión existente en el proceso.

Con extremos no visibles

En caso de no tener los extremos visibles (puede ser porque nuestro enlace se encuentra en un área muy extensa), la alineación de las antenas llevará un poco más de tiempo.

Además de lo listado anteriormente podemos llegar a necesitar:

- Un **GPS**, que nos sirve para medir la distancia de los puntos y también la altura del terreno.
- Una **brújula**.
- El programa Radio Mobile (que veremos luego en este capítulo).
- **Mapas** de la zona.
- Si no contamos con los mapas, podemos recurrir al programa **Google Earth**, donde se ven muchos detalles topográficos.

Si utilizamos **Google Earth** o Radio Mobile para determinar cuál es el rumbo correcto al que debemos apuntar las antenas en cada extremo, procederemos a realizar los mismos pasos vistos anteriormente para medir la intensidad de la señal en el receptor.

Enlaces de corta distancia

Los enlaces de corta distancia son redes inalámbricas implementadas en un área que abarca pequeñas dimensiones. Anteriormente definimos una red inalámbrica como un vínculo entre dos o más terminales que se comunican sin necesidad de utilizar cables. Tal como describimos, existen varias tecnologías que se diferencian por la frecuencia de transmisión que usan, el alcance y la velocidad de transmisión. Según el área de cobertura de la red, podemos clasificar las redes inalámbricas en varias categorías. Más adelante en este capítulo, nos encargaremos de ver las redes inalámbricas de área personal.

Una **red inalámbrica de área personal** (**Wireless Personal Area Network** o **WPAN**) es una red que cubre distancias cercanas a los 10 metros. En general, se la utiliza para vincular dispositivos que necesitan cierta movilidad y son de uso personal, en los que podemos prescindir de los cables. Estas redes WPAN conectan dispositivos como impresoras, teléfonos celulares, electrodomésticos, notebooks y agendas, entre otros, sin tener que utilizar cables.

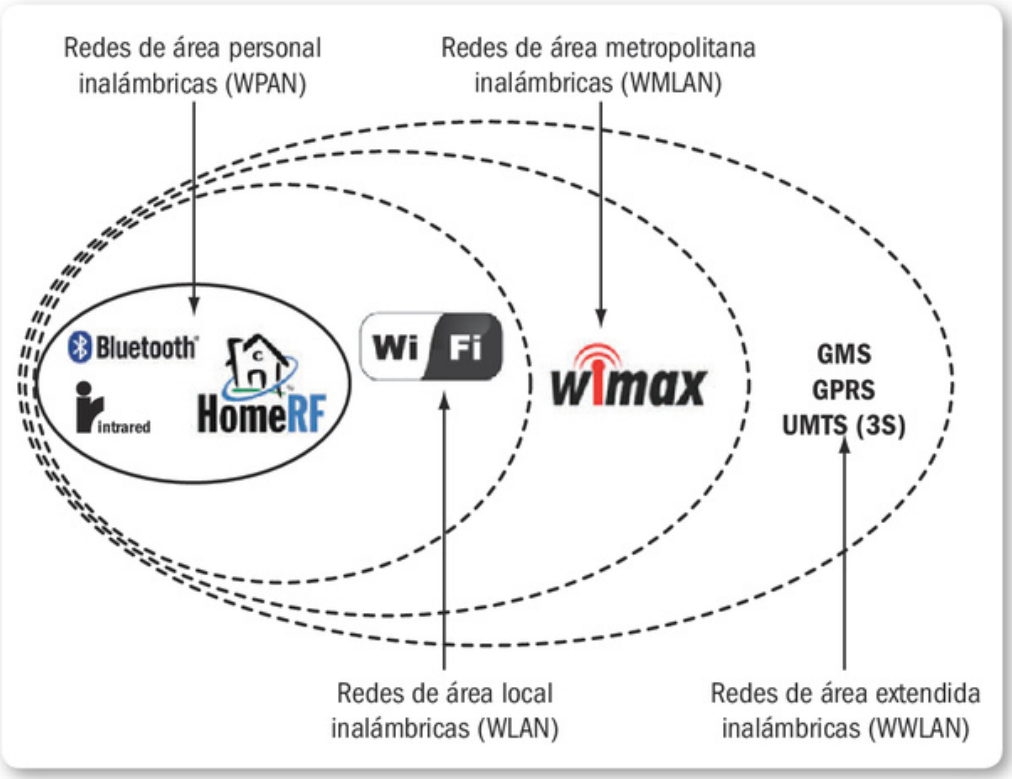


Figura 15. Una red inalámbrica de área personal se desarrolla donde el área de cobertura no supera los pocos metros.

Las comunicaciones punto a punto de corta distancia pueden ocurrir ya que, comúnmente, no se requiere de altos índices de transmisión de datos. El éxito de estas comunicaciones de corta distancia reside en que se pueden implementar con dispositivos pequeños, como por ejemplo, los teléfonos celulares, que funcionan con batería. Dado que no existe un alto consumo de energía para comunicarnos en una red **WPAN** (esto es por la corta distancia y la velocidad), podemos usar nuestros teléfonos sin preocuparnos por el gasto de la batería.

BLUETOOTH

La tecnología que hoy en día más se usa en redes WPAN es **Bluetooth**, que fue lanzada por la empresa Ericsson en 1994. La velocidad máxima que puede ofrecer es de 1 Mbps con un alcance que ronda los 10 metros (según el lugar). También se pueden lograr los 2 o 3 Mbps, si se usan técnicas específicas.



Figura 16. Las WPAN son redes que tiene como centro al usuario, y que permiten la comunicación entre dispositivos y el mundo exterior.

Estas redes nacieron de la necesidad que tenían los usuarios de desarrollar una forma rápida, confiable y eficiente para transferir información sin los molestos cables que vinculan los dispositivos hogareños hoy en día. Esta solución tomó el nombre de WPAN, y tiene la característica de orientar sus sistemas de comunicación en un área de algunos metros a la redonda, tomando como centro al **usuario** o dispositivo en movimiento o estático.

En comparación con las redes inalámbricas vistas anteriormente, las WPAN casi no necesitan de una infraestructura (puntos de acceso, routers o similares) para implementarse.

Los grupos de trabajo de la IEEE

Enfocados en la búsqueda de satisfacer diferentes necesidades de comunicación dentro de un área de implementación personal, la **IEEE** formó diferentes grupos de trabajo específicos.

El **IEEE 802.15** es un grupo de trabajo que está enmarcado dentro del estándar IEEE 802, especializado en redes inalámbricas de área personal. Existen cinco subgrupos de trabajo para la tecnología **WPAN** que a continuación veremos de forma general, nombrando algunas de sus características específicas más importantes.

- **IEEE 802.15.1** (WPAN/Bluetooth): este estándar se desarrolla basándose en la especificación 1.1 de Bluetooth. El IEEE 802.15.1 se publicó el 14 de junio de 2002.
- **IEEE 802.15.2** (Coexistencia): se estudian los posibles problemas que aparecen al coexistir las WPAN con otras redes inalámbricas locales (WLAN) o diferentes dispositivos que usen bandas de frecuencias similares. Es un estándar del año 2003.
- **IEEE 802.15.3** (WPAN de alta velocidad): para lograr mayores velocidades en las WPAN se trabaja en este estándar. De la misma forma, se investiga para lograr bajos consumos de energía y también soluciones de bajo costo. De esta forma, se quiere alcanzar velocidades de 20 Mbps o aún más.
- **IEEE 802.15.4** (WPAN de baja velocidad): este grupo trata las necesidades de sistemas donde se requiere poca velocidad de transmisión de datos pero muchas horas (o incluso meses) de vida útil de la batería del dispositivo. El protocolo **ZigBee** se basa en la especificación producida por este grupo de trabajo.
- **IEEE 802.15.5** (redes en malla): se trata de un grupo que se ocupa de todos los puntos necesarios para formar una red con topología en malla usando la tecnología WPAN. Recordemos que este estándar hace su aparición en el año 2009.

> LOS PROBLEMAS AL COEXISTIR WPAN CON REDES INALÁMBRICAS LOCALES AÚN ESTÁN EN ESTUDIO

AMPLIFICADOR DE ANTENA

Un **amplificador de antena** (antenna booster) es un dispositivo diseñado para amplificar la señal recibida. La idea básica de funcionamiento es lograr expandir el área de recepción de la antena. De este modo, puede capturar señales débiles. La forma más simple del amplificador es un tramo de cable que incrementa la longitud de la antena.

¿Dónde se aplica la tecnología WPAN?

Este estándar se pensó para ser aplicado en varios ámbitos. Por ejemplo, en nuestro hogar es muy común contar con algunos **periféricos** de la computadora (mouse, teclado o similar) que ya disponen de este tipo de tecnología usando Bluetooth. Además, la mayoría de los teléfonos celulares actuales poseen Bluetooth para vincularse, así como las agendas electrónicas o **joysticks de consolas** de video. Televisores, reproductores de DVD, controles remotos, radios y demás dispositivos electrónicos del hogar cuentan con esta tecnología. Todo esto nos permite tener un hogar totalmente automatizado. Existen, dentro de la automatización del hogar, sistemas de calefacción, ventilación, aire acondicionado y portones que utilizan los avances de este tipo de tecnologías.

En algunos casos se requiere un rango mayor de área de cobertura; por este motivo se está trabajando para lograr rangos desde los pocos metros hasta más allá de los 100 metros.

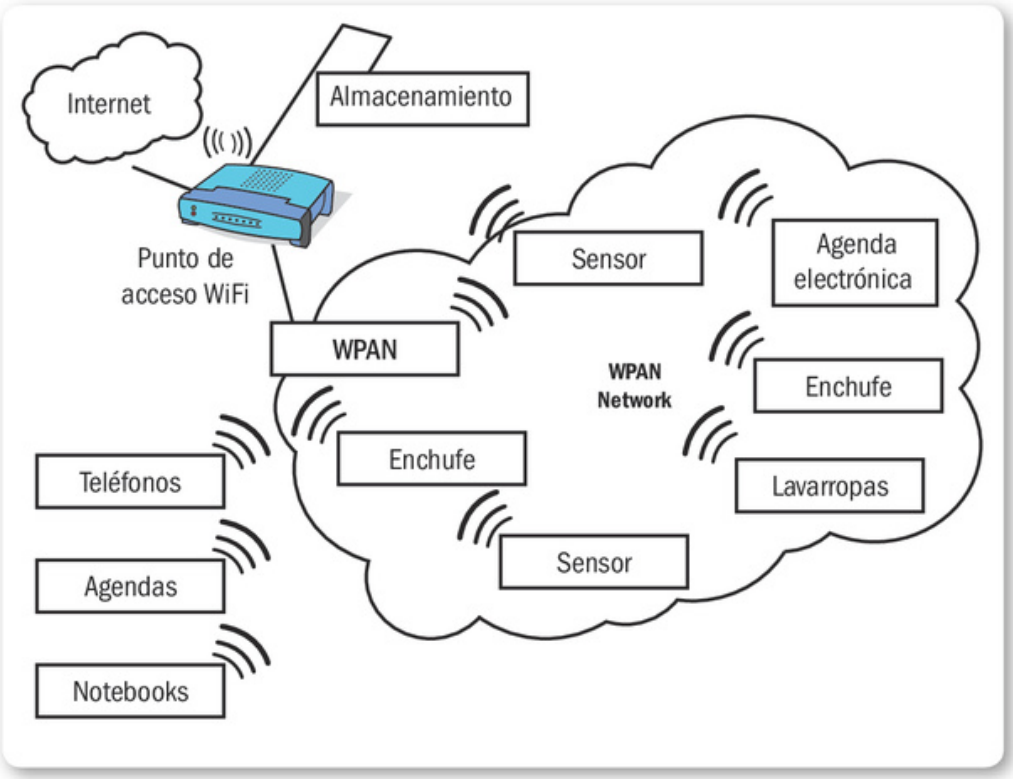


Figura 17. En un hogar del futuro podremos tener control total utilizando la tecnología que nos provee una WPAN.

Bluetooth: ¿qué es y cómo funciona?

Para comprender todo sobre **Bluetooth**, conozcamos la historia de esta tecnología. En 1994, **Ericsson** comenzó una investigación donde buscaba desarrollar una nueva técnica de comunicación vía ondas de radio, que fuera **barata**, que consumiera poca energía y que permitiera la interconexión entre teléfonos celulares y otros dispositivos. La idea que se perseguía era la de eliminar los cables entre dispositivos.

La tecnología Bluetooth es hoy en día un estándar abierto global para enlazar dispositivos por medio de ondas de radio, que ofrece, de manera económica y sencilla, transmisiones de voz y datos entre dispositivos. Bluetooth se puede incorporar en la gran mayoría de los aparatos electrónicos y ofrece una nueva forma de comunicación sin necesidad de cables; es compatible con cualquier fabricante (conseguimos la **interoperabilidad** entre diferentes dispositivos).



Figura 18. Ejemplo de conectividad Bluetooth. Se intenta alcanzar la conectividad total para dispositivos de la casa y oficina.

De esta forma, los dispositivos que utilizan **Bluetooth** pueden comunicarse entre sí cuando se encuentran dentro de su alcance. Ya que las comunicaciones se realizan usando ondas de radio, los

dispositivos involucrados no tienen que estar alineados (hasta pueden llegar a estar en lugares separados por paredes en caso de que la potencia de transmisión lo permita).

Según la potencia de transmisión de cada dispositivo, podemos clasificarlos en **Clase 1**, **Clase 2** y **Clase 3**. Tengamos en cuenta que existe compatibilidad entre las diferentes clases.

COBERTURA

CLASE	POTENCIA MÁXIMA PERMITIDA (MW)	POTENCIA MÁXIMA PERMITIDA (DBM)	ÁREA DE COBERTURA
1	100 mW	20 dBm	100 m aprox.
2	2.5 mW	4 dBm	10 m aprox.
3	1 mW	0 dBm	1 m aprox.

Tabla 1. Esta tabla muestra el área de cobertura según la potencia utilizada por cada una de las clases para Bluetooth, con otros datos importantes.

Topología de red

Un punto para destacar en Bluetooth es la topología de red utilizada, ya que se introduce un nuevo concepto llamado **piconets** (también se puede encontrar como **picoredes**). Cuando un dispositivo se encuentra dentro del área de cobertura de otro, se puede concretar una conexión inalámbrica con Bluetooth. Dos o más dispositivos **Bluetooth** que comparten un mismo canal forman una **piconet**. Uno de los dispositivos asumirá el rol de maestro, y los otros serán esclavos (por defecto, el dispositivo que establece la piconet asume el papel de maestro, y los demás quedan como esclavos). Se pueden intercambiar los roles entre los participantes en caso de que un dispositivo esclavo quiera ser maestro. De todas formas, solo es posible que exista un dispositivo maestro en la piconet al mismo tiempo.

Cuando varias piconets existen dentro del mismo lugar físico, se superponen las áreas de cobertura. Así, nace un nuevo concepto llamado **scatternet**, que son un grupo de piconets.

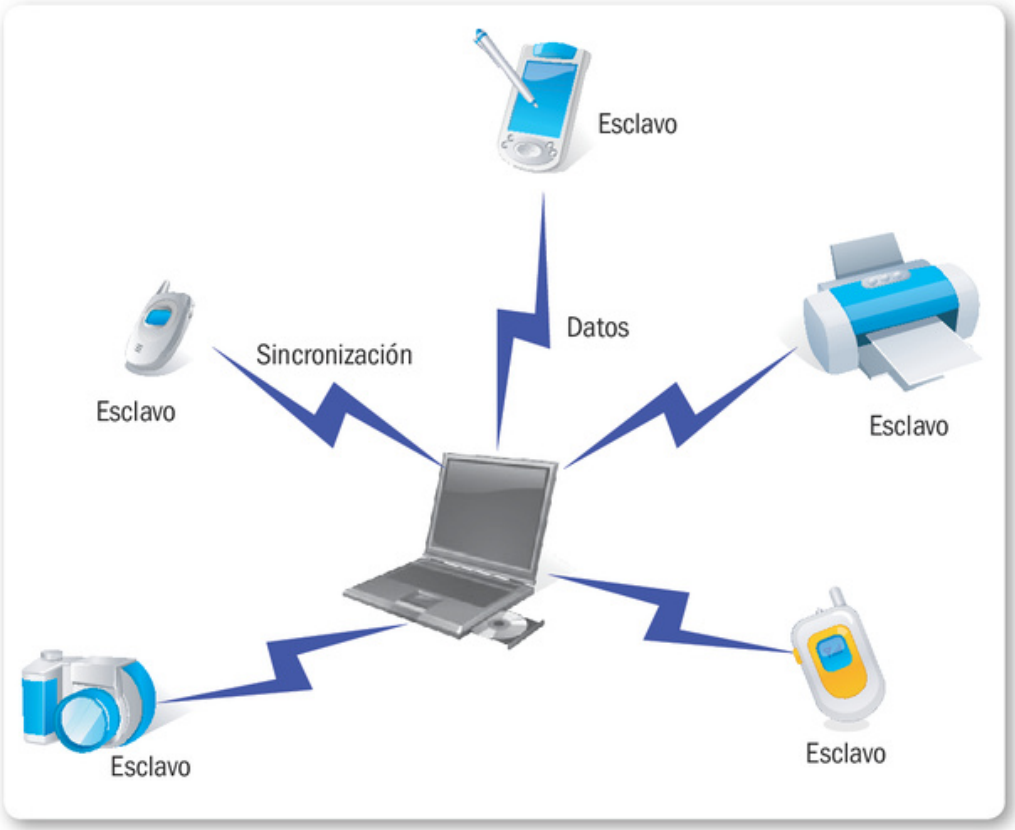


Figura 19. Esquema de conexión de varios dispositivos Bluetooth que forman una piconet.

RESUMEN

A lo largo del capítulo vimos todo lo necesario para completar de forma práctica un enlace inalámbrico a larga distancia. Clasificamos los tipos de radioenlaces posibles pero nos centramos en el enlace inalámbrico de larga distancia punto a punto, ya que es el más común de implementar. Luego evaluamos los factores importantes para concretar nuestro enlace y describimos cómo realizar el cálculo del enlace. Por último, utilizamos el software gratuito Radio Mobile para simular un enlace. Este programa ofrece una gran cantidad de opciones y nos permite simular un enlace de larga distancia.

Actividades

TEST DE AUTOEVALUACIÓN

1. Defina qué entiende por radioenlace.
2. ¿Qué es un radioenlace fijo?
3. ¿Qué es un radioenlace móvil?
4. ¿Cómo se define una comunicación Full Dúplex?
5. ¿Cómo se representa la topografía de un lugar?
6. ¿Qué es la sensibilidad del transmisor?
7. ¿Qué acciones se pueden implementar para lograr una señal óptima en el receptor?
8. ¿De qué manera hacemos la alineación de las antenas cuando tenemos línea visual?
9. ¿Qué es el presupuesto de potencia?
10. ¿Cuál es la fórmula para calcular un enlace?

ACTIVIDADES PRÁCTICAS

1. Utilizando el programa Radio Mobile, seleccione dos puntos de su ciudad y márquelos en un mapa topográfico.
2. Implemente una red para ese mapa en la banda de frecuencias de 2.4 GHz.
3. Configure los parámetros restantes tomando datos de equipos reales (consulte en Internet) y verifique si el enlace es viable.
4. Modifique las alturas de las antenas e incremente la potencia del transmisor en caso de no ser viable el enlace anterior.
5. Utilice la fórmula adecuada para calcular un enlace.

*07

Antenas

En este capítulo veremos uno de los elementos más importantes en el esquema transmisor y receptor que conocemos, las antenas. Estudiaremos su historia, funcionamiento y características. Además, analizaremos las diferentes clasificaciones de estas: según su construcción y patrón de radiación.

- **Antenas 172**
  - Características específicas 172
- **Clasificación de las antenas .. 178**
  - Según el patrón de radiación 179
  - Según su construcción 180
- **Resumen..... 183**
- **Actividades..... 184**

Antenas

Las antenas poseen un aspecto muy importante que es el principio de la reciprocidad, el cual establece que el comportamiento de la antena cuando se transmite es igual al comportamiento cuando la antena realiza funciones de recepción.

Como dijimos antes, el objetivo de una antena es transferir la máxima energía posible desde el cable (que viene del transmisor en el caso de una antena transmisora) hacia la dirección donde está el receptor. Para lograr este objetivo, existe otro parámetro fundamental para tener en cuenta y es la **impedancia característica de antena**. Si logramos acoplar la impedancia característica de la antena a la impedancia del cable, lograremos la máxima transferencia de energía posible en nuestro sistema radiante. En cambio, si las impedancias son diferentes y no existe un acople perfecto, tendremos pérdidas y la energía radiada no será máxima. En este caso, puede existir la posibilidad de que energía residual (que no fue radiada) se refleje hacia atrás y vuelva hacia el transmisor (lo que puede causar serios daños a nuestros equipos).

> LA IMPEDANCIA ES FUNDAMENTAL PARA ENTENDER EL FUNCIONAMIENTO DE UNA ANTENA

Es importante lograr que las impedancias se acoplen cuando estamos trabajando con antenas. Dada la reciprocidad en las antenas, si la nuestra transmite máxima energía en una dirección, también recibirá la máxima señal en esa dirección.

Características específicas

Veamos algunas características específicas que encontraremos en las antenas, sin importar cuál sea su forma.

Impedancia característica de antena

Cuando una antena capta una onda electromagnética que viaja por el espacio libre y pasa del aire hacia la antena, se nota una oposición al avance de la onda en el elemento de la antena. Esto ocurre ya que el material del elemento de la antena tiene una resistencia que modifica la

onda original (además de resistencia, posee capacitancia e inductancia, pero no son parámetros que nos preocupen ahora). Lo mismo ocurre en las antenas emisoras, ya que cuando las ondas pasan del metal (elemento de antena) hacia el aire, sienten una resistencia que se presenta en su camino. Esto es la impedancia de una antena. El aire libre también tiene impedancia (resistencia al paso de las ondas), pero es despreciable en comparación con la de la antena.

Ganancia de antena

Antes de hablar específicamente de la ganancia de una antena, debemos comentar un concepto básico que necesitamos manejar para entender por completo este parámetro.

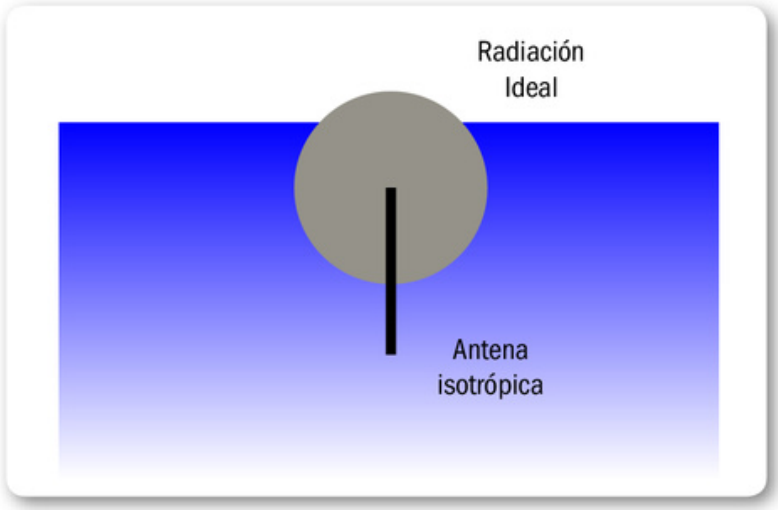


Figura 1. El modelo propuesto de antena isotrópica sirve para comparar la ganancia de nuestras antenas con el modelo teórico ideal, que irradia en forma de esfera.

ANTENAS DE HILO

Estas antenas se caracterizan por tener conductores de hilo como elementos radiantes. Se usan en las bandas de media frecuencia (medium frequency o MF), alta frecuencia (high frequency o HF), muy alta frecuencia (very high frequency o VHF) y ultra alta frecuencia (ultra high frequency o UHF).

Definiremos a una **antena isotrópica** como aquella que irradia (o recibe) energía desde todas las direcciones con igual intensidad. Este modelo de antena es ideal o teórico y no existe en la vida real, dado que ninguna antena irradia de igual forma en todas sus direcciones. Se puede hacer una analogía con la luz de una vela o una lámpara para entender cómo irradia una antena isotrópica.

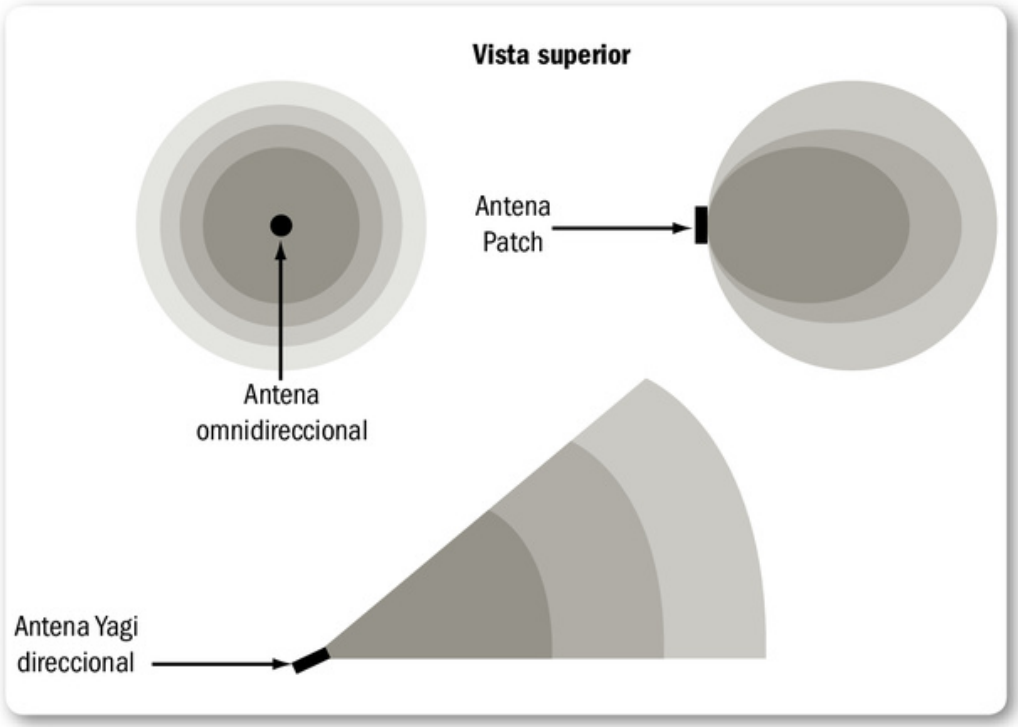


Figura 2. La vista superior de estas tres antenas muestra el diagrama de radiación, para ser directivas o no.

Usaremos este concepto de antena ideal para comparar con antenas reales y así determinar sus características. Entonces, si tenemos este concepto en mente, podemos definir la ganancia de una antena, que es el cociente entre la cantidad de energía irradiada en la dirección principal de nuestra antena y la que irradiaría una antena isotrópica alimentada por el mismo transmisor. Ya que estamos tomando la ganancia con relación a la antena isotrópica, expresamos el resultado en **dBi** (decibeles con relación a la antena isotrópica).

Como mencionamos anteriormente, al momento de diseñar una antena, necesitaremos dirigir la señal en cierta dirección. Por esto, las

antenas no se diseñan para irradiar energía en todas las direcciones, y sí, para hacerlo en una cierta área de cobertura. Para medir cuán directiva es nuestra antena, usamos el parámetro **ganancia de antena**. Cuanto más grande sea nuestra ganancia de antena, la antena será más directiva y el haz será más angosto.

Siempre hay que tener presente que nuestras antenas no pueden encargarse de amplificar las señales (ya que se trata de elementos definidos como pasivos) y que solamente concentran la señal en un haz para dirigirlos a cierta dirección específica.

Patrón de radiación de antena

La gráfica que muestra la potencia de la señal transmitida en función del ángulo se llama **patrón de radiación** (o en algunos casos, **diagrama de radiación**). Este gráfico presenta la forma y la ubicación de los lóbulos de radiación lateral y posterior, así como otros puntos donde la potencia irradiada es menor.

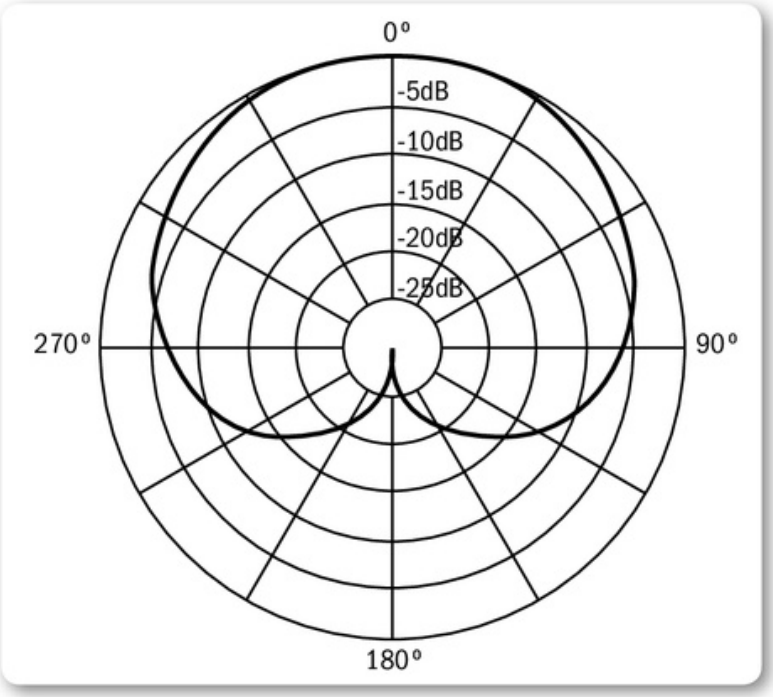


Figura 3. Diagrama de radiación direccional. Para este caso, el diagrama suele llamarse cardioide, ya que su forma es similar a un corazón.

Lo que se trata de hacer al diseñar una antena es reducir al mínimo los lóbulos extra (laterales y posteriores), porque no son de utilidad al momento de direccionar el haz. Si modificamos la geometría de la antena, lograremos esta reducción.

Otra representación posible de los diagramas de radiación es en **3D**.

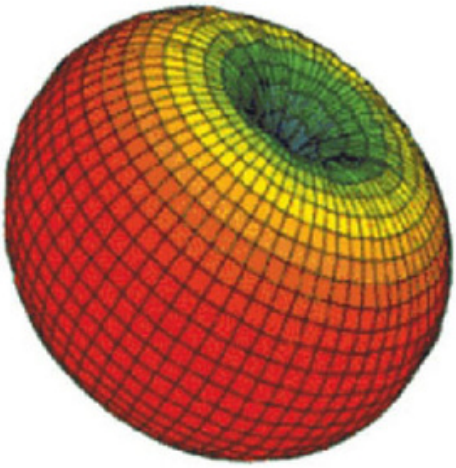


Figura 4. Dado que los diagramas de radiación son volúmenes, podemos representarlos en tres dimensiones.

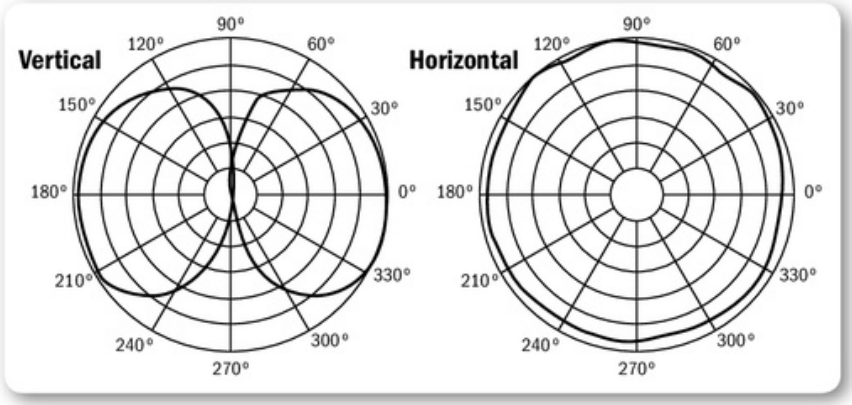


Figura 5. Los diagramas de radiación se realizan en dos planos: para radiación vertical y para la horizontal.

Ancho del haz

Definimos el **ancho del haz** (**beamwidth**) como el intervalo angular en el que la densidad de potencia radiada es igual a la mitad de la potencia máxima (en la dirección principal de radiación).

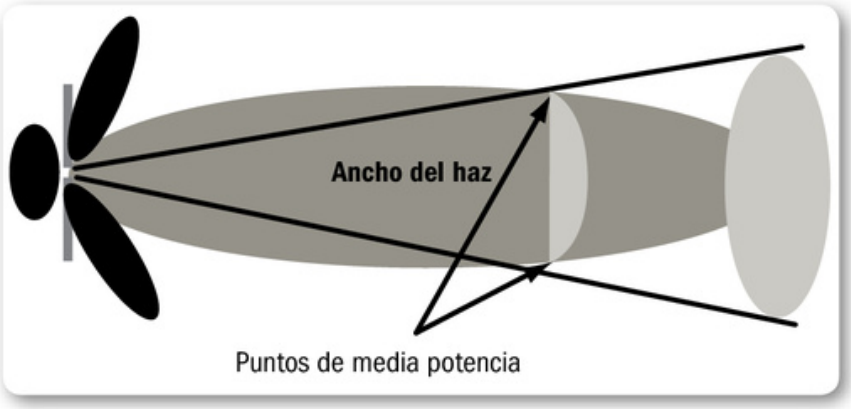


Figura 6. El parámetro ancho del haz está ligado directamente al diagrama de radiación y sus diferentes formas de graficarlo.

Polarización de la antena

La **polarización de una antena** se refiere solo a la **orientación del campo eléctrico radiado** desde ella. En general, la polarización puede ser horizontal o vertical.

Si la antena irradia una onda electromagnética polarizada verticalmente, decimos que tiene polarización vertical.

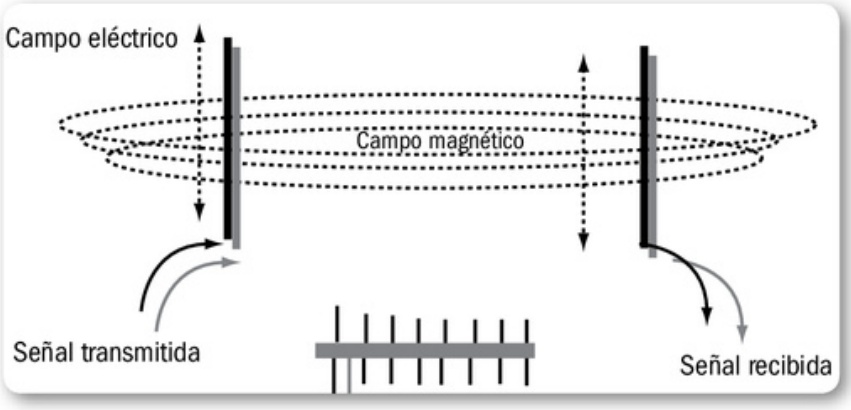


Figura 7. La polarización es vertical si nuestra onda mantiene el campo eléctrico en dirección vertical durante el recorrido.

En cambio, si la onda propagada está polarizada horizontalmente, la antena tendrá polarización horizontal.

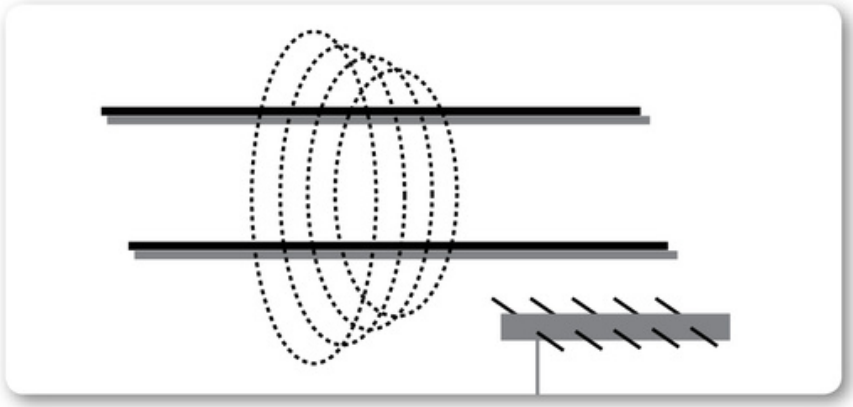


Figura 8. Al modificar la orientación de los elementos de las antenas, obtenemos la polarización horizontal.

Lo importante es saber que podemos emplear cualquier tipo de polarización siempre y cuando tengamos la misma configuración (polarización horizontal o vertical) en ambos extremos. Existen otras polarizaciones que no veremos en detalle en este libro.

Clasificación de las antenas

Tal como dijimos antes, existen diferentes antenas. La forma, el tamaño y el uso dependen de los parámetros vistos en la sección anterior. Así, para conocer algunos tipos de antenas que son habituales, podemos realizar una clasificación de ellas basándonos en algunas especificaciones. Por ejemplo, tendremos distintas clasificaciones según los siguientes parámetros: si es o no directiva, el tamaño, la frecuencia de uso, el patrón de radiación, cómo está construida

DIAGRAMA EN 3D

Al momento de obtener el diagrama de radiación de una antena, existen varias opciones para representarlo. Una es en tres dimensiones. Si no nos interesa el diagrama en tres dimensiones (ya que no podemos hacer mediciones exactas), podremos realizar un corte en el diagrama y pasarlo a dos dimensiones.

físicamente, para qué aplicación se la puede usar, y otras. Realizaremos nuestra clasificación según el patrón de radiación y según la **construcción de la antena**.

Según el patrón de radiación

Analizando el patrón de radiación de las antenas (este dato se puede consultar con el fabricante correspondiente), podemos clasificar algunas de las tantas antenas en:

- **Direccionales**: son antenas que irradian energía en una sola dirección. En general, poseen un ángulo de radiación de menos de 70 grados, de forma que se obtiene mayor alcance al proyectarse hacia adelante. Las podemos utilizar para enlaces de larga distancia punto a punto en ambos extremos, emisor y/o receptor.
- **Sectoriales**: si el diagrama de radiación corresponde a un área o zona específica, la antena se llama sectorial. Como detalle podemos decir que estas antenas poseen mayor ángulo de irradiación que las direccionales; de esta forma, tienen corto alcance porque no se proyectan hacia adelante.



Figura 9. Debemos saber que las antenas sectoriales varían su rango de ganancia entre 10 y 19 dBi.

Poseen mejor ganancia y, además, es posible inclinar las antenas para dar servicio a zonas de interés. Si logramos combinar varias antenas de este tipo, podremos dar cobertura en todo el plano horizontal. Cubriendo todo este plano, estaríamos haciendo lo mismo que una

antena omnidireccional, solo que a un mayor costo y con mejores prestaciones. La ganancia de las antenas sectoriales es más alta que la de las omnidireccionales. Son antenas ideales para usar en enlaces multipunto del lado transmisor, ya que son consideradas de alcance medio. En general, su valor de ganancia más común es de 14 dBi.

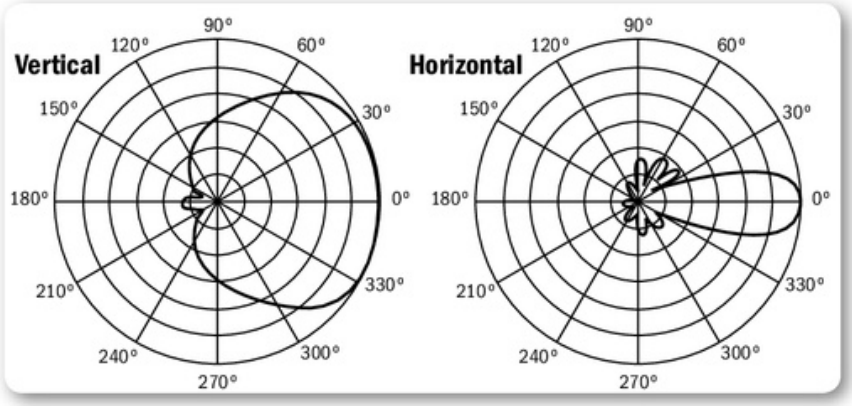


Figura 10. El diagrama de radiación horizontal posee la mayor energía irradiada en la parte frontal de la antena.

- **Omnidireccionales**: estas antenas irradian energía en todas las direcciones. Por eso se dice que su ángulo de radiación es de 360° en el plano horizontal. La ganancia típica de este tipo de antenas es de 8 a 12 dBi. Tienen menor alcance y pueden ser utilizadas para conformar la parte transmisora en un enlace multipunto y combinándolas con antenas altamente directivas.

Según su construcción

Para basarnos en esta diferenciación, veremos las antenas discriminadas según su complejidad para construirlas, desde la más sencilla hasta alguna de las más complejas.

- **Dipolos**: es una antena muy sencilla de construir para implementarla en una gran variedad de frecuencias. Básicamente, está conformada por dos trozos de material conductor. Se puede decir que es una antena omnidireccional que forma la base para construir otros modelos de antenas direccionales. Se puede usar con polarización horizontal o vertical según como se disponga el dipolo.

- **Biquad**: para construir esta antena es necesario un alambre de cobre y una base que haga de reflector de la señal. Así, se obtiene una antena direccional de fácil construcción, que nos brinda una ganancia cercana a los 11 dBi. Es común utilizar como elemento reflector antenas parabólicas en desuso.
- **Yagi-Uda**: es una antena construida en la década del 30 por el ingeniero japonés Yagi. Es uno de los modelos más encontrados cuando prestamos atención a las antenas utilizadas, dada su facilidad de construcción. Consta de un dipolo de media onda con una ganancia baja (de apenas 2.1 dBi), al que se le agrega otro dipolo ligeramente más largo en la parte posterior. Esto hace de reflector de la señal que intenta irradiarse en la parte posterior. Luego se agregan varios dipolos de longitud menor que hacen de directores (donde la energía es enfocada en una dirección, hacia adelante). Si hablamos de ganancia de antena, podemos decir que ronda los 14 dBi para la banda de 2.4 Ghz. La ganancia puede variar al modificar el número de elementos directores que posee el modelo. Muchos asimilan la forma de la antena con la espina de un pescado.



Figura 11. La antena Yagi-Uda junto con su creador, el ingeniero japonés Yagi.

- **Panel**: las antenas tipo panel (también llamadas **patch**) constan de una placa de circuito de cobre o metal impresa en su interior. El diseño de esta placa impresa funciona como el elemento activo de la antena. Se pueden conseguir elevadas ganancias con este tipo de antenas direccionales (cerca de los 20 dBi).



Figura 12. Antena panel con soporte para exteriores. Es fácil de identificar ya que es visualmente llamativa.

- **Parrilla**: también se puede encontrar esta antena con el nombre de malla o grid. Debemos tener en cuenta que la característica principal de este tipo de antenas es que su reflector posterior es similar a una **parrilla** (por esto el nombre). Se trata de antenas que se utilizan en zonas donde las inclemencias del tiempo son un factor para tener en cuenta a la hora de montarlas. Si, por ejemplo, necesitamos montar una antena en una zona de mucho viento, utilizando este modelo evitaremos posibles corrimientos del elemento, lo que provocaría una pérdida del enlace.

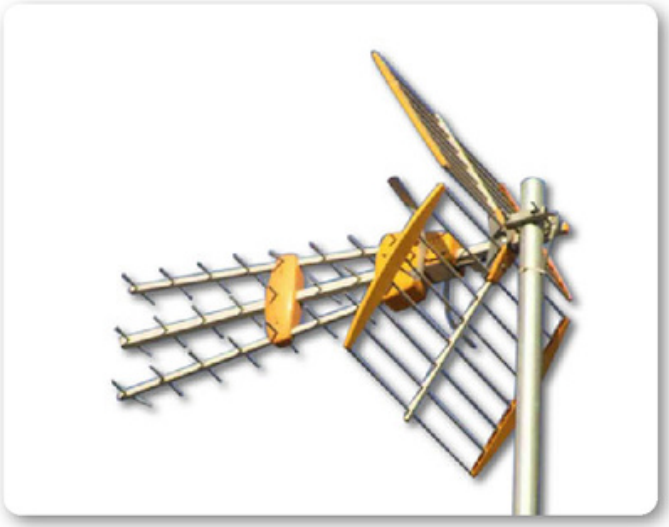


Figura 13. El reflector tipo parrilla identifica a estas antenas. Existen muchos modelos de antenas de esta clase.

- **Parabólicas**: la particularidad de estas antenas direccionales es que su reflector es de material sólido (a diferencia del tipo parrilla que veíamos antes). Utilizar un material sólido trae como ventaja que la ganancia de antena obtenida es de hasta 30 dBi. Estos reflectores reciben la señal en su superficie y la concentran en un punto llamado **foco**. De forma inversa, cuando se genera una señal en el foco, se la hace rebotar en las paredes del reflector y se concentra la energía en una única dirección.
  La frecuencia de operación de la antena solamente depende del elemento activo (el que irradia la onda electromagnética); así, es posible utilizar reflectores parabólicos con antenas (elemento activo) caseros. Por ejemplo, es muy común ver las antenas de televisión satelital recicladas para construir una antena con reflector parabólico. Para enlaces de larga distancia, estas antenas son ideales. Si analizamos el diagrama de radiación de este tipo de antenas, identificamos cierta similitud con el diagrama que corresponde al de una antena Yagi-Uda.
  La única diferencia se encuentra en que la antena con reflector parabólico posee un ángulo de radiación más angosto. Al tener este ángulo más pequeño, podemos encontrar dificultades a la hora de apuntar este tipo de antenas en un enlace a larga distancia. Debemos tener especial cuidado al implementar la antena en zonas de fuertes vientos, ya que se podría desapuntar el enlace



RESUMEN

En el inicio del capítulo aprendimos el concepto básico de antena, para luego especificar las características más importantes de su funcionamiento y aprender a caracterizarlas dependiendo de variados factores, tales como el patrón de radiación o el ancho del haz, entre otras. También accedimos a realizar la clasificación de las antenas según los elementos utilizados en su construcción física y dimos algunos consejos para montarlas en forma correcta.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué es una antena y de qué forma transmite una señal al espacio libre?
2. ¿Es importante que la antena sea eficaz transformando energía? ¿Por qué?
3. ¿Qué se genera cuando por un elemento conductor se hace circular una corriente eléctrica? ¿Cómo se llama esta ley?
4. ¿Cuál es el parámetro fundamental de una antena para lograr la máxima transferencia de energía?
5. ¿Cómo funciona una antena?
6. ¿Cuáles son las antenas sectoriales?
7. ¿Qué cable coaxial se recomienda usar para conexiones inalámbricas caseras de 2.4 GHz?
8. ¿Qué diferencia física existe entre un conector BNC y un TNC?
9. ¿Qué es un pigtail y para qué se utiliza?
10. ¿Qué son las radiaciones?

ACTIVIDADES PRÁCTICAS

1. Identifique una antena en un espacio libre.
2. Enumere las características de una antena isotrópica.
3. Diferencie una antena sectorial.
4. Caracterice un conector BNC y un TNC.
5. Identifique un dispositivo con radiación no ionizante.

Servicios al lector

En esta sección nos encargaremos de presentar un útil índice temático para que podamos encontrar en forma sencilla los términos que necesitamos.

▾ Índice temático.....186

Índice temático

A

ACL 107
Actualizaciones 124
Alineación de antenas 160
ALOHA 150
Amenazas 114
Amenazas de seguridad 113
Ancho de haz 176
Ángulo determinado 155
Antena 27
Antena isotrópica 174
Antenas 172
Antenas de hilo 173
Antenas direccionales 155
Antenas inteligentes 43
Antenas isotrópicas 173
Antenas onmidireccionales 174
Antenas patch 174
Antenas Yagi direccionales 174
AP 24
Apiladas 97
Asignación de IP 69
Asociación 105
Ataque de intercepción 113
Ataque de intromisión 113
Ataque de modificacion 113
Ataque de suplantación 113
Ataques de repetición 110
Atributos de seguridad 97
Autentificador 101
Ayuda en línea 126

B

Bandas sin licencia 160
Beamwidth 176
Bluetooth 164
BSSID 66

C

Capa de aplicación 16
Capa de enlace 52
Capa de Internet 18
Capa de presentación 16
Capa de red 17
Capa de sesión 16
Capa de transporte 17
Capa física 49
Capas 15
Cifrado pesado 107
Clasificación de las antenas 178
Clientes inalámbricos 41
Cluster 111
Codificación 36
Código de redundancia cíclica 109
Confidencialidad 98
Configuración de AP 87
Configuración del cliente 90
Configurar la red 80
Configurar red inalámbrica 79
Confirmación 134
Controlador 63
Corroborar resultados 134

D

Dbi 174
Delimitar el problema 125
Diagrama de radiación 174
Dípolos 180
Dirección IP 56
Dirección IP dinámica 68
Dirección IP fija 68
Documentar el problema 135
Documentar resultados 135
Drivers 62
Dúplex 150

E

EAPOL 103
Encerrar la causa 126
Encriptación 54
Enfoque metodológico 118
Enlace remoto 149
Enlace remoto fijo 149
Enlace remoto móvil 149
Enlace satelital 152
Escalabilidad 22
Escenarios prácticos 14
Espectro esparcido 148
ESSID 66
Estabilizador 122
Etiquetador de red 142

F

Fibra óptica 146
Filtrado MAC 54
Firewall 115
Firma electrónica 95
Firmware 124
Foco 183
Frecuencia de operación 183
Full dúplex 150
Funcionamiento de WPA 100

G

Ganancia de antena 173
Google Earth 162
GMS 163
GPRS 163
GPS 162

H

Hardware 61
Hardware inalámbrico 40
Herramientas 138
HiperLan 29
Homerf 49
HOP3 89
HTTP 108

I

IDS 115
IEEE 32
Impedancia 172
Inserción 94
Installshield 62
Intermitente 127
Intervalo de Beacon 53
Intrusos 94
IP duplicadas 134
IP privada 68
IP pública 68
Ipconfig 69

L

LAN 20
Leds 45
Llave compartida 106
Luz infrarroja 147
Luz ultravioleta 147

M

MAC 107
Máscara de red 56
Máscara de subred 78
Menos velocidad 22
Método 118
Microondas 23
Modos de operación 28
Monitorear 111

N

Nmap 138
No repudio 112
Nodos 71
Ntop 138
Número de canal 49

O

Ondas de radio 147
Ondas electromagnéticas 14
Opciones de TCPIP 67
Orientación 177

P

Packet radio 150
Panel 182
Parabólicas 183
Parrilla 182
Patrón de radiación 175
Picoredes 168
Ping 129
Ping graficado 142
Ping plotter 141
Placa de red 24
Plan 134
Planear la solución 127
Polarización de la antena 177
Portabilidad 21
Portal cautivo 108
Potencia de transmisión 51
Propiedades del dispositivo 62
Puerta de enlace 91
Puertos Ethernet 121
Punto a multipunto 154
Punto a punto 154
Puntos de acceso 25

R

Radiación 46
Radiación ideal 173
Radioenlace 146
Radioenlace infrarrojo 152
Radioenlace UHF 152
Radiopaquete 148
RADIUS 99
Rayos gamma 147
Rayos X 147
Red 14
Red congestionada 140
Red fuera de servicio 142
Red inalámbrica 19
Repetidores 30
Repetidores activos 153

R

Repetidores pasivos 153
Retardo en la red 143
Router inalámbrico 26

S

Satelital 148
Seguridad inalámbrica 95
Selección de la red 66
Semidúplex 150
Servicios segmentados 118
Servidor de autenticación 101
Servidor DNS 79
Sharpmark 142
Simplex 151
Sistema de distribución 87
Slot PCI 64
Software de gestión 156
Solicitante 101
SSID 53

T

Tasa de transmisión 35
TCP/IP 17
Tcpdump 140
Telecomunicación 42
Telnet 141
Tensión eléctrica 120
Tipos de enlaces 152
Topografía 151
Tracert 138
Transformadores 123

V

Ventajas satelitales 159
VisualRoute 139
VisualWare 139

W

WDS 55
WEP 50
Wireshark 138
WLAN 20

usershop.redusers.com Llegamos a todo el mundo OCA DHL



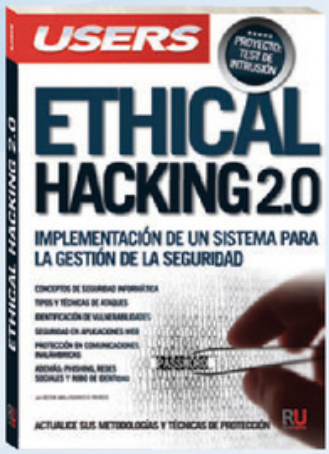
Una obra ideal para aprender todas las ventajas y servicios integrados que ofrece Office 365 para optimizar nuestro trabajo.

→ 320 páginas / ISBN 978-987-1857-65-4



Esta obra presenta las mejores aplicaciones y servicios en línea para aprovechar al máximo su PC y dispositivos multimedia.

→ 320 páginas / ISBN 978-987-1857-61-6



Esta obra va dirigida a todos aquellos que quieran conocer o profundizar sobre las técnicas y herramientas de los hackers.

→ 320 páginas / ISBN 978-987-1857-63-0



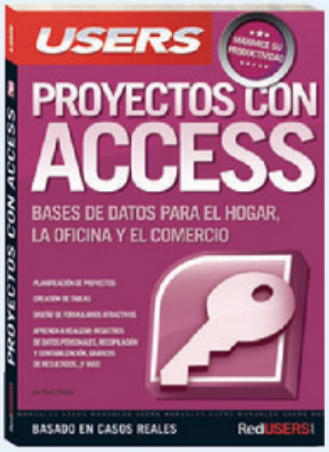
Este libro se dirige a fotógrafos amateurs, aficionados y a todos aquellos que quieran perfeccionarse en la fotografía digital.

→ 320 páginas / ISBN 978-987-1857-48-7



En este libro encontraremos una completa guía aplicada a la instalación y configuración de redes pequeñas y medianas.

→ 320 páginas / ISBN 978-987-1857-46-3



Esta obra está dirigida a todos aquellos que buscan ampliar sus conocimientos sobre Access mediante la práctica cotidiana.

→ 320 páginas / ISBN 978-987-1857-45-6



Este libro nos introduce en el apasionante mundo del diseño y desarrollo web con Flash y AS3.

→ 320 páginas / ISBN 978-987-1857-40-1



Esta obra presenta un completo recorrido a través de los principales conceptos sobre las TICs y su aplicación en la actividad diaria.

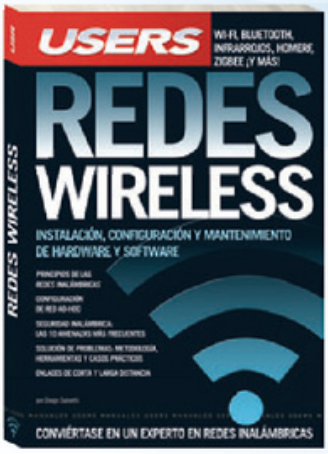
→ 320 páginas / ISBN 978-987-1857-41-8



Este libro está dirigido tanto a los que se inician con el overclocking, como a aquellos que buscan ampliar sus experiencias.

→ 320 páginas / ISBN 978-987-1857-30-2

+ 54 (011) 4110-8700 usershop@redusers.com



Este manual único nos introduce en el fascinante y complejo mundo de las redes inalámbricas.

→ 320 páginas / ISBN 978-987-1773-98-5



Esta increíble obra está dirigida a los entusiastas de la tecnología que quieran aprender los mejores trucos de los expertos.

→ 320 páginas / ISBN 978-987-1857-01-2



Esta obra se encuentra destinada a todos los desarrolladores que necesitan avanzar en el uso de la plataforma Adobe Flash.

→ 320 páginas / ISBN 978-987-1857-00-5



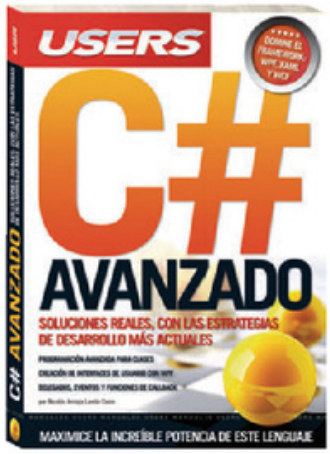
Un libro clave para adquirir las herramientas y técnicas necesarias para crear un sitio sin conocimientos previos.

→ 320 páginas / ISBN 978-987-1773-99-2



Una obra para aprender a programar en Java y así insertarse en el creciente mercado laboral del desarrollo de software.

→ 352 páginas / ISBN 978-987-1773-97-8



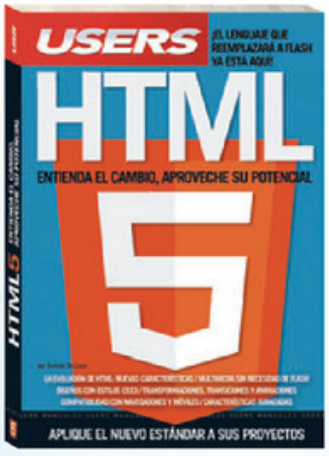
Este libro presenta un nuevo recorrido por el máximo nivel de C# con el objetivo de lograr un desarrollo más eficiente.

→ 320 páginas / ISBN 978-987-1773-96-1



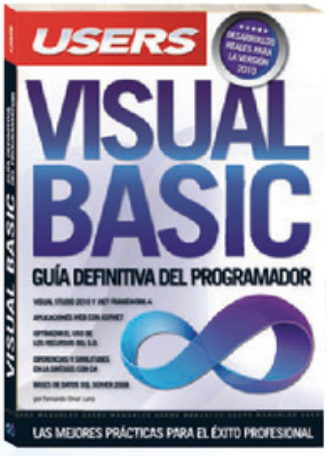
Esta obra presenta todos los fundamentos y las prácticas necesarios para montar redes en pequeñas y medianas empresas.

→ 320 páginas / ISBN 978-987-1773-80-0



Una obra única para aprender sobre el nuevo estándar y cómo aplicarlo a nuestros proyectos.

→ 320 páginas / ISBN 978-987-1773-79-4



Un libro imprescindible para aprender cómo programar en VB.NET y así lograr el éxito profesional.

→ 352 páginas / ISBN 978-987-1773-57-2

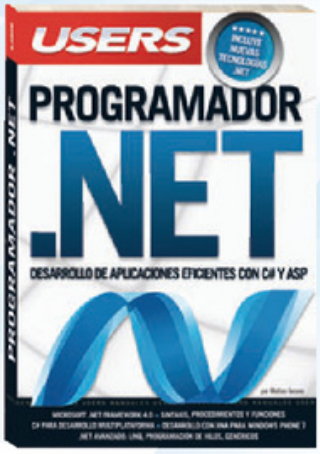
Descargue un capítulo gratuito
Entérese de novedades y lanzamientos

Compre los libros desde su casa
y con descuentos



Una obra para aprender los fundamentos de los microcontroladores y llevar adelante proyectos propios.

→ 320 páginas / ISBN 978-987-1773-56-5



Un manual único para aprender a desarrollar aplicaciones de escritorio y para la Web con la última versión de C#.

→ 352 páginas / ISBN 978-987-1773-26-8



Un manual imperdible para aprender a utilizar Photoshop desde la teoría hasta las técnicas avanzadas.

→ 320 páginas / ISBN 978-987-1773-25-1



Una obra imprescindible para quienes quieran conseguir un nuevo nivel de profesionalismo en sus blogs.

→ 352 páginas / ISBN 978-987-1773-18-3



Un libro único para ingresar en el apasionante mundo de la administración y virtualización de servidores.

→ 352 páginas / ISBN 978-987-1773-19-0



Esta obra permite sacar el máximo provecho de Windows 7, las redes sociales y los dispositivos ultraportátiles del momento.

→ 352 páginas / ISBN 978-987-1773-17-6



Este libro presenta la fusión de las dos herramientas más populares en el desarrollo de aplicaciones web: PHP y MySQL.

→ 432 páginas / ISBN 978-987-1773-16-9



Este manual va dirigido tanto a principiantes como a usuarios que quieran conocer las nuevas herramientas de Excel 2010.

→ 352 páginas / ISBN 978-987-1773-15-2



Esta guía enseña cómo realizar un correcto diagnóstico y determinar la solución para los problemas de hardware de la PC.

→ 320 páginas / ISBN 978-987-1773-14-5

+ 54 (011) 4110-8700 usershop@redusers.com

usershop.redusers.com Llegamos a todo el mundo OCA DHL

CURSOS INTENSIVOS CON SALIDA LABORAL

Los temas más importantes del universo de la tecnología, desarrollados con la mayor profundidad y con un despliegue visual de alto impacto: explicaciones teóricas, procedimientos paso a paso, videotutoriales, infografías y muchos recursos más.



- 25 Fascículos
- 600 Páginas
- 2 DVDs / 2 Libros

Curso para dominar las principales herramientas del paquete Adobe CS3 y conocer los mejores secretos para diseñar de manera profesional. Ideal para quienes se desempeñan en diseño, publicidad, productos gráficos o sitios web.



Obra teórica y práctica que brinda las habilidades necesarias para convertirse en un profesional en composición, animación y VFX (efectos especiales).

- 25 Fascículos
- 600 Páginas
- 2 CDs / 1 DVD / 1 Libro



- 25 Fascículos
- 600 Páginas
- 4 CDs

Obra ideal para ingresar en el apasionante universo del diseño web y utilizar Internet para una profesión rentable. Elaborada por los máximos referentes en el área, con infografías y explicaciones muy didácticas.

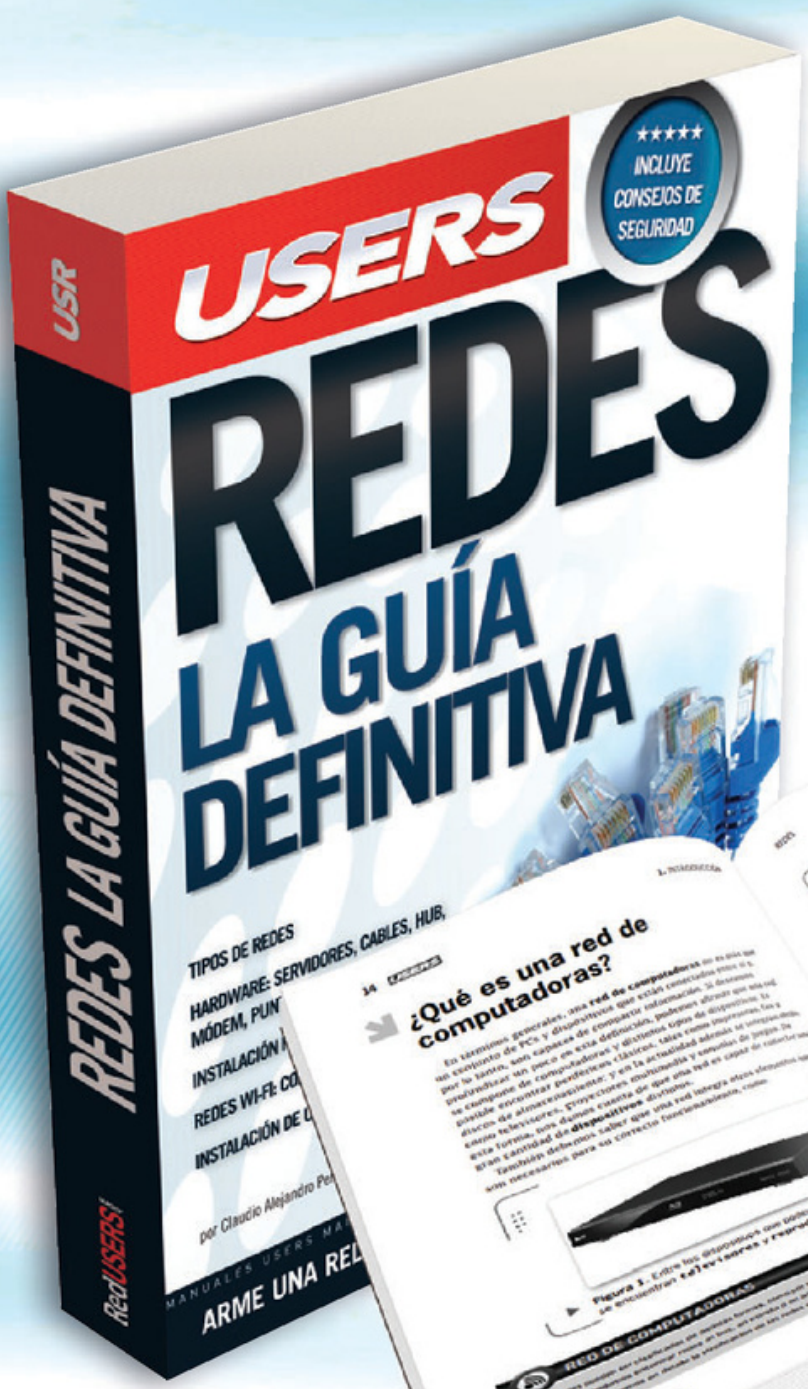


Brinda las habilidades necesarias para planificar, instalar y administrar redes de computadoras de forma profesional. Basada principalmente en tecnologías Cisco, busca cubrir la creciente necesidad de profesionales.

- 25 Fascículos
- 600 Páginas
- 3 CDs / 1 Libros

+ 54 (011) 4110-8700 usershop@redusers.com

CONÉCTESE CON LOS MEJORES LIBROS DE COMPUTACIÓN





En este libro encontraremos una completa guía aplicada a la instalación y configuración de redes pequeñas y medianas. Es ideal, tanto para entusiastas que busquen dar sus primeros pasos, como técnicos informáticos que quieran mejorar sus conocimientos.

» HOME / REDES
» 320 PÁGINAS
» ISBN 978-987-1857-46-3

LLEGAMOS A TODO EL MUNDO VÍA OCA* Y DHL**

MÁS INFORMACIÓN / CONTÁCTENOS

usershop.redusers.com +54 (011) 4110-8700 usershop@redusers.com

*SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // **VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

USERS

REDES WIFI EN ENTORNOS WINDOWS

Esta obra está dirigida a todos aquellos entusiastas que busquen dar sus primeros pasos en redes inalámbricas, como así también a aquellos ya experimentados que quieran mejorar sus conocimientos. A lo largo de sus páginas, conoceremos los pasos necesarios para la instalación y puesta en marcha de una red inalámbrica, a través de ejemplos prácticos de configuración. Además, trabajaremos sobre las topologías de red más frecuentes y definiremos el hardware requerido. También nos dedicaremos a las antenas, analizando sus características y modelos posibles; sin dejar de lado los cables y conectores, que ocupan un lugar central a la hora de vincular nuestros equipos.
En conclusión, aquí encontraremos un material de consulta que explica con un lenguaje claro y sencillo aquellos conceptos que muchas veces resultan difíciles de comprender.

> **Hoy en día nos evitamos realizar tendidos de cables en edificios y casas particulares, lo que implica un ahorro de tiempo y, principalmente, de dinero**

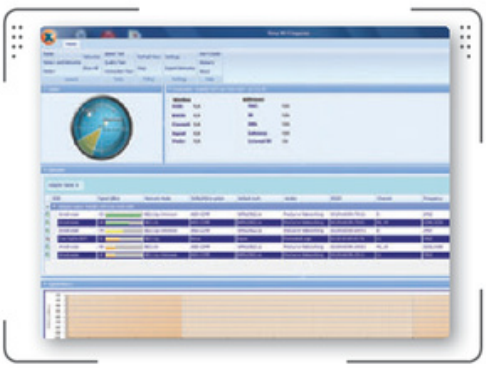
EN ESTE LIBRO APRENDERÁ:

- **Introducción:** conceptos sobre redes, y modelos OSI y TCP/IP. Las redes inalámbricas y sus componentes. Los modos de operación y el estándar IEE.
- **Hardware:** cuál es el hardware indicado para redes inalámbricas. Qué aspectos se deben tener en cuenta para configurar los puntos de acceso y el modelo OSI.
- **Windows:** instalación de clientes en Windows. Cómo configurar el hardware y una red inalámbrica AD HOC.
- **Seguridad en la red:** atributos de seguridad y confidencialidad en WLAN. Autenticación en redes inalámbricas. Las 10 amenazas más comunes.
- **Problemas:** enfoque metodológico. Cuáles son los pasos fundamentales para verificar y qué herramientas considerar para resolver los problemas.
- **Conexión:** enlaces de corta y larga distancia. Clasificación de antenas. Cables y conectores para establecer una red.



» Parte del contenido de este libro fue publicado previamente en la obra "Redes Wireless"





» **NIVEL DE USUARIO**
Principiante / Intermedio

» **CATEGORÍA**
Redes / Home

ISBN 978-987-1857-64-7

RU RedUSERS

REDUSERS.com
En nuestro sitio podrá encontrar noticias relacionadas y también participar de la comunidad de tecnología más importante de América Latina.

PROFESOR EN LÍNEA
Ante cualquier consulta técnica relacionada con el libro, puede contactarse con nuestros expertos: profesor@redusers.com.