USERS

WI-FI, BLUETOOTH, INFRARROJOS, HOMERF, ZIGBEE ¡Y MÁS!

REDES WIRELESS

INSTALACIÓN, CONFIGURACIÓN Y MANTENIMIENTO DE HARDWARE Y SOFTWARE

- PRINCIPIOS DE LAS REDES INALÁMBRICAS
- CONFIGURACIÓN DE RED AD-HOC
- SEGURIDAD INALÁMBRICA: LAS 10 AMENAZAS MÁS FRECUENTES
- SOLUCIÓN DE PROBLEMAS: METODOLOGÍA, HERRAMIENTAS Y CASOS PRÁCTICOS
- ENLACES DE CORTA Y LARGA DISTANCIA

por Diego Salvetti

MANUALES USERS MANUALES USERS MANUALES USERS MANUALES USERS MA

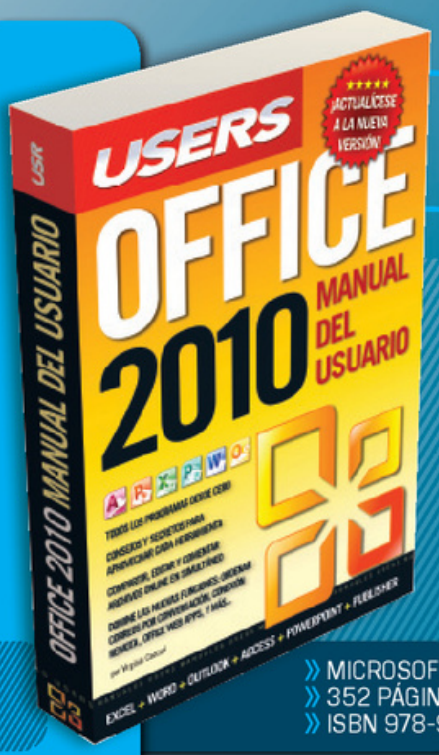
CONVIÉRTASE EN UN EXPERTO EN REDES INALÁMBRICAS

CONÉCTESE
CON LOS MEJORES LIBROS DE COMPUTACIÓN

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

usershop.redusers.com
usershop@redusers.com

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



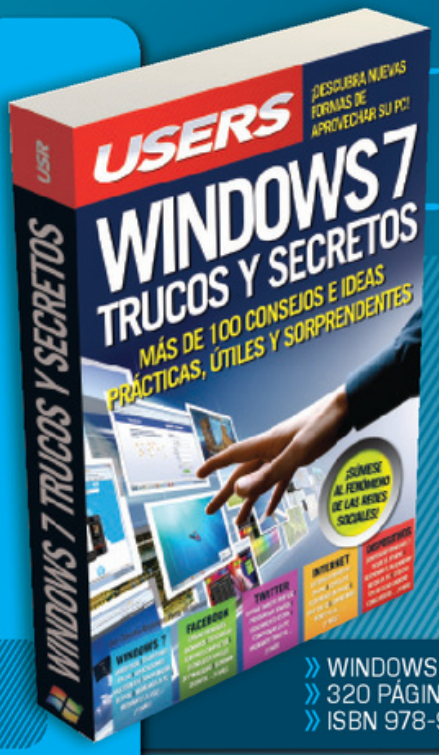
DOMINE TODAS LAS HERRAMIENTAS DE OFFICE Y SUS NUEVAS FUNCIONES

» MICROSOFT / OFFICE
» 352 PÁGINAS
» ISBN 978-987-26013-6-2



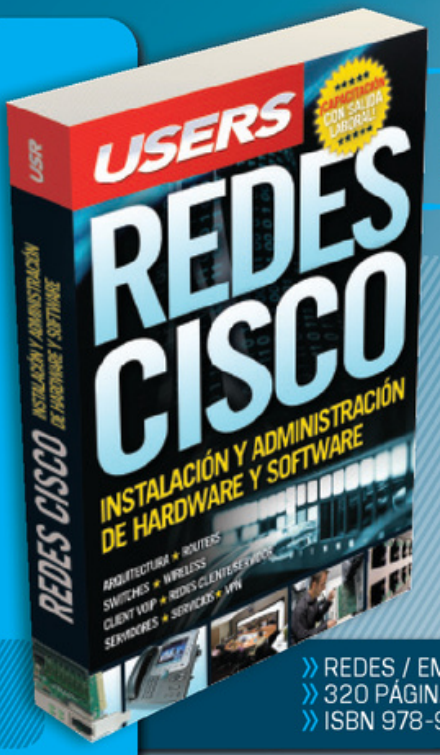
PROTEJA SUSUS DATOS Y PRIVACIDAD CONTRA TODO TIPO DE AMENAZAS

» SEGURIDAD / HOME
» 336 PÁGINAS
» ISBN 978-987-663-004-7



CONOZCA A FONDO EL ÚLTIMO SISTEMA OPERATIVO DE MICROSOFT

» WINDOWS / MICROSOFT
» 320 PÁGINAS
» ISBN 978-987-663-015-3



PLANIFICACIÓN, INSTALACIÓN Y ADMINISTRACIÓN DE REDES COMPLEJAS

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

REDES WIRELESS

INSTALACIÓN, CONFIGURACIÓN Y MANTENIMIENTO DE HARDWARE Y SOFTWARE

por Diego Salvetti

RedUSERS



TÍTULO: Redes Wireless

AUTOR: Diego Salvetti

COLECCIÓN: Manuales USERS

FORMATO: 17 x 24 cm

PÁGINAS: 320

Copyright © MMXI. 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 XII, MMXI.

ISBN 978-987-1773-98-5

Salvetti, Diego

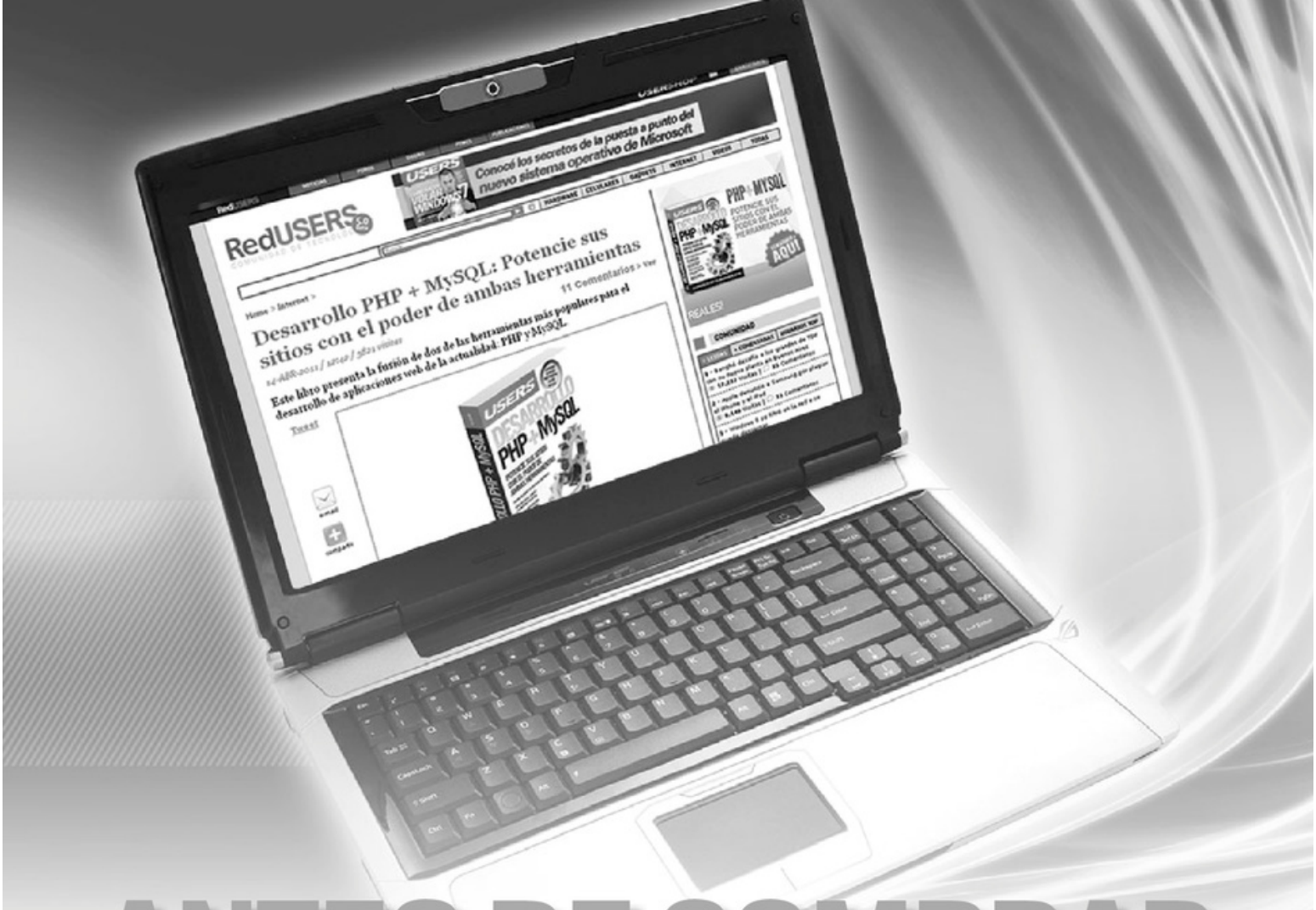
Redes Wireless. - 1a ed. - Buenos Aires : Fox Andina; Dalaga, 2011.

v. 220, 320 p. ; 24x17 cm. - (Manual users)

ISBN 978-987-1773-98-5

1. Informática. I. Título

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

Diego Iván Salvetti



Diego Iván Salvetti es ingeniero en Telecomunicaciones y técnico en Electrónica, interesado en las tecnologías inalámbricas. En su formación como técnico en Electrónica en la ciudad de Rosario, desarrolló varios proyectos vinculados a las comunicaciones inalámbricas y la domótica. Luego, la carrera universitaria le dio un perfil enfocado a las redes de datos y la informática, obteniendo de esta forma conocimientos en sistemas operativos Windows y Linux y fuertes nociones en lenguajes de programación. Su primera experiencia laboral lo vinculó a la VoIP (Voz por IP). Durante varios años, se desempeñó como ingeniero de soporte para una firma local con clientes en Argentina y Brasil.En la actualidad, desarrolla tareas como ingeniero de performance para una empresa extranjera en la ciudad de Córdoba, Argentina.

Email: diegosalvetti@hotmail.com

Dedicatorias

Este libro está dedicado a mis amigos de Cañada de Gómez, Córdoba, Rosario y especialmente a Milton, que ya no está con nosotros y se lo extraña.

Agradecimientos

A mi familia (Carlos, Cristina, Dudo, Ariel y Natalia), que está presente en todos mis proyectos. A mi tía Hilda, que siempre piensa en mí y en la familia.

A Romi, por el tiempo compartido al escribir este libro y por el amor que me da, así como por su incondicional apoyo al momento de compartir proyectos e ideas. También quiero agradecer a todo el grupo Tele2001, que permanece unido aunque ya no estemos en la universidad.

Prólogo

A más de cinco años de haber completado la carrera universitaria, no dejo de pensar en la frase que un profesor, el Ingeniero Morsicato, solía decirnos: "En un mundo, donde la única certeza es la incertidumbre, la única fuente segura de ventaja competitiva es el conocimiento". Esta frase es de Ikujiro Nonaka. En aquel momento ninguno de los presentes teníamos una idea real de qué significaba esta frase tan importante.

Al tener esto dando vueltas en mi cabeza, siempre intenté aprender cosas nuevas y profundizar las que ya conocía. En todo ámbito, no solo en las nuevas tecnologías o la informática, esta frase me provocaba algo diferente, que ocurría de manera inconsciente y me permitía avanzar.

Poco a poco, me fui dando cuenta que el conocimiento es un gran capital intangible, que en un mundo como el nuestro marca la diferencia para cualquier empresa. La importancia de este libro reside en el hecho de comunicar ese conocimiento a otra persona, proporcionarle herramientas útiles al momento de enfrentar diferentes desafíos y que así pueda tener esa ventaja competitiva que tanto desean las empresas.

El contenido tratado me obligó, desde un principio, a tener en cuenta los temas más relevantes para incluir información útil relacionada a las redes inalámbricas, haciendo énfasis en los usuarios sin mucha experiencia. De esta forma el conocimiento se acercaría a su destino.

Los temas seleccionados poseen un valor agregado, son el resultado de varios años de experiencia trabajando en redes hogareñas con problemas. Esto último me permitió estar en contacto directo con los usuarios y tomar conciencia de sus necesidades y dificultades, a la hora de adquirir nuevos conocimientos.

Es mi deseo que este texto sirva para todos aquellos que pretendan iniciarse en las redes inalámbricas. ¡Éxito en sus primeros pasos y que siempre exista en ustedes ese hambre de conocer nuevos caminos!

Ing. Diego Iván Salvetti

El libro de un vistazo

Esta obra está destinada a todos aquellos que quieran iniciarse, o ya estén iniciados, en las redes inalámbricas con el sistema operativo Windows Seven. Estudiaremos los conceptos básicos de las redes y también aprenderemos los conceptos y configuraciones más avanzados.

*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. Luego, entraremos en el mundo inalámbrico identificando los componentes de estas redes. Finalizaremos hablando de los estándares IEEE 802.11, describiremos sus variantes y características.

*02 HARDWARE PARA REDES INALÁMBRICAS

En este capítulo, presentamos la configuración e instalación de los equipos usados en una red inalámbrica, discriminando entre clientes y puntos de acceso a la red. Basándonos en el modelo OSI, desarrollado en el capítulo 1, aprenderemos cómo instalar y configurar el hardware necesario.

*03 CONFIGURACIÓN EN WINDOWS

Con la ayuda de este capítulo, vamos a identificar y configurar el hardware de la red para el sistema operativo Windows Seven. Veremos diferentes tipos de configuraciones para nuestra red y la forma de conectarnos a esta. Es un capítulo práctico, así que nos pondremos manos a la obra.

*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 forma crear y mantener redes inalámbricas. En el final del capítulo conoceremos las amenazas de seguridad más comunes.

*05 RESOLVER PROBLEMAS

El objetivo de este quinto capítulo es enseñar un método ordenado para identificar y corregir problemas en las redes inalámbricas. Tomaremos como base el modelo OSI para crear una "receta" y de esta forma simplificar y ordenar el proceso a la hora de buscar fallas en nuestra red.

*06 ENLACES DE LARGA DISTANCIA

Los enlaces de larga distancia se pueden considerar como una configuración avanzada

en redes inalámbricas hogareñas. Detallaremos las claves necesarios para utilizar la tecnología inalámbrica en este tipo de redes donde unimos puntos distantes. También realizaremos una parte práctica con un software que facilitará los cálculos.

*07 ENLACES DE CORTA DISTANCIA

Cuando utilizamos nuestro teléfono celular con Bluetooth para transferir archivos a la PC estamos formando redes de corta distancia. En este capítulo analizaremos estas redes y nos enfocaremos en la tecnología Bluetooth, tan común en nuestros días, para ver su funcionamiento y aplicaciones.

*08 ANTENAS Y CONECTORES

Las antenas se consideran componentes fundamentales de una red inalámbrica. Explicaremos su funcionamiento y las características básicas para comprender cómo se transmite la información. Finalizaremos el capítulo analizando si las ondas electromagnéticas pueden o no ser perjudiciales para la salud.

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 identificarlos 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



Desarrollos temáticos en profundidad

Libros.

Coleccionables.

Cursos intensivos con multimedia





Capacitación dinámica

Revistas.

Sitios Web.

Noticias al día, downloads, comunidad





Información actualizada al instante

Newsletters.

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

redusers.com

Contenido

Sobre el autor 4
Prólogo 5
El libro de un vistazo 10
Información complementaria 11
Introducción 12

*01 Introducción a las redes inalámbricas

¿A qué llamamos red? 14
El modelo OSI 14
Funciones de cada capa 15
El modelo TCP/IP 17
Tipos de redes 19
Topologías básicas de red 21
Topologías de redes inalámbricas 23
¿Cuáles son las redes inalámbricas? 25
¿Cómo funcionan las redes inalámbricas? 26
Ventajas de utilizar redes inalámbricas 28
Desventajas de utilizar redes inalámbricas 29
Componentes de redes inalámbricas 31
Puntos de acceso 33
Modos de operación 38
Modo ad hoc 38
Resumen 59
Actividades 60

*02 Hardware para redes inalámbricas

Introducción al hardware inalámbrico 62
Configuración de puntos de acceso 65
Pautas generales a tener en cuenta 65
Instalar el hardware y actualizarlo 67
Configurar con el modelo OSI 84
Capa física 85
Capa de enlace 90
Capa de red 97
Capa de aplicación 98
Resumen 99
Actividades 100

*03 Configuración en Windows

Instalar clientes en Windows 102
¿Qué hardware utilizar? 103
Instalar el hardware es fácil 103
Configurar el hardware en Windows 111
Configurar la red inalámbrica 126
Configurar la red para compartir 134
Configuración de red inalámbrica, modo infraestructura 139
Configuración de una red inalámbrica AD HOC 145
Configuración de Internet en una red AD HOC 147
Resumen 149
Actividades 150

*04 Segurida en la red

¿Seguridad inalámbrica? 152
¿A que llamamos seguridad de la información? 154
Confidencialidad 157
Autenticación 158
Integridad 158
Disponibilidad 159
No repudio 160
Seguridad de la información + WLAN 160
Atributos de seguridad 161
Confidencialidad en WLAN 162
Autenticación en redes inalámbricas 168

Integridad de datos en WLAN 173
Disponibilidad en WLAN 174
No repudio en redes inalámbricas 175
Las 10 amenazas más comunes 175
Resumen 177
Actividades 178

*05 Resolver problemas

Enfoque metodológico 180
Pasos fundamentales a verificar 182
Tensión eléctrica estable 182
Actualizaciones 186
Nuestro método 186
¿Cuáles herramientas usar para resolver problemas? 201
Escenarios prácticos 203
Resumen 205
Actividades 206

*06 Enlaces de larga distancia

Introducción 208
¿Qué es un radioenlace? 211
Tipos de enlaces 215
¿Qué necesito para llegar más lejos? 223
Consideraciones previas 226
Alineación de antenas 232
Con extremos visibles 232
Con extremos no visibles 233
Cálculo de enlace 234
Presupuesto de potencia 234
Cálculo con Radio Mobile 236
Resumen 243
Actividades 244

*07 Enlaces de corta distancia

Red inalámbrica de área personal 246
Los grupos de trabajo de la IEEE 247
¿Dónde se aplica la tecnología WPAN? 248
Tipos de WPAN 249
Principio básico de funcionamiento 250
Bluetooth: ¿qué es y cómo funciona? 253
Topología de red 256
Seguridad 257
Vulnerabilidades 259
Resumen 261
Actividades 262

*08 Antenas y conectores

¿Qué es una antena? 264
¿Cómo funciona una antena? 267
Características generales de una antena 271
Características específicas de una antena 272
Clasificación de las antenas 278
Según el patrón de radiación 279
Según su construcción 281
Cables y conectores usados 286
Radiación y salud 297
¿Es peligrosa la radiación electromagnética? 302
Resumen 303
Actividades 304

* Servicios al lector

Índice temático 306
Sitios web relacionados 309
Programas relacionados 313

Introducción



Con la explosión del servicio de Internet y el uso intensivo de la banda ancha, el desarrollo de las telecomunicaciones dio un rotundo cambio de dirección en los últimos años. Muchos sistemas basados en cable (xDSL, fibra óptica o cable coaxial) que llegan hasta el domicilio del usuario para ofrecer conectividad a la red de redes tienen un costo muy alto de instalación. Además, dejar el servicio configurado y listo para usarse implica un tiempo considerable. Sumado a esto, si incluimos las zonas rurales que no quieren quedarse fuera de este nuevo mundo digital, vemos que existe una alta inversión al momento de ofrecer el servicio para toda la población o parte de ella.

Teniendo en mente esta situación y muchas otras limitaciones, tanto topográficas como tecnológicas, se han buscado alternativas en las que la transferencia de información no dependa de un medio físico como es el cable. Como consecuencia, al no utilizar cables, el tiempo necesario para desplegar esta tecnología se reduce considerablemente, entre otros ítems.

Con esta problemática planteada, nacieron y se desarrollaron los estándares inalámbricos IEEE 802.11 (más comúnmente conocidos como WiFi), que forman una alternativa a los medios convencionales con los que se accedía al servicio. Se introdujeron, de esta forma, nuevos y mejores servicios de telecomunicaciones apuntando siempre a satisfacer las necesidades del usuario final.

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 principalmente de dinero.

El objetivo de esta obra es presentar la tecnología inalámbrica a los lectores que no tengan conocimiento en este tema y aportar 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 para todo interesado en redes.

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 al mundo de lo inalámbrico.

Definir el hardware que se utiliza en este tipo de redes es muy importante, por lo tanto, desarrollamos un capítulo entero sobre este tema, en el que brindamos diferentes ejemplos prácticos de configuración del hardware utilizado.

La seguridad para nuestra red inalámbrica es un área a la que le damos central relevancia, ya que nuestros datos quedan expuestos de forma sencilla a cualquier persona que pueda estar escuchando nuestra información.

Por último, nos dedicamos a las antenas para redes inalámbricas, describimos sus características típicas y detallamos los diferentes modelos que existen. No olvidamos los cables y conectores, que también son determinantes a la hora de vincular nuestros equipos con una antena para armar un enlace de distancia considerable, según veremos en ejemplos.

Esperamos que el presente libro sea de utilidad tanto para lectores inexpertos como para aquellos que con algo más de conocimiento poseen mayor experiencia, lo que les permitirá montar y mantener redes inalámbricas hogareñas.

*01 -

Introducción a las redes inalámbricas

Nos introduciremos en la teoría básica de las redes. Partiremos del concepto de 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 la evolución de estas.

- **¿A qué llamamos red? 14**
- **El modelo OSI 14**
  - Funciones de cada capa 15
- **El modelo TCP/IP 17**
  - Tipos de redes 19
  - Topologías básicas de red 21
  - Topologías de redes inalámbricas 23
- **¿Cuáles son las redes inalámbricas? 25**
  - ¿Cómo funcionan las redes inalámbricas? 26
  - Ventajas de utilizar redes inalámbricas 28
  - Desventajas de utilizar redes inalámbricas 29
- **Componentes de redes inalámbricas 31**
  - Puntos de acceso 33
- **Modos de operación 38**
  - Modo ad hoc 38
- **Resumen 59**
- **Actividades 60**

¿A qué llamamos 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 ello hacía imposible que la comunicación fuera exitosa. La ISO creó un idioma en común para toda red de computadoras, de esta forma, nos aseguramos, sin problema, la compatibilidad en estas.



PRINCIPIO DEL MODELO OSI

En **1980**, las redes estaban en 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. Como analogía, podríamos decir que se hablaban diferentes idiomas hasta que con el modelo OSI se unificaron en un idioma universal.

El modelo OSI consta de **7** capas numeradas y cada una de ellas muestra una función de red específica. Con esta **división en capas** se logra que los usuarios puedan ver las funciones de red de cada capa y así comprendan cómo son transportados los datos.

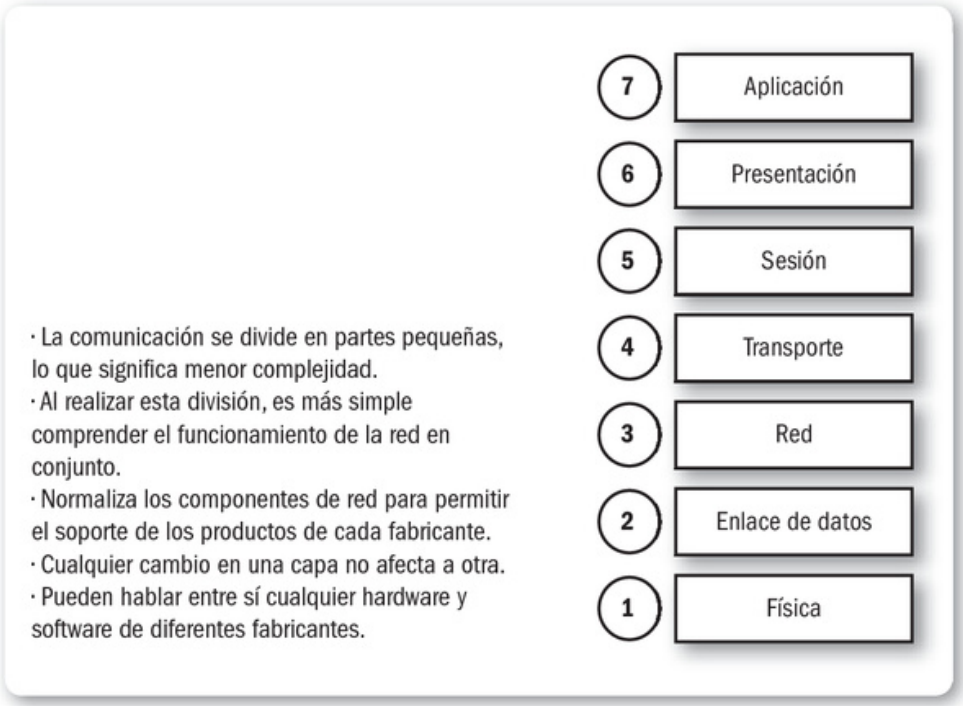


Figura 1. La división en capas de las funciones en nuestra red planteada por el modelo OSI nos permite tener algunas ventajas.

Es muy práctico que podamos pensar a las 7 capas del modelo OSI como una línea de ensamblaje de una fábrica. Entonces, a medida que avanzamos por cada capa, los datos sufren ciertas modificaciones y se preparan para ir a la siguiente capa.

Funciones de cada capa

En nuestro 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.

Realizaremos una breve descripción de las capas tal como aparece en la figura que se encuentra en la página siguiente.

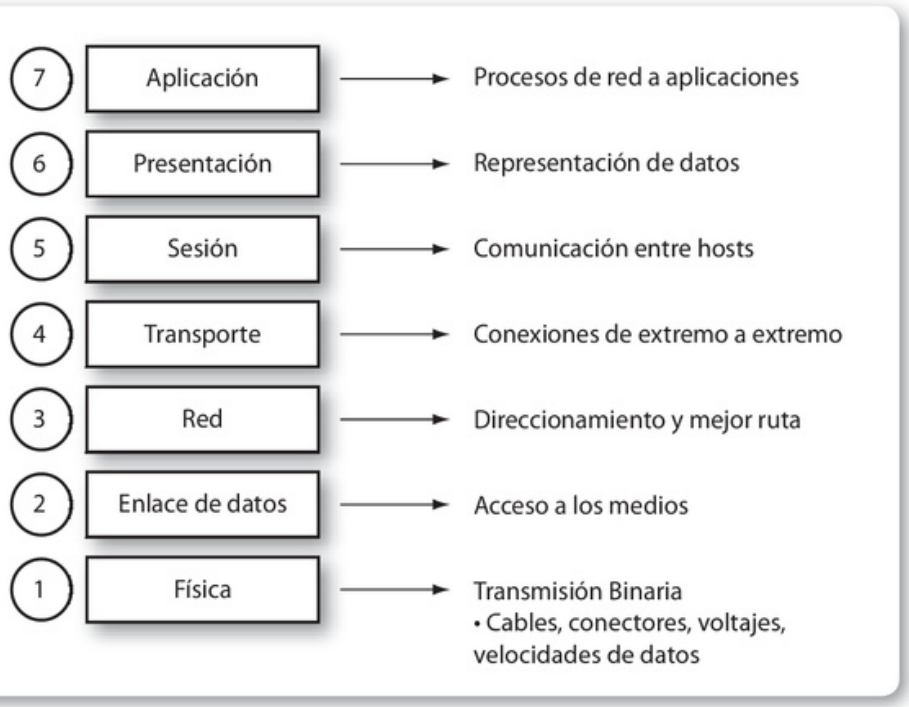


Figura 2. Cada una de las capas del modelo OSI posee funciones que con ayuda de este esquema podremos recordar fácilmente.

• 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, se garantiza que los datos enviados por la capa 7 de un sistema pueda ser entendido por la misma capa 7 pero de otro sistema. En caso de ser necesario, la información será traducida usando un formato en común. Ejemplos en esta capa pueden ser los formatos **MP3**, **JPG**, **GIF**, entre otros.

• 5 – Capa de sesión: en esta capa establecemos, mantenemos y terminamos las comunicaciones entre 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 estos en un solo flujo de datos dentro

de la red física. A esto lo llamamos **control de flujo de datos**. Además se realiza la verificación de errores y recuperación de datos.

• 3 – Capa de red: determina cómo serán enviados los datos al receptor. Realiza 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 le 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 hardware del modelo. Acá se definen las especificaciones o características físicas de la red, como niveles de voltaje, cableado, distancias de transmisión máximas, conectores físicos usados, entre otros atributos descriptos dentro de las especificaciones de la capa física.

Para que recordemos fácilmente todas las capas podemos dividirlas en dos grupos, **grupo de aplicación** y **grupo de flujo de datos**. Las que pertenecen al grupo de aplicación realizan funciones vinculadas al tratamiento y preparación de los datos, para que luego sean transportados a destino por el grupo de flujo de datos (o también llamado grupo de transporte). Las capas del grupo de aplicación son la **Capa de aplicación**, **Capa de presentación** y **Capa de sesión**.

Y las del grupo de flujo de datos: **Capa de transporte**, **Capa de red**, **Capa de enlace de datos** y **Capa física**.



El modelo TCP/IP

Existe otro modelo paralelo al modelo OSI llamado TCP/IP, que es mucho más conocido entre los usuarios. 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 Internet** y 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 de TCP/IP que detallamos a continuación:

4 – Capa de aplicación: se combinan todos los aspectos relacionados con las aplicaciones en una sola capa. 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: directamente se corresponde con la capa de Transporte del modelo OSI. En esta capa usamos uno de sus protocolos, el TCP (protocolo para el control de la transmisión) que nos ofrece formas flexibles y de alta calidad para crear comunicaciones confiables y con errores bajos. Este protocolo es orientado a la conexión, lo que significa que los datos (segmentos) viajan entre dispositivos para comprobar que exista la conexión lógica para un determinado tiempo. Esto último es conocido como **conmutación de paquetes**.

2 – Capa de internet: como vemos en el diagrama, corresponde a la capa de Red del modelo OSI. El principal objetivo es enviar 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. El objetivo es enrutar los datos entre dispositivos en la misma red.

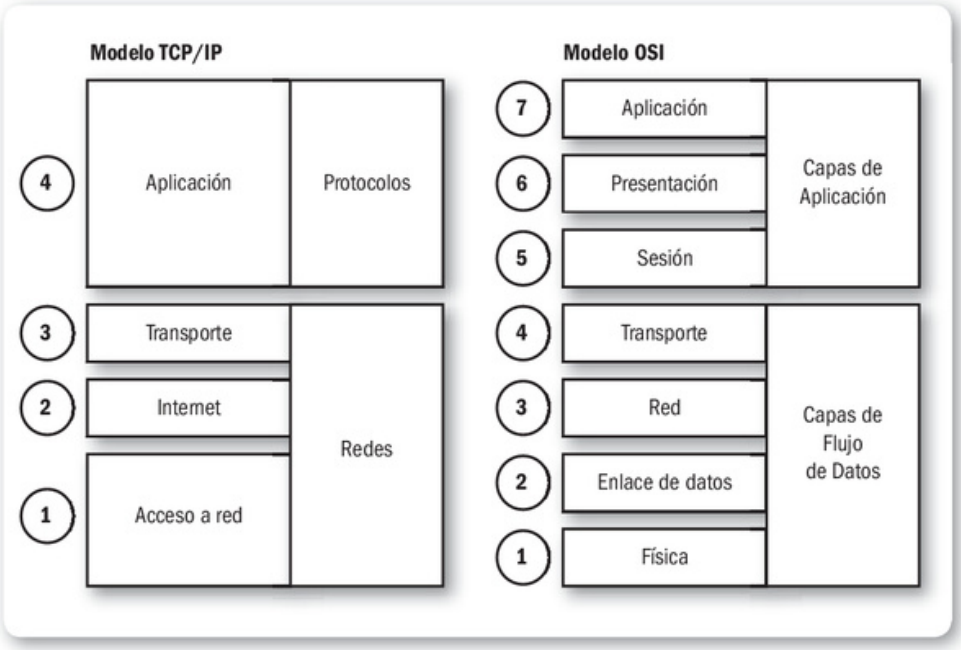


Figura 3. Comparación entre el modelo TCP/IP de 4 capas y el modelo original OSI de 7 capas. Vemos las capas que se entremezclan en el modelo OSI para obtener las equivalentes en TCP/IP.

Tipos de redes

De forma general, podemos clasificar las redes según su extensión geográfica, así tenemos tres tipos principales: redes **LAN** (redes de área local), redes **MAN** (redes de área metropolitana) y redes **WAN** (redes de área amplia). Las desarrollaremos en este apartado.

Las redes LAN pertenecen a usuarios de una entidad privada, por ejemplo la red de un campus universitario o de una oficina son consideradas redes LAN. Pueden extenderse hasta varios kilómetros pero están restringidas en tamaño, lo cual tiene como punto a favor que su administración se ve simplificada, tiene poco retardo en las transmisiones de datos y los errores son menores. Las velocidades de transferencia van desde los 10 hasta los 100 Mbps. Veamos, a continuación, un diagrama de este tipo de red.

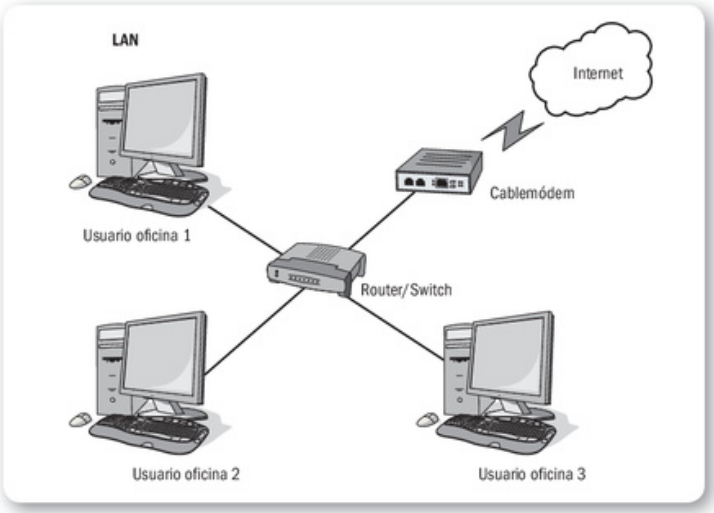


Figura 4. Ejemplo de una red LAN. En este caso, perteneciente a una pequeña oficina con 3 usuarios.

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. Fue creado en el año 1970 por DARPA. 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. El modelo TCP/IP ofrece conectividad entre dos extremos y especifica la forma en que los datos deben ser manipulados para enviarlos y así llegar a destino.

A una versión de mayor escala de la red LAN y que usa casi la misma tecnología la llamamos red MAN. Varias redes LAN interconectadas que cubren una larga área o conectan algunas redes LAN de, por ejemplo, un campus universitario son una red MAN. Existen dispositivos como **routers** y **switchs** que se conectan para formar la red MAN, generalmente, dentro de una misma ciudad.

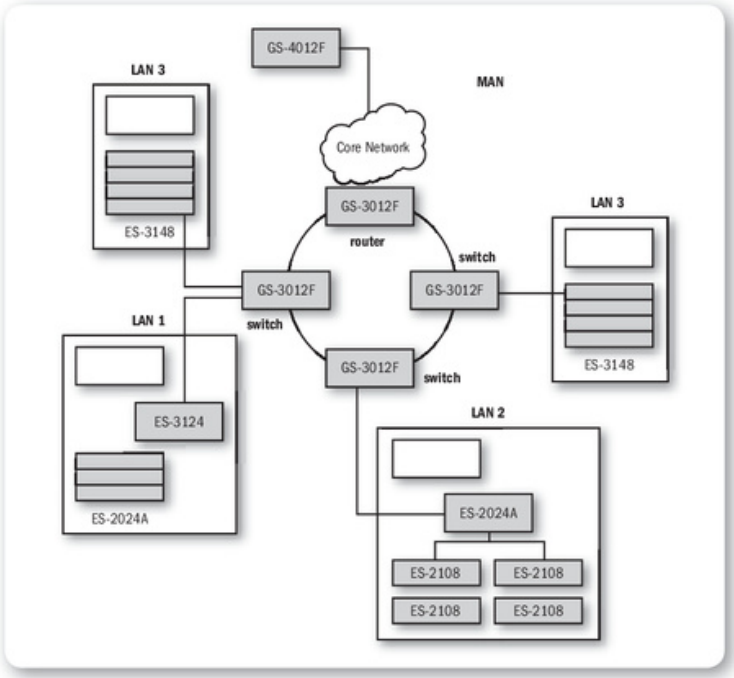


Figura 5. Vemos que varias redes **LAN** interconectadas con dispositivos de red (**routers**, **switchs**) nos permiten formar las redes **MAN**.

Por último, las redes WAN se desarrollan en áreas geográficas relativamente amplias y pueden pensarse como enlaces para grandes distancias que extienden la red LAN hasta convertirla en una red de área amplia (WAN).

Por lo tanto, una WAN conecta varias LAN interconectadas. No existen las limitaciones geográficas, pudiendo conectar equipos de usuarios en diferentes puntos del planeta.Como ejemplo, la más grande y popular de las redes WAN es **Internet**. Podemos pensar Internet como una union de pequeñas redes (LAN), las cuales, al interconectarse entre ellas, forman una gran red global (WAN).

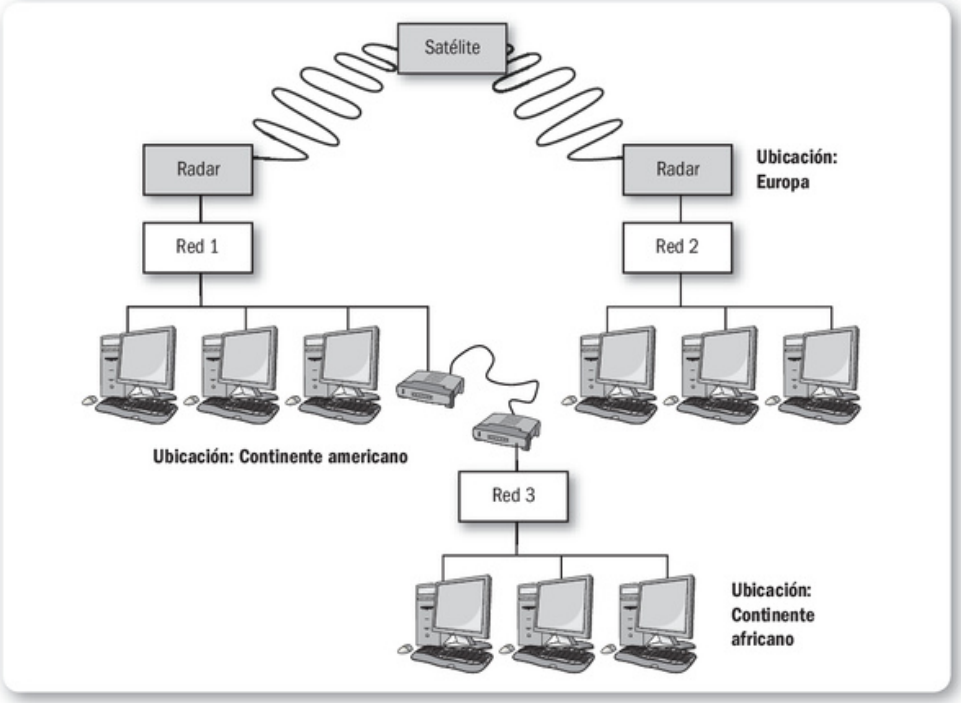


Figura 6. Una red **WAN** es una red que se extiende en un área mayor que las **LAN** y **MAN** y hasta puede ser de alcance mundial.

Topologías básicas de red

Existen varias formas de conectar computadoras para así formar redes. La manera en que estas se conecten depende de variables como las distancias entre computadoras, el grado de estabilidad deseado para la red, ya que es importante que al ocurrir una falla no se caiga todo el conjunto de dispositivos.

A cada dispositivo en la red lo llamaremos **nodo**. Esto puede ser una computadora, una impresora, un escáner u otro elemento.

La disposición de los enlaces que conectan los nodos de una red es lo que definimos como **topología de red.**

Tenemos dos formas de describir la topología de red: **física** o **lógica**.

Para referirnos a la primera, la topología física, tendremos en mente la configuración de los cables, las antenas, las computadoras y otros dispositivos de red. En otras palabras es la forma en la que el cableado se realiza en una red. Mientras que para definir la topología lógica necesitamos pensar en un nivel más abstracto, considerando, por ejemplo, el método y el flujo de la información transmitida

entre los nodos, este tipo de topología implica la forma en que los datos viajan por las líneas de comunicación. A continuación, desarrollaremos algunas de las topologías más comunes:

• **Topología Bus** o **Barra**: es la manera más simple para organizar una red. Todos los equipos están conectados a la misma línea de transmisión por un cable común o compartido. Tiene como ventaja su facilidad para implementarla y ponerla en funcionamiento. Sin embargo, una gran desventaja es que si una de las conexiones es defectuosa, eso afecta a toda la red.

• **Topología Estrella**: los equipos se conectan a un hardware llamado **concentrador**. Todos los datos pasan a través del concentrador antes de llegar a destino. Podemos eliminar una conexión sin que se vea afectada toda la red. Pero como punto crítico tenemos el concentrador, sin este los equipos no pueden comunicarse. Es común para redes Ethernet e inalámbricas.

• **Topología Árbol**: es una combinación de las topologías Bus y Estrella. Un conjunto de nodos configurados como estrella se conectan a un cable común llamado normalmente **backbone**.

• **Topología Anillo**: se forma un lazo cerrado (anillo) con todos los nodos conectados entre sí, o sea que cada nodo se conecta directamente a otros dos dispositivos. Tiene como desventaja la difícil instalación, requiere mantenimiento y al romperse el cable que forma el anillo se para toda la red.

• **Topología Malla**: para formar la malla, es necesario tener enlace directo entre todos los pares de nodos de la red. Es una tecnología costosa pero es muy confiable. Este tipo se utiliza principalmente para aplicaciones militares.



TOPOLOGÍA ANILLO

Las redes con topología en anillo, en realidad, no tienen los nodos directamente conectados entre sí, sino que están conectados a un **distribuidor** (llamado **MAU**, *Multi-Station Access Unit*, en español se puede traducir como **unidad de acceso multiestación**) que administra la comunicación entre los equipos. Un MAU es un dispositivo con varios puertos donde se conectan los nodos. Así se ofrece un control centralizado de todas las conexiones de la red, además de mover las señales entre estaciones de trabajo. También existe la topología de anillos dobles.

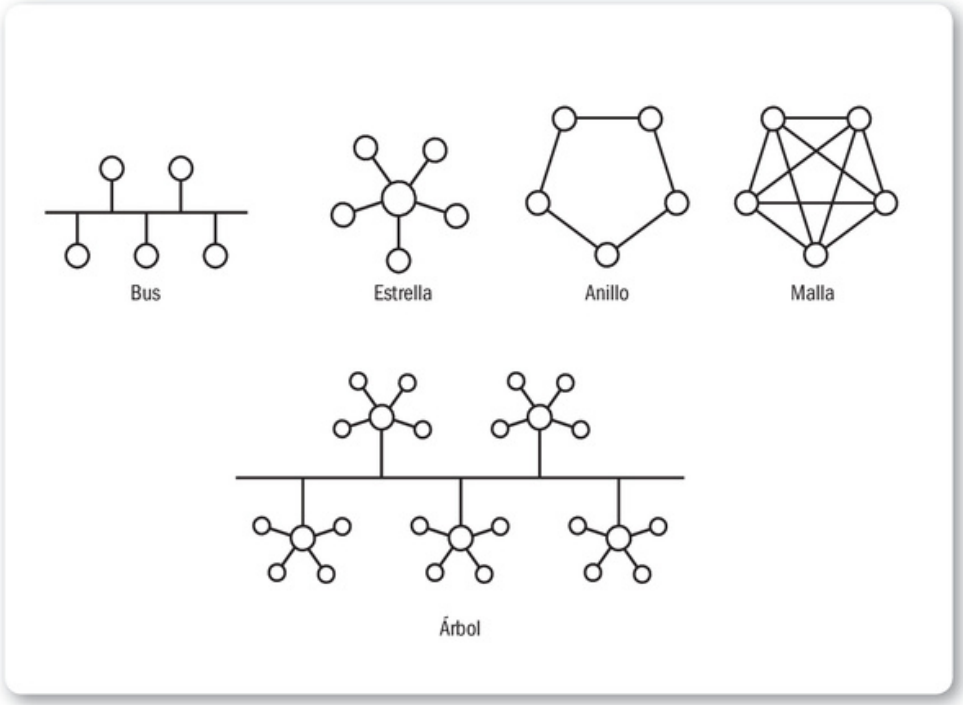


Figura 7. En este diagrama, podemos observar las topologías de red más utilizadas en la actualidad.

Topologías de redes inalámbricas

Como veremos más adelante, las redes inalámbricas son aquellas que no utilizan cables para lograr la comunicación entre los dispositivos. Es decir, para establecer una comunicación inalámbrica no se requiere de un medio (ya sea cables, aire, éter u otro similar), para ello se usan las **ondas electromagnéticas**. Por eso, cuando dibujamos una línea en los diagramas de topología para una red inalámbrica, eso representa una (posible) conexión que se está llevando a cabo. Además es de notar que la comunicación inalámbrica es siempre en dos sentidos (**bidireccional**).

De la misma forma que se tratan las topologías en redes de cables, podemos seleccionar las más convenientes para nuestra red inalámbrica. Veamos ahora cuáles topologías de red pueden aplicarse en nuestras redes inalámbricas.

La principal utilizada (y que podríamos decir es un modelo a seguir en una red inalámbrica) es la topología Estrella, en la que, recordamos, existe un concentrador que vincula todos los nodos.

Si quisiéramos implementar un Bus, veríamos que, generalmente, no es posible, ya que cada nodo se conecta con los demás nodos por un cable en común y para una red inalámbrica esto sería equivalente a una red Malla trabajando en un canal único.

La topología **Árbol** es usada comúnmente por los **ISP** (*Internet Service Provider*; en español se traduciría como **proveedores de servicio de Internet**) inalámbricos.

Por último, sería muy raro tratar de implementar en una red inalámbrica una topología **Anillo**, ya que en esta topología cada dispositivo debe funcionar correctamente para asegurar el funcionamiento de una red operativa. Estas redes existen, pero son muy dificiles de encontrar en el mundo real.

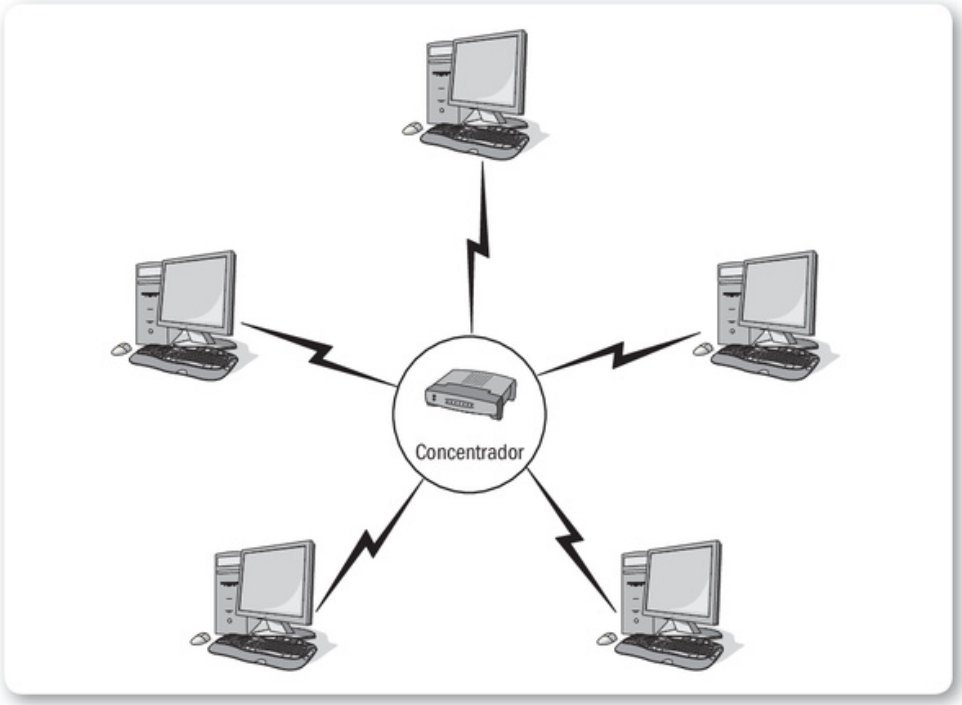


Figura 8. En redes inalámbricas, la topología **Estrella** es la más común de encontrar. Es de fácil funcionamiento e instalación.

La principal ventaja de las redes con topología Anillo es su arquitectura y ampliación sencilla. Además, a diferencia de una topología de bus, las redes en anillo evitan las colisiones ya que transmiten información en un solo sentido.

¿Cuáles son las 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 forma que lo hicimos con las redes cableadas, en este caso tendremos 4 categorías, basándonos en el alcance: redes WAN, redes MAN, redes LAN y redes PAN.

Teniendo en mente el alcance, vemos que las dos primeras categorías WAN/MAN abarcan las redes que cubren desde decenas hasta miles de kilómetros. La categoría LAN es la que está conformada por las redes que alcanzan hasta los 100 metros. La última es una nueva categoría llamada **PAN**, donde están las redes que tienen un alcance de hasta 30 metros.

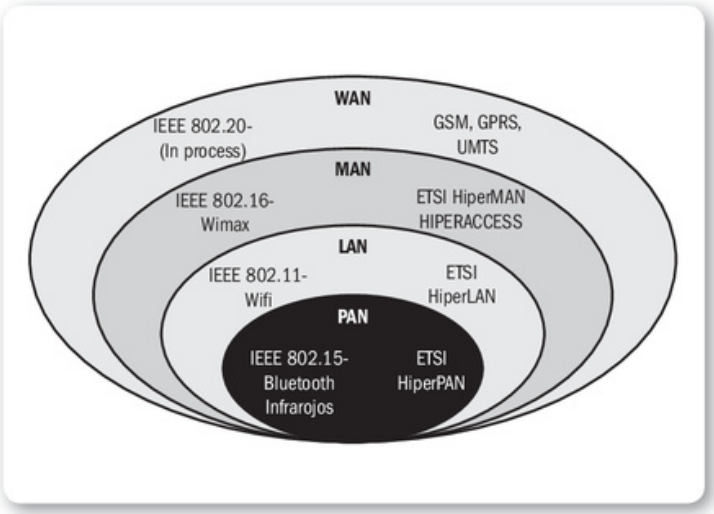


Figura 9. Estas son las diferentes tecnologías inalámbricas junto con sus estándares. Para LAN, tenemos el estándar **IEEE 802.11-WiFi**.

COPIANDO A LAS MOSCAS

Para mejorar el diseño de redes inalámbricas, científicos de la **Universidad de Carnegie Mellon** (EE.UU.) estudiaron el sistema nervioso de la mosca de la fruta. La mejora se logró copiando la organización de las células del sistema nervioso de este insecto. Algunas de estas células actúan como líderes y establecen conexión con otras células nerviosas. Los investigadores desarrollaron el mismo modelo para utilizarlo en redes informáticas distribuidas.

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 y que llamaremos **WLAN**. A este tipo de red inalámbrica se la conoce en el mercado como **WiFi** y opera en la banda de **2.4 GHz**.

¿Cómo funcionan las redes inalámbricas?

En estas redes usamos las ondas electromagnéticas para enlazar, mediante un concentrador, los dispositivos de una red, reemplazando los cables de las redes LAN convencionales.

Dar conectividad y acceso a las redes cableadas son las funciones principales de este tipo de redes. Podemos pensar que son una especie de **extensión** de las redes cableadas pero que nos ofrecen la flexibilidad y la movilidad de las comunicaciones inalámbricas. Al utilizar frecuencias de uso libre, no necesitamos pedir autorización o permiso para usar estas redes. Lo que sí debemos tener en cuenta es la regularización del espectro de frecuencias que varía de país en país.

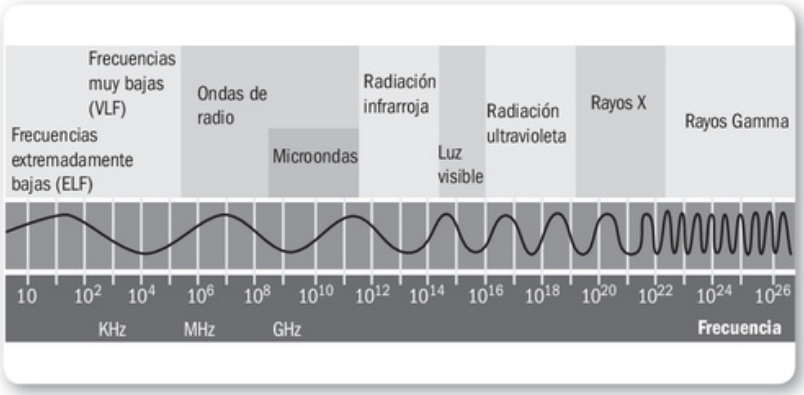


Figura 10. En el diagrama vemos el espectro electromagnético y sus diferentes usos según la banda de frecuencia.

Una desventaja que se presenta, cuando usamos las frecuencias de uso libre (estas son las de **2.4 Ghz** y **5 Ghz**), es que las comunicaciones pueden sufrir **interferencias** y **errores**

de transmisión. Al tener estos errores, los datos se reenvían una y otra vez. Entonces, si en una transmisión la mitad de los datos no llegan a destino a causa de estos errores, tendremos una reducción a las dos terceras partes de la velocidad eficaz real. Esto dará como resultado una variación en la velocidad máxima especificada en teoría comparándola con la que obtenemos en la realidad.

Teniendo largas distancias, la velocidad real en las redes WiFi estará muy por debajo que la especificada en las normas, dado que factores como la potencia de transmisión, las distancias o el área de cobertura, el tipo de modulación empleada, el ambiente propenso a la interferencia, entre otros, afectan directamente a esta velocidad.

> LA FLEXIBILIDAD ES OTRA VENTAJA DE LAS REDES SIN CABLES

Por ejemplo, muchas redes 802.11g (veremos más adelante en este capítulo la familia de IEEE 802.11) en interiores tienen un área de cobertura de hasta 200 metros. Si agregamos potencia podemos extender esta distancia, pero dependerá de los objetos o paredes que puedan interferir la señal.

El término **SSID** (*Service Set Identifier*, en español: **identificador del conjunto de servicio**) puede parecernos familiar, ya que es el mecanismo que utilizan los usuarios para identificarse en la red al momento de conectarse. Este debe ser el mismo para todos los integrantes de una red inalámbrica específica. Todos los puntos de acceso y usuarios del mismo **ESS** (*Extended Service Set*, en español: **conjunto de servicio extendido**) deben configurarse con el mismo **identificador** (**ESSID**). Pensemos a este identificado, como el nombre de la red inalámbrica a la que nos queremos conectar, todos los usuarios conectados a esta tendrán idéntica etiqueta.

BANDA BASURA

La historia del WiFi inicia en **1985**, cuando el gobierno de los Estados Unidos (junto con la **Comisión Federal para las Comunicaciones**) decide que se pueden usar ciertas bandas del espectro sin tener una licencia. La llamada **banda basura de 2.4Ghz** era una de estas bandas, que solo era utilizada para hornos microondas o equipos similares que generaban ruido de radiofrecuencia.

Ventajas de utilizar redes inalámbricas

Vamos a describir algunas ventajas que obtenemos al usar una red inalámbrica comparándola con las redes cableadas clásicas. La primer ventaja que aparece y una de la más importante es la **movilidad** que adquiere el usuario de estas redes. Una computadora o cualquier dispositivo (**laptop**, **teléfono**, **impresora**, entre otros) puede acomodarse en cualquier punto dentro del área de cobertura de la red, sin tener que preocuparnos si es posible o no hacer llegar un cable de red hasta este lugar. No es necesario estar atado a un cable para imprimir documentos, compartir música o navegar por Internet, entre otras muchas tareas que podemos realizar.

UNA DE LAS VENTAJAS MÁS IMPORTANTES DE LAS REDES INALÁMBRICAS ES LA MOVILIDAD

La **portabilidad** es otro punto importante de las redes inalámbricas, 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. Se facilita el trabajo permitiendo la movilidad por toda el área de cobertura.

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.

También el uso de las redes inalámbricas es indicado para lugares donde se necesitan accesos esporádicos o temporales (como lo son las conferencias, los entrenamientos empresariales, charlas, hoteles, lugares públicos, instituciones educativas, entre otros.)

Al tratar de extender una red cableada clásica se presentan ciertos problemas, ya que esto no es una tarea fácil ni barata. En cambio, cuando queremos expandir la red inalámbrica, luego de su instalación inicial, simplemente debemos adquirir una placa de red inalámbrica (si es que la computadora no cuenta con ella) para ya estar conectados. Esto se llama **escalabilidad**, que se define como la facilidad de expandir la red luego de ser instalada. Si lo contrastamos con las redes cableadas, necesitaríamos instalar un nuevo cableado para esa nueva computadora, lo que implica pérdida de tiempo y dinero.

Y este último punto es otra ventaja, el **ahorro de costos** que genera este tipo de redes, ya que no existe el gasto en diseñar e instalar que tenemos en una red cableada.

Nuevamente la facilidad de instalación e implementación nos permite tener nuestra red doméstica o en nuestra oficina, funcionando en poco tiempo y con un costo bajo.



Figura 11. Ventajas de las redes inalámbricas: portabilidad y flexibilidad al tener una red hogareña.

Desventajas de utilizar redes inalámbricas

Las redes inalámbricas también presentan ciertas desventajas, no todo es color de rosa cuando queremos utilizar estas redes. Veamos cuáles son los principales puntos en contra que tenemos.

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 (veremos más adelante qué significa esto) que llegan a mejores velocidades pero el precio es muy superior.

Podemos decir que es necesaria una **mayor inversión inicial**, ya que el costo de los equipos de red inalámbricos es superior al de los necesarios en la red cableada. Pero no es tanta la diferencia para una red hogareña pequeña o de oficina.

Dijimos anteriormente que una ventaja de las redes inalámbricas es la de no necesitar un medio físico para funcionar. Esto se convierte en desventaja cuando tenemos en cuenta la **seguridad** de nuestra red. Pensemos que cualquier persona con una notebook o un teléfono con WiFi puede intentar acceder a nuestra red tan solo estando en el área de cobertura. Ya que esta área no está delimitada por paredes u otra barrera, la persona interesada en ingresar a nuestra red no necesita estar dentro de nuestra casa o edificio y menos estar conectada por medio de un cable. Veremos más adelante el sistema de seguridad que tienen las redes WiFi.

El **alcance** de una red inalámbrica está determinado por la potencia de los equipos y la ganancia de las antenas, así si estos parámetros no son suficientes habrá puntos en nuestra casa u oficina donde no tengamos cobertural, suele haber obstáculos que interfieren.

Por último, pero no menos importante, tenemos a las interferencias sufridas en la banda de frecuencias de 2.4 GHz como desventaja. Al no requerir licencia para operar en la banda de 2.4 GHz, muchos equipos del mercado la utilizan (**teléfonos inalámbricos**, **microondas**, entre otros) sumado a que todas las redes WiFi funcionan en la misma banda de frecuencias, incluida la de nuestro vecino.

Cuanto mayores sean las interferencias producidas por otros equipos o que existan en el ambiente, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que las tengamos ya que la mayoría de las redes inalámbricas funciona sin problemas.



Figura 12. En este caso, el **horno microondas** y el **teléfono** provocan una pérdida de señal.

Componentes de redes inalámbricas

Estudiaremos los diferentes dispositivos que son necesarios en nuestras redes inalámbricas, los fundamentales son: placa de red inalámbrica, punto de acceso (**AP**, *Access Point* en inglés), router inalámbrico y las antenas. Además existen otros equipos y accesorios que se utilizan y veremos pero con menos detalles.

> EXISTEN TRES TIPOS DE ADAPTADORES PARA UTILIZAR EN NUESTRAS REDES: PCI, PCMIA/PCCARD Y USB

• **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). Si poseemos una notebook o algún celular nuevo, la placa viene integrada.

Existen tres tipos de adaptadores para utilizar en nuestras redes: 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.

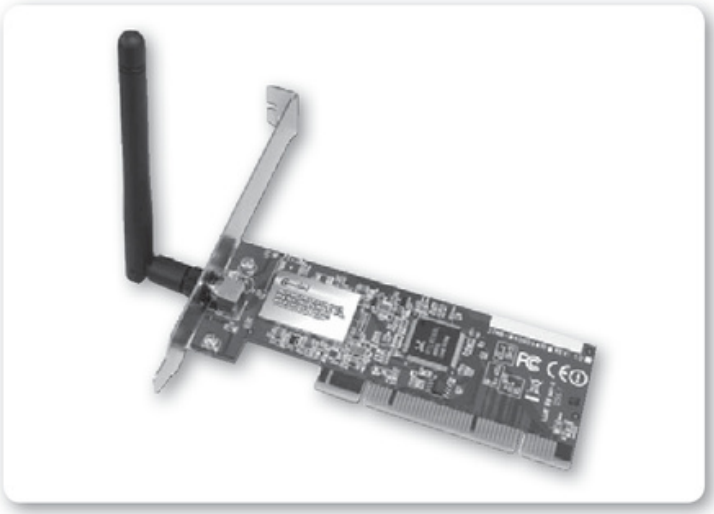


Figura 13. Las placas PCI inalámbricas son utilizadas en nuestras computadoras hogareñas para evitar conectarnos con cables a la red.

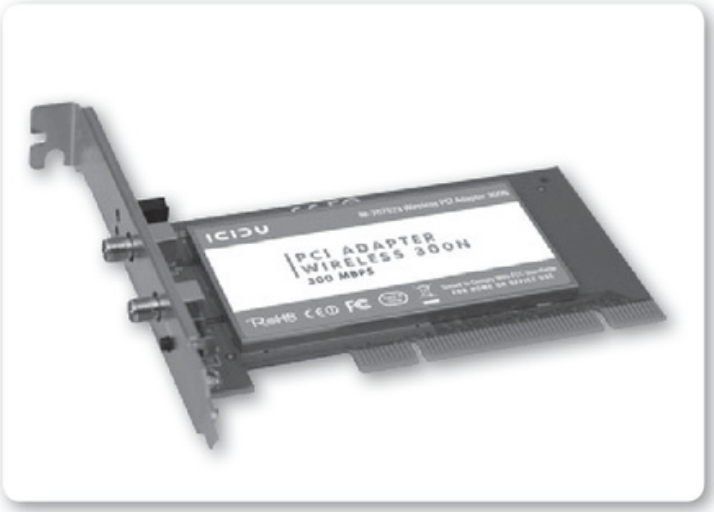


Figura 14. Muchas placas PCI que utilizan la norma 802.11n poseen varias antenas.

Estas placas inalámbricas nos permiten conectarnos a una red de forma fácil.



Figura 15. En las primeras laptops no existían las placas de red inalámbricas integradas, por eso teníamos la opción PCMCIA/ Pccard.

VER A TRAVÉS DE LAS PAREDES CON WIFI

En la **Universidad de Utah**, en los Estados Unidos de Norteamérica, 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**.



Figura 16. En la actualidad es común el uso del dispositivo USB para conectarse a la red 3G que proveen algunos prestadores telefónicos.

La placa inalámbrica USB es ideal para utilizarla en viejas computadoras de escritorio.



Figura 17. El dispositivo inalámbrico USB puede tener antena externa

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

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



Figura 18. La figura nos muestra un AP que encontramos en el mercado.

Los AP trabajan en velocidades de 54 Mbps a 108 Mbps y en general poseen dos antenas que pueden ser reemplazadas por otra de mayor ganancia. Hay modelos donde la antena es interna y reemplazarla no es posible. Como seguridad poseen encriptación con claves WEP, WPA y WPA2, así como filtros por **MAC** o incluso uso de servidor **Radius**. Estos conceptos los veremos en detalle más adelante,en este mismo libro.

Existen dos características importantes en un AP: la potencia de su transmisor y la sensibilidad del receptor. La primera se refiere a qué tan potente es la señal que irradia el equipo y la medimos en **dbm** (unidad de medida de potencia) o **mw** (miliwatts). En cuanto a la sensibilidad del receptor se refiere a qué tan débiles pueden llegar a ser las señales que detecta el AP, utilizamos el dbm para medirla.

Nosotros consideramos un equipo **óptimo** aquel que tiene buena potencia de salida y buena sensibilidad de recepción que nos permita detectar señales de poca potencia. Suelen ser equipos de mejor calidad y un tanto más caros.



Figura 19. Muchas marcas reconocidas fabrican sus propios AP que apuntan a las pequeñas y medianas empresas.

• **Router inalámbrico**: si tenemos una conexión **ADSL** que nos da acceso a Internet a través de nuestra línea telefónica, este dispositivo será el encargado de conectarnos. Pero no es la única función, ya que además permite distribuir Internet mediante cables y de forma inalámbrica con el punto de acceso que tiene integrado. También realiza restricciones de acceso, por usuarios, servicios, horarios, entre otros y en muchos casos puede controlar el ancho de banda y las prioridades de acceso por cliente conectado o servicio. Todas estas facilidades nos permiten tener un control de lo que ocurre en nuestra red inalámbrica o cableada.



Figura 20. Un router inalámbrico nos permite usar las diversas configuraciones en nuestra red.



Figura 21. Algunos modelos de routers inalámbricos que existen en el mercado poseen antenas externas.

• **Antenas**: son un elemento muy importante en nuestra red, ya que se encargan 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. Si la transformación es eficaz, obtendremos mayor área de cobertura (o alcance) sin importarnos el equipo que tengamos.

Pensemos en la antena como un dispositivo que nos permite convertir la señal eléctrica en ondas electromagnéticas. Solamente la antena se considera más del 50% de la calidad de conexión para un dispositivo de la red, de esta forma necesitamos que la antena sea buena o superior.

Existen diferentes tipos de antenas, algunas son complejas y robustas pero otras son fáciles de instalar y con buen rendimiento. Lo que siempre buscamos es que la transformación de energía sea realizada sin pérdidas, o sea de forma óptima, y así nuestra antena

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)

será considerada una **buena antena**. Podemos diferenciar las antenas por su forma de irradiar la energía electromagnética, así tenemos antenas **omnidireccionales** (que irradian en todas las direcciones) y las **direccionales** (que difunden la energía electromagnética en una sola dirección).Veremos más del funcionamiento de las antenas en el **Capítulo 8**.



Figura 22. Existen muchas variedades de antenas según sus características, como ganancia, tamaño, entre otras.

Tenemos otros equipos y accesorios en una red inalámbrica que no son fundamentales para su funcionamiento y se transforman en soluciones puntuales o específicas para ciertos casos. Estos son: **cámaras de vigilancia inalámbricas**, **amplificadores de señal**, **protectores de rayos**, equipos **PoE** (de sus siglas en inglés, *Power over Ethernet*) que permiten recibir con un cable de red **UTP** no solo datos sino también energía y así alimentar, por ejemplo, un AP. **Divisores de señal**, **cajas Estanca** (o *weather proof*) y torres para

¿QUÉ SIGNIFICA AD HOC?

Para tener como dato, el término ad hoc es latino y significa **para esto**, sin embargo se usa comúnmente para describir situaciones o eventos improvisados y en general espontáneos. En una red inalámbrica el modo ad hoc es un método por el cual los dispositivos se comunican directamente entre ellos dentro de un area determinada.

montar equipos son tenidos en cuenta al armar una red inalámbrica de largo alcance, comúnmente llamados **enlaces de larga distancia**.

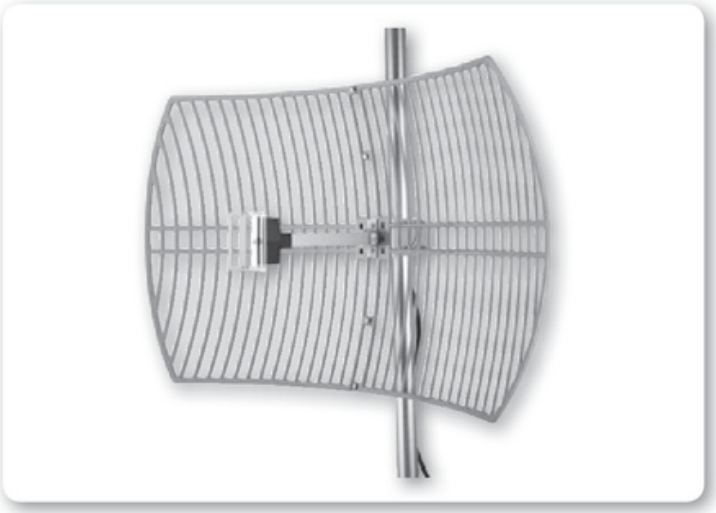


Figura 23. Este tipo de antenas son ideales para los enlaces punto a punto en largas distancias.

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**. Debemos tener presente que estos modos no siempre se ven reflejados en la topología, así un enlace que vincule dos puntos distantes (llamado enlace punto a punto) puede implementarse en modo ad hoc o infraestructura y nosotros podríamos pensarla como una red estrella conformada por conexiones ad hoc. De esta forma, el modo sería la configuración de la placa de red inalámbrica en un nodo y no una característica de toda la red.

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 (notebooks, smartphones, entre otros) que poseen placas de red inalámbricas. También se lo conoce con el

nombre de punto a punto, ya que permite establecer una comunicación directa entre los usuarios de la red sin necesidad de involucrar un punto de acceso central que realice el vínculo. 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).

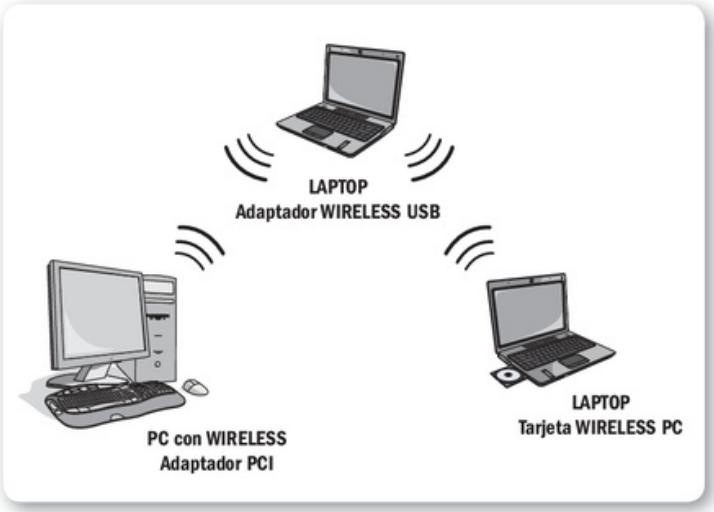


Figura 24. Ejemplo de una red ad hoc conformada por dispositivos comunes en cualquier hogar.

Cuando configuramos este tipo de redes, debemos considerar como requisito fundamental el rango de cobertura de la señal. Como vemos en la figura anterior, necesitamos que los dispositivos móviles estén dentro de cierto rango para que la comunicación sea efectiva. Cada uno de los usuarios en nuestra red inalámbrica deberá configurar la placa de red en modo ad hoc y utilizar los mismos **SSID** y **número de canal** de la red.

Podemos deducir que en un pequeño grupo de dispositivos dispuestos cerca uno de otro conformando nuestra red ad hoc, el rendimiento es menor a medida que el número de nodos aumenta dado que se incrementan las conexiones necesarias entre los usuarios para comunicarse entre ellos.

Si nosotros quisiéramos conectarnos desde nuestra red ad hoc a una red LAN cableada o a Internet, necesitamos usar un dispositivo que funcione como **pasarela** o **gateway**. Esto es así ya que los dispositivos tienen conectividad entre ellos pero no hacia una red externa, como puede ser Internet.

Caso de ejemplo: punto a punto

Si disponemos de dos notebooks que están en diferentes oficinas, ubicadas una en cada extremo del edificio y queremos vincularlas de forma directa, usaremos el modo ad hoc. Lo mismo haremos si necesitamos conectar más de dos usuarios a nuestra red.

TABLA 1

▼ CONFIGURACIÓN	▼ USUARIO A	▼ USUARIO B
MODO	Ad hoc	Ad hoc
SSID	RED_SSID	RED_SSID
CANAL	Mismo para todos	Mismo para todos
DIRECCIÓN IP	Dirección fija	Dirección fija

Tabla 1. En esta tabla vemos los datos que utilizaremos para configurar de modo correcto nuestras estaciones de trabajo.

Como dijimos antes, si un usuario o nodo está conectado a Internet, podemos extender esa conexión a otros usuarios que se vinculan inalámbricamente a nosotros con el modo ad hoc.

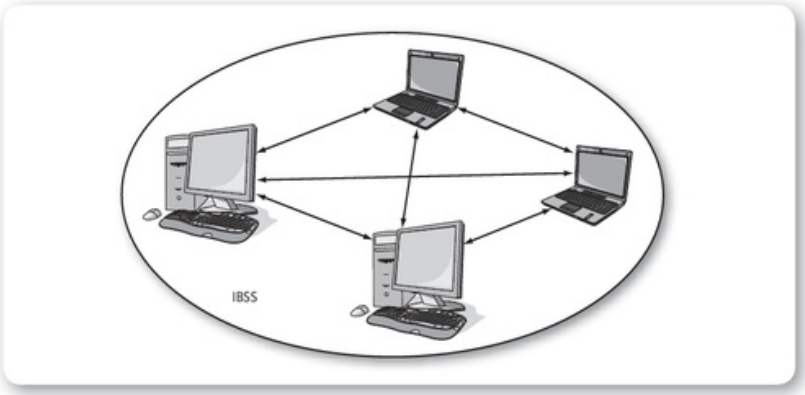


Figura 25. El modo ad hoc, según el estándar inalámbrico, se denomina Conjunto de Servicios Básicos Independientes.

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 nuestra red, ya que ahora la distancia máxima no es entre estaciones, sino entre una estación y un punto de acceso. Estos dispositivos capaces de extender nuestra red son colocados en lugares estratégicos, en general son lugares altos y además realizan la coordinación del funcionamiento entre usuarios. Con solo un punto de acceso podemos soportar un grupo acotado de usuarios y nuestro 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.

> LOS PUNTOS DE ACCESO FUNCIONAN COMO REPETIDORES Y , POR ESO, PUEDEN DUPLICAR SU ALCANCE

Para lograr optimizar la capacidad total de la red, no es necesario configurar el mismo canal para todos los puntos de acceso que están en la misma área física.

Cada uno de los usuarios descubrirán (mediante un proceso llamado **escaneo de red**) el canal que usa el punto de acceso, por lo tanto no hace falta tenerlo configurado de antemano.

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. De esta forma, 802.11b ofrece un rendimiento máximo de 11 Mbps -que decáe a 6 Mbps en la práctica- en un area de cobertura de hasta 300 metros (en pruebas al aire libre), con la frecuencia de 2.4 GHz y 3 canales disponibles.

Se conoce este modo como Conjunto de Servicios Básicos (BSS por sus siglas en el idioma inglés).

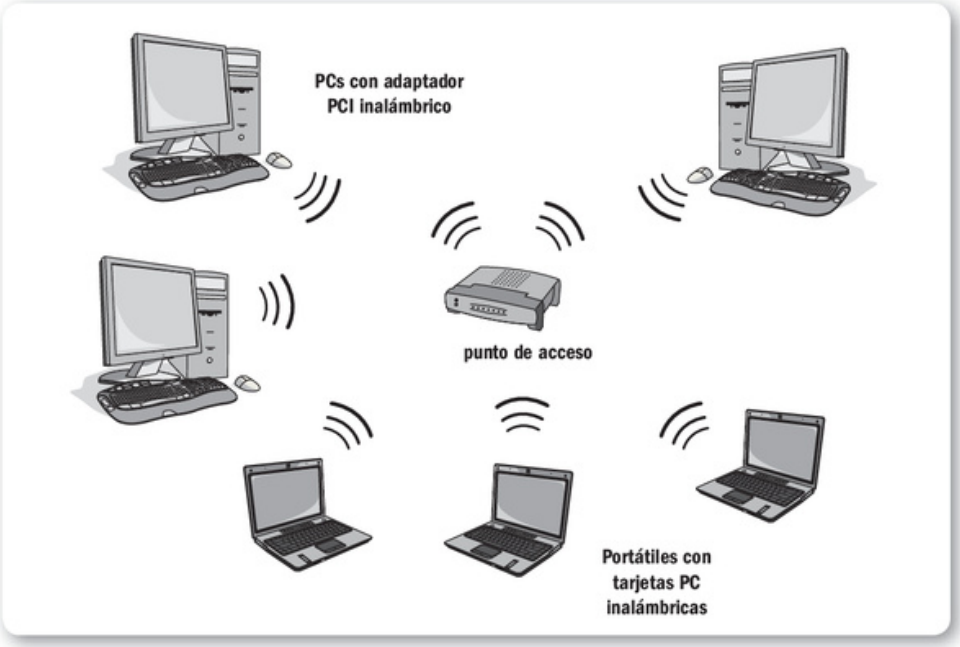


Figura 26. En el diagrama vemos cómo un mismo punto de acceso puede proveer de comunicación a usuarios con diferentes adaptadores de red inalámbrica en modo infraestructura.

Podemos vincular nuestra red inalámbrica de forma fácil con la red cableada para poder proveer a nuestros usuarios de servicios como e-mail, servidor de impresiones, acceso a Internet, entre otros.

802.11 EN JAPÓN Y EUROPA

Debido a su tardía llegada al mercado, la norma **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. En **Japón**, la frecuencia de 5 Ghz también está parcialmente disponible por lo tanto no es muy común encontrar dispositivos que usen 802.11a. Por ejemplo, HiperLan, cuyo estándar fue aprobado en 1996, ofrece una solución estándar para operar en un rango de comunicación corto entre estaciones como lo haría 802.11a.

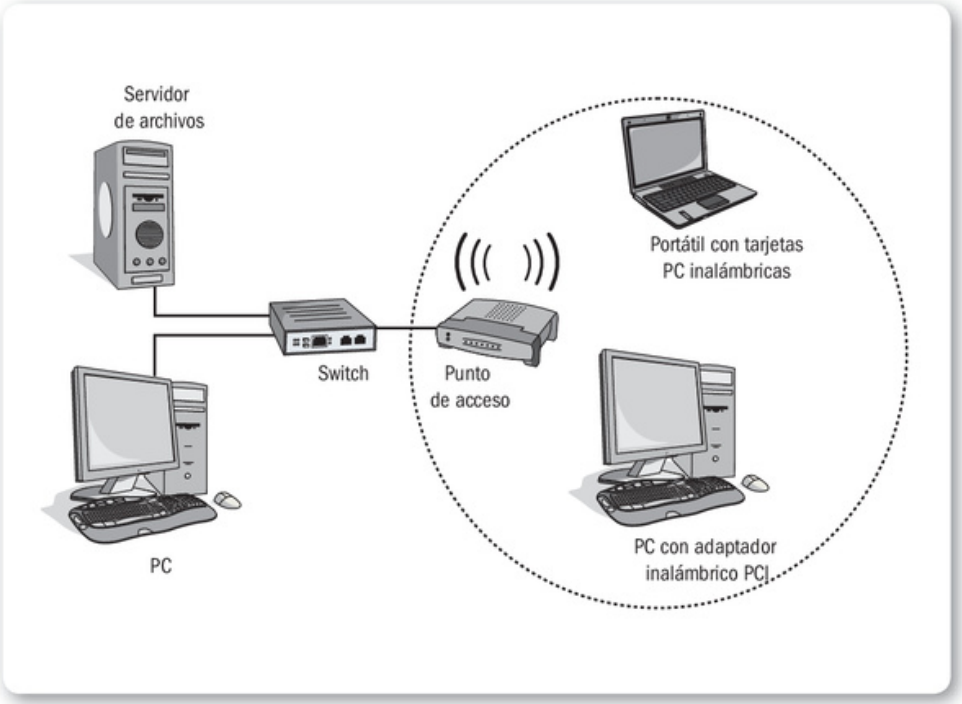


Figura 27. En la imagen se introduce un switch que alarga la red a nuevos usuarios. dentro de cierta área.

Caso de ejemplo: estrella, punto a punto, repetidores y malla

El primer ejemplo que veremos será el de estrella, ya que, tal como lo habíamos dicho, es la configuración más común de encontrar en redes inalámbricas. Esta tecnología es la que se utiliza en los tan famosos **hotspot** (punto de conexión a Internet), que podemos

WIFI + PICNIC + REUNIÓN

WiFiPicning es la última moda para conocer gente si uno es tímido. Esta moda nacida en Francia pero extendida a todos lados agrupa personas con sus notebooks en torno a un **hotspot** donde comparten charlas, bebidas y tiempo. Lo llamativo es que los participantes se conectan a un chat e interactúan desde sus computadoras. La palabra WiFiPicning es una combinación de las palabras Wi-Fi, picnic y *happening* (palabra de lengua inglesa que se puede traducir como evento, ocurrencia o suceso). En América Latina también se está utilizando.

encontrar en universidades, aeropuertos o espacios públicos. Un proveedor de servicios de Internet inalámbrica (WISP por sus siglas en inglés) generalmente utiliza esta disposición en sus redes, la cual combina con topologías Árbol o elementos de otras topologías.

TABLA 2

▼ CONFIGURACIÓN	▼ USUARIO A	▼ USUARIO B
Modo	Infraestructura	Infraestructura
SSID	Seleccionar el SSID	Conectarse al SSID definido
Canal	Fijar un canal	Descubrir el canal
Dirección IP	Posee servidor DHCP	Toma IP que se le asigna por DHCP

Tabla 2. Lograremos configurar una topología en estrella para el modo infraestructura siguiendo los parámetros de esta tabla.

Un elemento que es considerado un estándar de la infraestructura inalámbrica son los enlaces punto a punto (PtP). Analizando la topología, vemos que estos enlaces pueden ser parte de una estrella, una simple línea imaginaria que une dos puntos de forma inalámbrica, o similar en otra topología. Los enlaces PtP los podemos conformar en modo ad hoc o infraestructura. De esta forma, no siempre tiene que existir una línea visual entre equipos.

MÚSICA EN TODOS LADOS

La empresa Sonos nacida en EE.UU. que fabrica equipos inalámbricos presentó un sistema de música distribuida para toda nuestra casa. Funciona ubicando sistemas de sonido especiales 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. La transmision de los contenidos musicales se realiza con alta calidad y, además. el sistema no ofrece ningún tipo de retardo en la transferencia de información. Actualmente, en América Latina, muchos equipos de música vienen con tecnología WiFi.

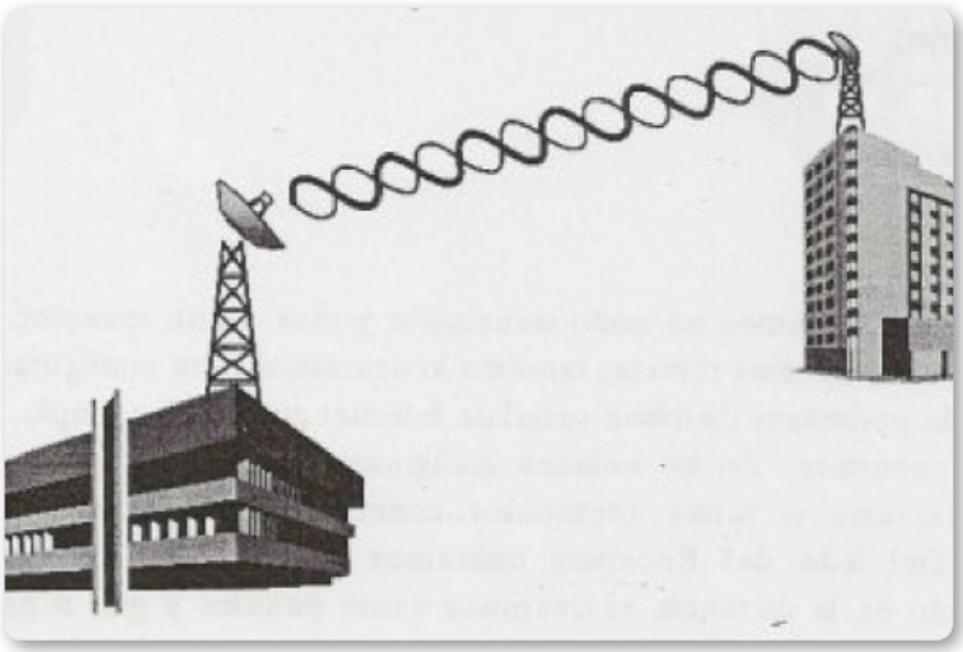


Figura 28. La imagen muestra un enlace **PtP** entre dos edificios de una misma empresa. Podemos usar modo ad hoc o infraestructura en distancias cortas o largas.

Con un ejemplo apreciamos la simplicidad de la configuración.

TABLA 3

▼ CONFIGURACIÓN	▼ USUARIO A	▼ USUARIO B
Modo	Cualquiera	Cualquiera
SSID	RED_ SSID	RED_ SSID
Canal	Cualquiera	Cualquiera
Dirección IP	Establecer dirección fija	Establecer dirección fija
Dirección física (MAC)	Indicar la dirección física del otro nodo	Indicar la dirección física del otro nodo

Tabla 3. Configuración de enlace punto a punto entre dos usuarios.

Utilizamos repetidores cuando tenemos obstáculos en la línea visual directa entre nuestros nodos (en general para enlaces PtP de largas distancias ocurre esto) o existe una distancia muy larga para un solo enlace. El dispositivo equivalente que existe en las redes cableadas para el repetidor inalámbrico es el **hub** (concentrador).

Por último, la topología Malla es una la opción reinante en ambientes urbanos, aunque también se adapta a mayores distancias donde es difícil implementar una infraestructura central. La encontramos en redes del gobierno, barrios o en campus universitarios.

Todos los nodos de una malla tienen que tener el mismo protocolo, pero pueden tener diferentes sistemas operativos y distintos tipos de hardware.Veamos la tabla siguiente con su configuración.

TABLA 4

▼ CONFIGURACIÓN	▼ USUARIO A	▼ USUARIO B
Modo	Ad hoc	Ad hoc
SSID	RED_ SSID	RED_ SSID
Canal	Canal fijo	Canal fijo
Dirección IP	Establecer dirección fija	Establecer dirección fija
Dirección física (MAC)	Indicar la dirección física del otro nodo	Indicar la dirección física del otro nodo

Tabla 4. Configuración típica de una red malla donde se recomienda usar direcciones IP estáticas en los nodos.

El estándar IEE

Muchas personas desconocen la importancia de un estándar, en nuestro caso esto nos servirá como guía para las redes inalámbricas. Es muy común escuchar sobre IEEE 802.11, pero ¿tenemos conocimiento de qué implica que cierto estándar sea más rápido que otro?

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

Entonces, nos preguntaremos ¿para qué sirve un estándar? Los estándares se utilizan por vendedores para darles garantías a sus clientes de la seguridad, la calidad y la consistencia de sus productos y a los cliente les permite no estar **vinculados** a un único vendedor.

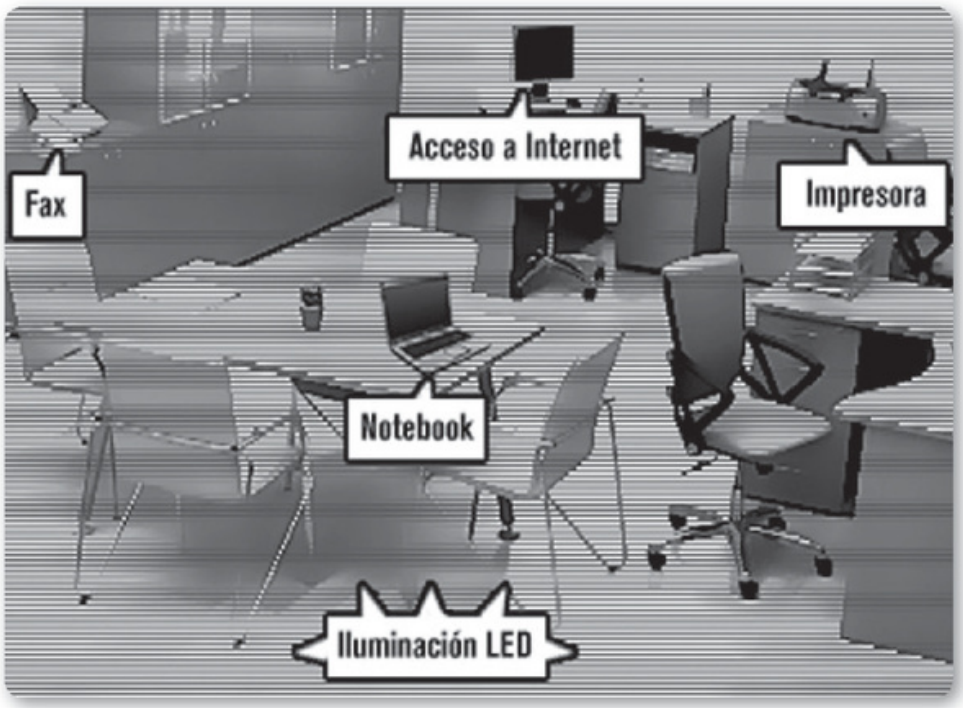


Figura 29. Poseer un estándar nos permite que diferentes artefactos en nuestros ámbitos puedan interactuar y realizar funciones sin problemas.

Estándar abierto y cerrado

Hablar de estándar abierto y cerrado es similar a decir estándar que es público o propio de un fabricante o vendedor. Para graficarlo de alguna forma, si creamos un documento de Excel será un estándar cerrado, mientras que un ejemplo de estándar abierto es escribir código para una página web en **lenguaje HTML**. Cualquiera puede hacer uso de un estándar abierto, esto incrementa la compatibilidad entre el hardware, el software o los sistemas. Si lo vemos desde el lado práctico, seguir el estándar abierto cuando desarrollamos un

producto nos permitirá crear algo que pueda trabajar en conjunto con otros productos que sigan las mismas especificaciones de ese estándar.

Es un error pensar que un estándar abierto es gratuito y no debe pagarse por el uso de derechos o licencias. Muchos se pueden usar sin cargo pero en otros, los titulares de esas patentes pueden solicitar algún tipo de remuneración por el uso del estándar.

LOS ESTÁNDARES PARA REDES LAN/MAN SON UNOS DE LOS PRODUCTOS MÁS CONOCIDOS

Así, podemos decir que estándares abiertos facilitan la interoperabilidad y el nacimiento de nuevos productos, ya que se crea una competición entre fabricantes que tienen que atarse a reglas de juego comunes dictadas por el estándar.

Los grupos de trabajo de la IEEE

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**).

Existen varios grupos de trabajo que realizan diferentes actividades. Los integrantes son voluntarios de todas partes del mundo que se juntan varias veces al año para votar y discutir diferentes propuestas que pueden o no salir a la luz.



Figura 30. El logo del Instituto de Ingenieros Eléctricos y Electrónicos es certificado de calidad.

Familia IEEE 802

La IEEE es la principal generadora de estándares para redes, en la que la IEEE 802 fue definida como una familia de estándares referentes a redes LAN y MAN. La norma solo abarca las redes que transportan paquetes de información con tamaño variable (redes Ethernet) y no redes con paquetes fijos.

Anteriormente vimos que las dos capas de más bajo nivel del modelo OSI son la capa física y la de enlace de datos, estas son las capas que se relacionan directamente con las especificaciones detalladas en la IEEE 802. Dentro de la IEEE, existe un comité de estándares LAN/MAN que mantiene la familia IEEE 802, en el que se establecen grupos de trabajo para cada una de las 22 áreas que incluye.

En el siguiente apartado, veremos el IEEE 802.11, que es el dedicado a redes LAN inalámbricas.

¿Qué es IEEE 802.11?

Nuestro estándar IEEE 802.11 posee una tecnología clave que es el **DSSS** (Espectro de dispersión de secuencia directa). El DSSS nos permite transmitir hasta 11 Mbps operando dentro del intervalo de 1 a 2 Mbps, si opera por encima de los 2 Mbps no se cumpliría con la norma. Se especifica como método de acceso al medio el **CSMA/CA** (Acceso múltiple por detección de portadora/Limitación de colisiones), similar al usado en las redes cableadas.

El **CSMA/CA** es un método bastante ineficaz, ya que utiliza mucho ancho de banda para asegurar que la transmisión de datos sea confiable. Pensemos al ancho de banda como una cañería de agua de nuestros hogares, donde el caudal interno que fluye son los datos. Nuestra cañería tiene una determinada capacidad (ancho de



ESTANDAR 802.11G

Nuestro estándar inalámbrico 802.11g demoró varios años en ser aprobado, ya que se trataron varios puntos referidos a la compatibilidad con 802.11b donde los intereses comerciales fueron puntos fuertes a tener en cuenta dado que se competiría directamente con otros productos de mayor velocidad pero incompatibles el estándar con 802.11b

banda) que al ser utilizada por un caudal de agua importante (datos) nos disminuye la velocidad de transporte. Con este simple ejemplo buscamos comprender el concepto anterior.

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 para atrás** es importante, ya que nos permite actualizar nuestra red sin necesidad de cambiar nada.

Luego, en el estándar 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, dada su frecuencia.

Una nueva enmienda llamada IEEE 802.11g nos ofrece compatibilidad para 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.

TABLA

ESTÁNDAR WLAN	EEE 802.11B	EEE 802.11A	EEE 802.11G	EEE 802.11N
Organismo	IEEE	IEEE	IEEE	IEEE
Finalización	1999	2002	2003	2005
Denominación	WiFi	WiFi 5	WiFi	
Banda de frecuencia	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz y 5.8 GHz
Velocidad máxima	11 Mbps	54 Mbps	54 Mbps	108 Mbps
Thoughput medio	5.5 Mbps	36 Mbps		
Interfase aire	DSSS	OFDM	OFDM	OFDM

Tabla 5. Comparación de las diferentes tecnologías normalizadas por la IEEE donde vemos las principales diferencias entre cada enmienda.

¿Cómo se dice WiFi, WLAN o 802.11?

La principal confusión en los nombres surge de afirmar que el término WiFi (que no posee un significado en sí) proviene de *Wireless Fidelity*. En el año 1999, las empresas Nokia y Symbol Technologies crearon una asociación llamada Alianza de Compatibilidad Ethernet Inalámbrica (WECA, *Wireless Ethernet Compatibility Alliance*), que, luego en 2003, se pasó a llamar Wi-Fi Alliance. Tenía como objetivo crear una marca que permitiese fomentar de manera fácil la nueva tecnología inalámbrica y asegurar la compatibilidad. La WECA necesitaba de un logo o emblema para identificar y recordar su estándar. Entonces, contrató a Interbrand, una empresa de publicidad, para que le diera un nombre más llamativo que **IEEE 802.11b de Secuencia Directa.** Así nació el nombre **Wi-Fi** y el **Style Logo del Ying Yang**, que es una marca exclusiva para identificar los productos que cumplen los requerimientos de interoperabilidad entre dispositivos basados en el estándar IEEE 802.11, en otras palabras una red WiFi es una red que cumple y se basa en los estándares IEEE 802.11 recomendados.

> NUESTRO ESTÁNDAR IEEE 802.11 POSEE UNA TECNOLOGÍA CLAVE QUE ES EL DSSS



Figura 31. Podemos encontrar en cualquier café o espacio en nuestra ciudad el famoso logo de WiFi creado por la Wi-Fi Alliance.

También es común encontrar el termino 802.11x, que se usa para referirse a todo el grupo de estándares (donde x puede ser b, a, g, etc.).



Figura 32. La Wi-Fi Alliance garantiza la interoperabilidad entre productos certificados. con los logos que vemos en la imagen.

Características técnicas de la IEEE 802.11

Se partió de la norma original IEEE 802.11 y se desarrollaron varias reformas donde se contemplaron las técnicas de modulación, las frecuencias usadas y la calidad de servicio (*Quality of service*, o **QoS**, por sus siglas en inglés).

Las diferentes técnicas de modulación influyen en la transferencia de datos de un punto a otro. La **modulación** de los datos es la forma en que estos se acomodan en un medio (en nuestro caso el aire o espectro radioeléctrico) para ser transmitidos. Si codificamos de forma eficiente los datos (es decir, usamos alguna técnica que represente nuestros datos y así nos ocupe menos ancho de banda), lograremos mejores tasas de transferencia de información, pero también requeriremos hardware más sofisticado.

CONFUSIÓN DE NOMBRES

No solo es común confundir el término WiFi. Se da otra confusión con Wireless LAN o WLAN que es usado como el nombre para redes de área local inalámbrica, en las que se usan ondas de radio para comunicarse entre usuarios conectados. De esta forma Wireless LAN es un nombre alternativo del estándar IEEE 802.11 y no un producto diferente.

Podemos identificar tres técnicas principales de modulación:

• **FHSS**: espectro esparcido por salto de frecuencia. Esta modulación no es la más común actualmente.

• **DSSS**: espectro esparcido por secuencia directa. Esta técnica se utilizó entre los años 1999 y 2005.

• **OFDM**: modulación por división de frecuencias ortogonales. Esta técnica de modulación se utiliza desde 2005.

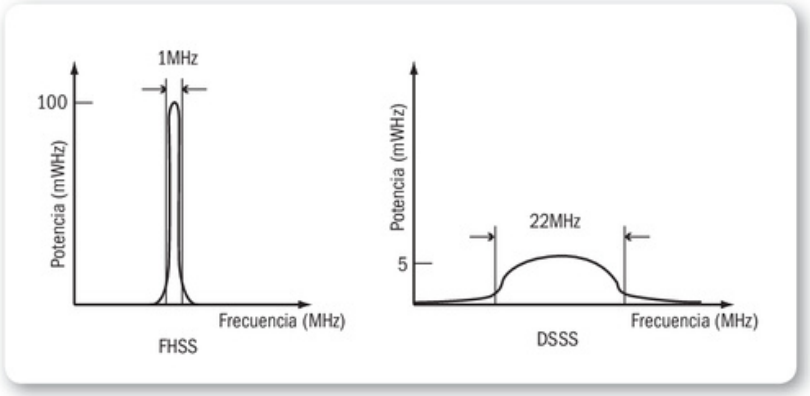


Figura 33. FHSS concentra toda la potencia de emisión en una franja estrecha del espectro y **DSSS** lo hace en un rango mayor.

Si hablamos de **Frecuencia**, vemos que los estándares 802.11b y 802.11g usan la banda de 2.4 GHz, mientras que el 802.11a lo hace en los 5 GHz. La primera banda es llamada ISM y la de 5 GHz, UNII. Al no poseer licencia, la banda de 2.4 GHz se volvió bastante ruidosa y llena de interferencias, ya que otros dispositivos también la utilizan. Así, encontramos que la banda de 5 GHz tiene menos interferencia pero tenemos otros problemas debido a su naturaleza, como ser muy sensible a la absorción. Entonces, la señal se atenúa con el agua, los edificios cercanos u otros objetos porque existe una alta absorción de la señal en este rango. Deducimos así que necesitaremos mayor cantidad de puntos de acceso para cubrir la misma área que en una red 802.11b.

Mejoras de la IEEE 802.11

Muchas reformas fueron realizadas desde la original IEEE 802.11 que define nuestras redes inalámbricas, veremos de forma 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 este estándar se mejoró, en comparación con el estándar original, la tasa de transmisión de datos, se la elevó hasta 11 Mbit/s (se lee mega bits por segundo), lo que significa una gran mejoría.

Como dato extra, podemos decir que inicialmente se soportan 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 nombramos la incompatibilidad con 802.11b, ya que opera en diferente frecuencia.

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.



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 esta forma, cuando utilizamos tasas de 2 Mbit/s y 1 Mbit/s tendremos menor probabilidad de sufrir interferencias o pérdidas de datos. No debemos confundir la tasa de transmisión con otros conceptos como el ancho de banda de nuestra conexión.

Tenemos las mismas capacidades que el 802.11b y sumamos el incremento de la velocidad. De esta forma los estándares 802.11b y 802.11g difieren muy poco.

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 sus propios protocolos para la autoconfiguración de rutas entre AP. Esto extiende el estandar IEEE 802.11 con un protocolo y arquitectura totalmente nuevos.

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. Este concepto es llamado MIMO (*Multiple Input, Multiple Output*) y aumenta la tasa de transferencia de datos y el alcance. Lo notables es que MIMO aprovecha lo que otros estándares consideran un obstáculo: la **multitrayectoria**.

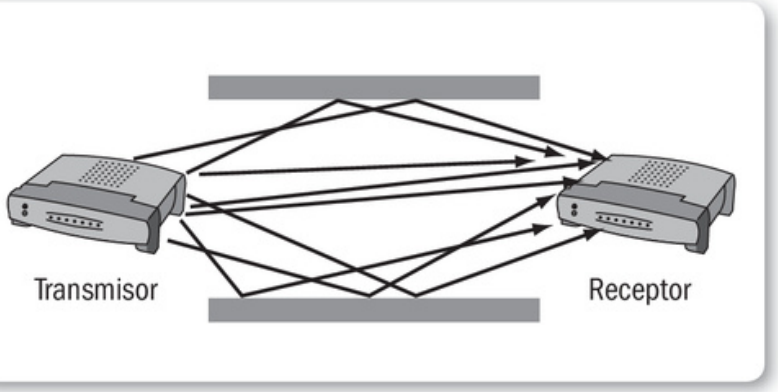


Figura 34. El concepto de la tecnología **MIMO** es aprovechar las señales que recorren otro trayecto sin tratarlas como ruido.



Figura 35. Equipo que trabaja con el estándar **802.11n** disponible en el mercado.

Para tratar de resumir lo que vimos anteriormente, haremos una comparación entre las 4 reformas más importantes del 802.11 y luego un resumen de los estándares sobresalientes. Vamos a considerar según el nombre del estándar, su frecuencia, la técnica de modulación utilizada, la tasa de transmisión y el área de cobertura (siempre dentro de un recinto cerrado).

APPLE Y SU WIFI

La empresa **Apple** desarrolló un producto llamado **AirPort** para utilizar la tecnología WiFi. La norma 802.11b se utiliza en los llamados AirPort, mientras que 802.11g para los **AirPort Extreme**. Una solución más simple y compacta es el **AirPort Express** que permite a los usuarios de **Mac** conectarse a una red. Obviamente, ambos estándares son exclusivos de los sistemas Mac. Airport fue presentado por primera vez el 21 de Julio de 1999 en la expo MacWorld de Nueva York. No en todo el mundo tiene el mismo nombre, por ejemplo, en Japón, AirPort está bautizado con el nombre AirMac.



Figura 36. Las placas inalámbricas internas también hacen uso de la tecnología **MIMO** en 802.11n.

No debemos olvidar que la zona donde tendremos señal inalámbrica es siempre limitada.

TABLA 5

ESTÁNDAR	FRECUENCIA	TÉCNICA DE MODULACION	TASA DE TRANSMISIÓN	ÁREA DE COBERTURA (INTERNO)
802.11a	5 Ghz	OFDM	54 Mbit/s	50 metros aproximadamente
802.11b	2.4 GHz	DSSS, CCK	11 Mbit/s	100 metros aproximadamente
802.11g	2.4 GHz	OFDM, CCK, DSSS	54 Mbit/s	100 metros aproximadamente
802.11n	2.4 y 5 GHz	OFDM	540 Mbit/s	250 metros aproximadamente

Tabla 6. La tabla muestra que el área de cobertura no supera los 300 metros para las diferentes enmiendas por ahora.

En la tabla que se encuentra a continuación tenemos un resumen de cada uno de los estándares IEEE 802.11 con sus principales mejoras o cambios dictados por la IEEE.

TABLA 6



ESTÁNDAR	DESCRIPCIÓN
802.11	El original, tasas de 1 y 2 Mbit/s en 2.4GHz. Estándar de RF e IR (1999)
802.11a	54 Mbit/s, en 5 GHz (1999, los productos salen en 2001)
802.11b	Mejoras en 802.11 para soportar 5.5 y 11 Mbit/s (1999)
802.11c	Procedimientos en operación Puente, incluido en 802.11d (2001)
802.11d	Extensión del roaming internacional (país a país) (2001)
802.11e	Mejoras en Calidad de Servicio (QoS) (2005)
802.11f	Protocolo Inter-Access Point (2003)
802.11g	54 Mbit/s, en 2.4 GHz. Compatible para atrás con b. (2003)
802.11h	Manejo del espectro 802.11a (5 GHz) para compatibilidad en Europa
802.11i	Mejora en seguridad (2004)
802.11j	Extensión para Japón (2004)
802.11k	Mejoras en la medición de recursos de radio (2007)
802.11l	(Reservada y no disponible para el uso)
802.11m	Mantenimiento del estándar
802.11n	Incremento de la tasa usando MIMO (2009)
802.11o	(Reservada y no disponible para el uso)
802.11p	WAVE (acceso inalámbrico para el automóvil) Intercambio de datos entre vehículos
802.11q	(Reservada y no disponible para el uso)
802.11r	Fast roaming Working. Permite que el cambio de AP sea rápido. Importante en VoIP
802.11s	ESS Protocolo para redes Malla o Mesh
802.11T	WPP (Wireless Performance Prediction)
802.11u	Interoperabilidad con redes no 802 (por ejemplo, redes celulares)
802.11v	Configuración remota de dispositivos cliente

▼ ESTÁNDAR	▼ DESCRIPCIÓN
802.11w	Protección para redes a causa de sistemas externos
802.11x	(Reservada y no disponible para el uso)
802.11y	Operación en banda de 3650 a 3700 MHz en USA

Tabla 7. Vemos en la tabla que existen muchos estándares que están reservados, en general, para uso científico o militar.



RESUMEN

En conclusión, existen diferentes topologías de red 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 como 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	Enumere las topologías físicas y nombre la que se forma de la combinación de Bus con Estrella.
4	¿Cuál es la topología inalámbrica más usada?
5	¿A qué tipo de red llamamos WLAN y en qué banda opera?
6	¿Qué consecuencia sufren los datos cuando las comunicaciones tienen interferencias en las frecuencias de uso libre?
7	¿Qué significa el termino SSID y para qué sirve?
8	¿Cuáles son los dos modos fundamentales de operación en los estándares 802.11?
9	¿Cuál es la diferencia entre estándar abierto y cerrado? Nombre ejemplos.
10	¿En qué banda funciona IEEE 802.11g y cuál modulación utiliza?
11	¿Qué elemento de una red inalámbrica se puede encontrar en universidades, aeropuertos o espacios públicos y usa la configuración de Estrella?
12	¿Cuándo se recomienda el uso de repetidores en los enlaces PtP?
13	¿De qué manera podemos identificar los productos que cumplen y se basan en los estándares IEEE 802.11?
14	¿Qué logramos realizando una codificación de los datos eficiente en IEEE 802.11?
15	¿Por qué razón IEEE 802.11a es incompatible con IEEE 802.11b?

*02

Hardware para redes inalámbricas

Veremos 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, aprenderemos cómo configurar los puntos de acceso. Entre otros temas, analizaremos parámetros como el SSID, la velocidad de transmisión y la potencia de transmisión, vinculados a la capa física.

- **Introducción al hardware inalámbrico 62**
- **Configuración de puntos de acceso 65**
  - Pautas generales a tener en cuenta 65
  - Instalar el hardware y actualizarlo 67
- **Configurar con el modelo OSI. 84**
  - Capa física 85
  - Capa de enlace 90
  - Capa de red 97
  - Capa de aplicación 98
- **Resumen 99**
- **Actividades 100**

Introducción al hardware inalámbrico

Albert Einstein dijo: "**El telégrafo inalámbrico** no es difícil de entender. El telégrafo es como un gato muy muy largo. Tiras de su cola en New York y su cabeza maúlla en Los Ángeles. ¿Lo entiendes? Bueno la radio trabaja exactamente de la misma manera: tú envías señales aquí, ellos las reciben allá. La diferencia es que no hay gato". Esta analogía nos deja comprender la manera en que la información viaja de un sitio a otro sin elementos físicos visibles.

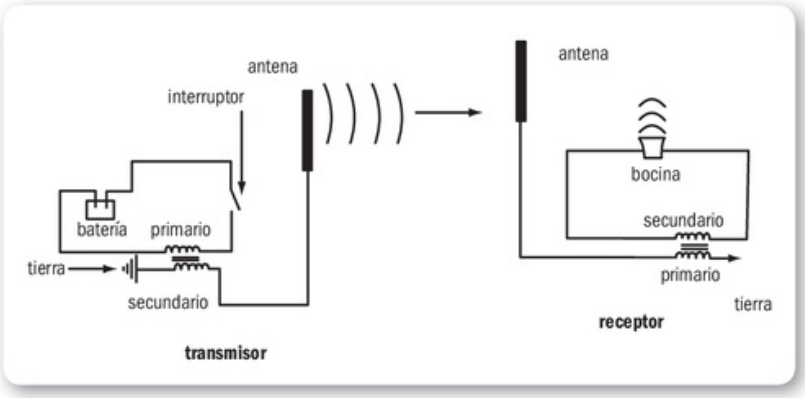


Figura 1. El esquema muestra cómo está conformado el telégrafo inalámbrico.

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, **radio AM**

CODIGO MORSE

Inventado por **Samuel Morse** y en uso desde **1838**, fue el sistema para transmitir mensajes que hizo realidad las telecomunicaciones. En una época fue el código de comunicación más importante, aunque hoy su uso se ha restringido a las bandas de frecuencia que usan los radioaficionados, ya que es un código muy robusto para transmitir mensajes aunque existan malas condiciones atmosféricas.

y **FM**, antenas de televisión satelital, entre otros. En todos ellos un transceptor, que se pueder ser definido 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.

Básicamente necesitamos de dos partes de hardware para conformar cualquier red inalámbrica: un punto de acceso y un adaptador de red.



Figura 2. Un router inalámbrico que no realiza modificaciones en la información enviada funciona como punto de acceso para nuestra red.

Es muy común encontrar dispositivos, los cuales podemos comprar en cualquier comercio, que cumplen las tareas de un Access Point. Estos dispositivos suelen ser externos e independientes de nuestra PC. Por otro lado, tenemos las placas de red inalámbricas, que, por lo general, están instaladas dentro de la PC (en el caso de las PCs de escritorio); en notebooks o similares, donde no es posible agregar hardware de forma interna, se utilizan los USB.

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.

Hablaremos de estas dos configuraciones que ya vinimos anticipando en el capítulo anterior.

En muchos textos que actualmente existen sobre esta tecnología, los autores se centran en decirnos el botón que se debe presionar.

Nosotros, por el contrario, deseamos que el lector pueda comprender lo que implica cada una de las opciones disponibles y por qué se necesita esa configuración específica.

De lo visto en el capítulo anterior vamos a hacer uso de las capas de enlace y física del modelo OSI para nuestra explicación.



Figura 3. Los usuarios que desean utilizar nuestra red inalámbrica deben contar con un adaptador de red en su computadora.

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

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

Estos pasos se aplican para cualquier sistema operativo con el que trabajemos. En nuestro caso usaremos MS Windows 7, así es que no

COMIENZOS DE LA TELECOMUNICACIÓN

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, que es la transmisión a larga distancia de mensajes escritos.

tendremos mayores problemas en los pasos 1 y 2 (lo mismo sucederá con cualquier versión de MS Windows). Si el sistema operativo fuese Linux (OpenSource o diferente a MS Windows) no es tan sencillo, estos dos primeros pasos requerirán mucha atención.

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 forma, si fuese necesario verificar algún paso por motivo de un error o problema sería algo muy fácil de realizar.

Pautas generales a 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, la humedad del ambiente, entre otros factores.

• Hacer un dibujo de la red (TCP/IP), el cual servirá como un plano con las indicaciones a seguir. Con esto lograremos identificar la topología usada en nuestra red. Debemos incluir la mayor cantidad

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 PC olvidada. Para los que estén interesados pueden leer más en **www.zeroshell.net**.

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 específico posible, recomendamos utilizar gráficos o esquemas que ayuden a la comprensión.

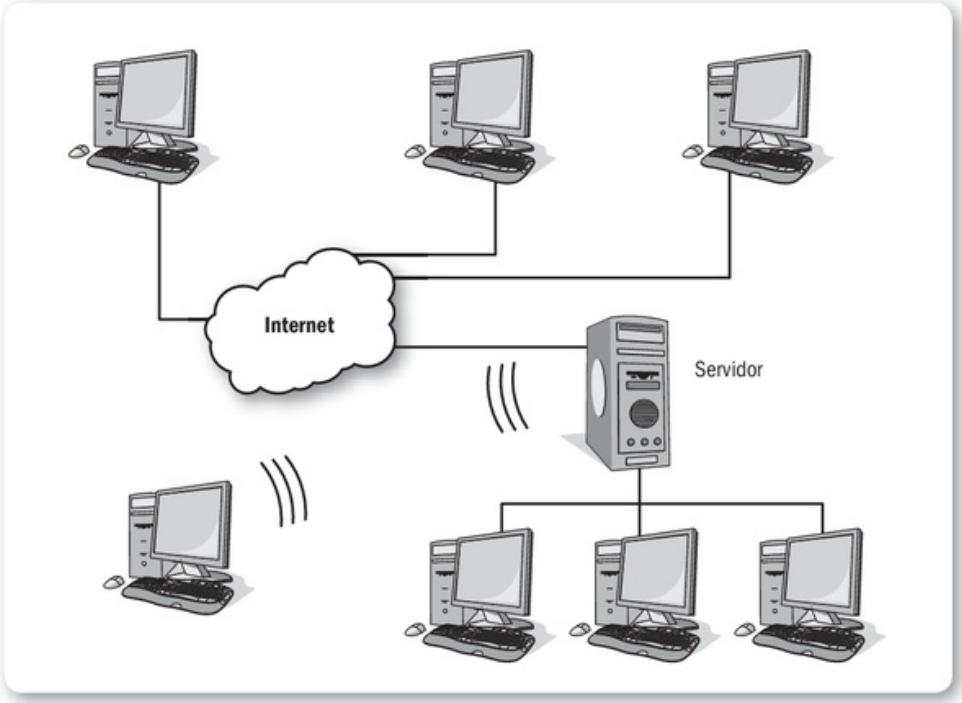


Figura 4. Tener nuestro diagrama de red nos permite hacer cambios de última hora antes de iniciar las configuraciones.

• Si estamos consultando material en alguna página web, es importante bajarlo para tenerlo en caso de que nuestra conexión sufra algún problema. Descarguemos todo así podemos trabajar aun sin tener conexión a Internet.

• Recomendamos tener papel y lápiz a mano para tomar nota de cada paso que realicemos, esto va a ser muy útil cuando tengamos que cambiar direcciones IP, contraseñas, opciones de red, etc.

• Siempre debemos verificar que tengamos todo el hardware que vamos a utilizar para componer nuestra red (PC, tarjeta de red, cables de red en caso de ser necesario, etc.).

• 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 nuestra tarea instalando la parte física de la red, el hardware. Vamos a conectar el punto de acceso a nuestra computadora (de escritorio o portátil) y actualizaremos el **firmware** (esto es opcional). Tal vez nos suene esta última palabra, en un principio el firmware existía en el límite entre el hardware y el software (el término hace referencia a la programación firme, 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 se ejecuta desde la memoria del dispositivo. Este software está integrado en la parte del hardware, es decir que viene dentro del dispositivo, así podemos proponer, desde nuestro punto de vista, que el firmware es hardware y software al mismo tiempo.

> INICIAMOS NUESTRA TAREA INSTALANDO LA PARTE FÍSICA DE LA RED, EL HARDWARE

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.



Figura 5. Algunas distribuciones de firmware creadas por terceros nos permiten tener un mayor número de opciones de configuración.

Instalar el dispositivo físicamente

Para 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 del disposito que nos indican el estado.
2. Las interfaces de conexión Ethernet e inalámbrica.



Figura 6. Si hay algún problema, lo primero que verificaremos será el estado de los LEDs del punto de acceso.

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 verde) algunos de los siguientes parámetros:

1. Alimentación 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.

Estos LEDs nos proporcionan información muy útil a la hora de diagnosticar o encontrar los problemas que puedan aparecer en la red. Recomendamos leer el manual de cada dispositivo para tener pleno conocimiento del significado de cada luz (en sus diferentes estados) antes de empezar a configurar.

Nuestro punto de acceso cuenta con interfaces de conexión, estas son:

• **Ethernet**: también llamada WAN, esta interfaz hace referencia a que el dispositivo se conecta a una red de área amplia como Internet o

LAN. Diferenciamos a los puntos de acceso por la cantidad de puertos Ethernet que poseen, así si solo tenemos un puerto Ethernet decimos que es un punto de acceso **transparente** (puente inalámbrico), pero si contamos con más de un puerto Ethernet entonces es un gateway (enrutador/pasarela) inalámbrico.

• **Antenas**: nos permiten realizar un vínculo, sin necesidad de cables, entre nuestro dispositivo y el de los clientes.

> DEBEMOS PRESTAR ATENCIÓN A DOS PARTES BIEN DIFERENCIADAS EN UN PUNTO DE ACCESO

Algunos dispositivos inalámbricos nuevos en el mercado vienen con más de una interface inalámbrica (dos o más antenas).

Si miramos la parte de atrás veremos que en la mayoría de los productos que tenemos en el mercado encontramos:

1. Entrada para conectar alimentación de 12 V, 5 V o 3,5 V DC: acá enchufamos la fuente que viene con el equipo.
2. **Botón de reset**: al presionarlo volvemos a la configuración por defecto que trae de fábrica.
3. **Bocas LAN** (para conectores RJ45): son para conectarnos a una red LAN proponer, desde nuestro punto de vista,
4. **Puerto WAN** (para conectores RJ45): nos permite conectar el cablemódem o cualquier otra interfaz que use nuestro proveedor de Internet para conexión de red de área amplia.



Figura 7. 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. Si tenemos antenas externas vamos a poder moverlas para así orientarlas según nuestra necesidad para que la recepción sea óptima.

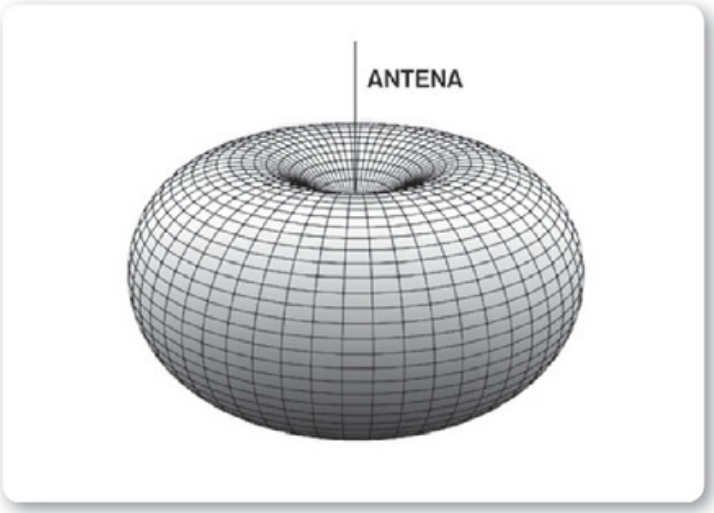


Figura 8. El diagrama de radiación de una antena es una representación de la energía radiada por la antena junto con su dirección.

Actualizar el firmware

Como describimos anteriormente, el **firmware** (también llamado **microcódigo**) es un software que se escribió dentro de la memoria de solo lectura no volátil o ROM (acrónimo en inglés de *read only memory*) y por lo tanto es algo que permanece en el dispositivo aunque este se haya apagado.

Si deseamos modificarlo, debemos seguir un procedimiento especial teniendo extremo cuidado, ya que si existe alguna interrupción (corte de luz, comunicación entre computadoras o

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 mejor ancho de banda.

similar) se puede causar un daño irreparable al dispositivo que es actualizado. En general, todos los fabricantes ponen a disposición de los usuarios actualizaciones de firmware para sus productos. Esto lo realizan constantemente para que de esta forma los usuarios puedan tener nuevas configuraciones y solucionar los problemas que se reportan por otros usuarios del producto.

Recomendamos que, siempre que sea posible, se actualice el punto de acceso con la última versión de firmware "estable" (significa que el fabricante nos garantiza que todo el código funciona correctamente) antes de empezar a configurarlo y luego debemos estar atentos ante posibles nuevas actualizaciones de firmware (podemos consultar el sitio web del fabricante para buscarlas).

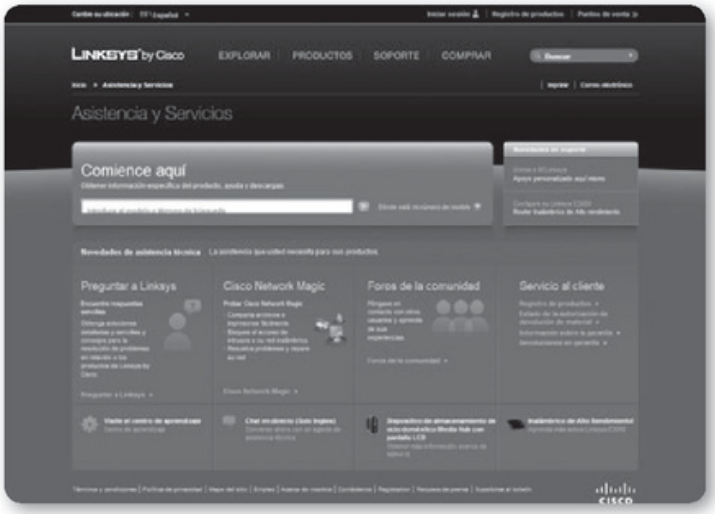


Figura 9. Dentro del sitio web del fabricante podemos encontrar ayuda y soporte para solucionar problemas comunes de nuestros dispositivos.

Veremos, tomando como ejemplo el router Linksys modelo WRT160N, los pasos necesarios para actualizar nuestro firmware y así tener el dispositivo al día.

- Bajar el nuevo firmware desde el sitio oficial.
- Realizar una copia de seguridad de la configuración actual de nuestro router (esto incluye las opciones configuradas por defecto o por nosotros en el dispositivo utilizado).
- Actualizar el firmware.
- Finalizar la actualización del firmware.
- Restaurar la configuración del router.
- Completar el proceso de actualización del firmware.



Figura 10. El modelo **WRT160N** de Linksys es un router inalámbrico que soporta **IEEE 802.11n**.

Ahora veremos los pasos necesarios para actualizar el firmware.

ACTUALIZACIÓN FIRMWARE WRT160N

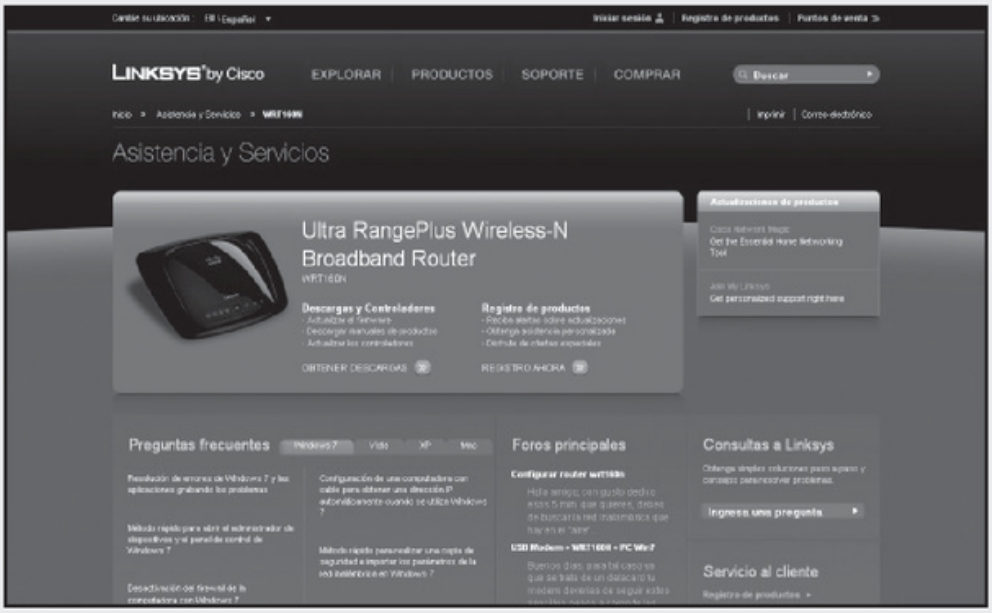
01 Verifique que su conexión a Internet funciona correctamente y si usa el router inalámbrico conectado a su computadora será mejor que lo desconecte y enchufe su computadora directamente a su **cablemódem** o **módem DSL** de su proveedor .



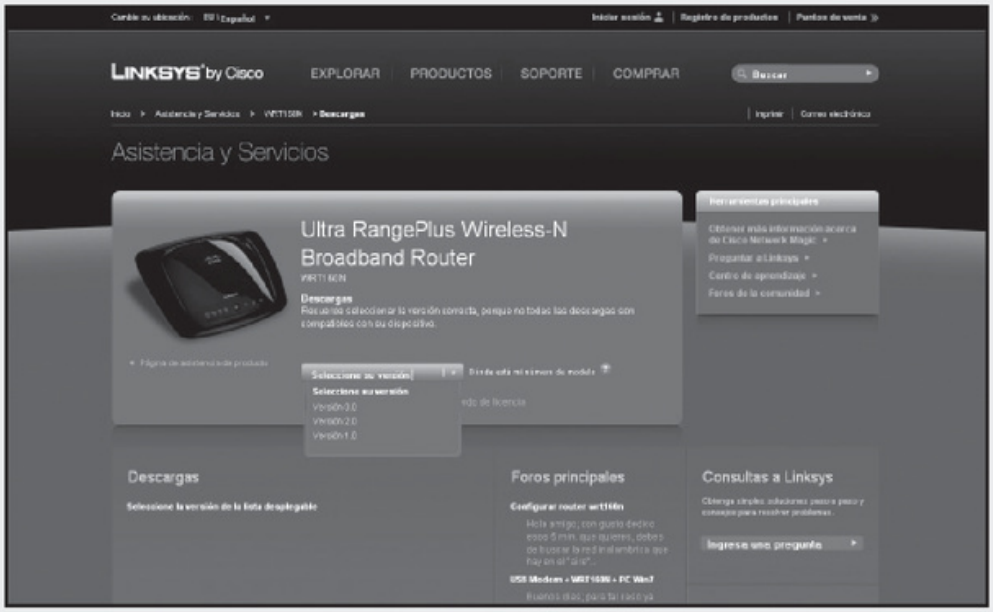
02 Para continuar, debe ingresar al sitio web oficial del fabricante (en nuestro ejemplo es **www.linksysbycisco.com**) y hacer clic en **Soporte** para ingresar su modelo de router (en nuestro caso es WRT160N).



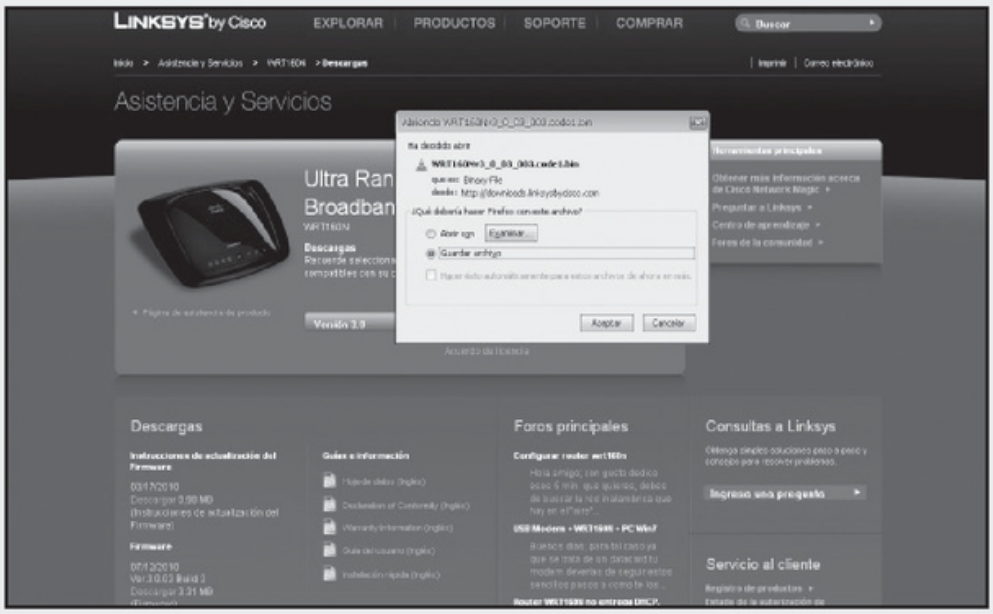
03 En el margen izquierdo podrá ingresar el modelo o término de búsqueda. Allí coloque el modelo del router: WRT160N y verá la siguiente pantalla.



04 Haga clic en OBTENER DESCARGAS y seleccione su versión de router inalámbrico en el menú desplegable (si no conoce cuál es su versión, haga clic en el signo de pregunta que está al lado del texto "Dónde está mi número de modelo" para averiguarlo).



05 Abajo a la izquierda tendrá la sección Descargas. Haga clic en `Descargar` (resaltado en color) para bajar su versión de firmware. Presione `Guardar` en el cuadro de diálogo que aparece. Cuando se complete la descarga haga clic en `Cerrar`. Nota: tenga en cuenta que el nombre del archivo descargado puede variar.



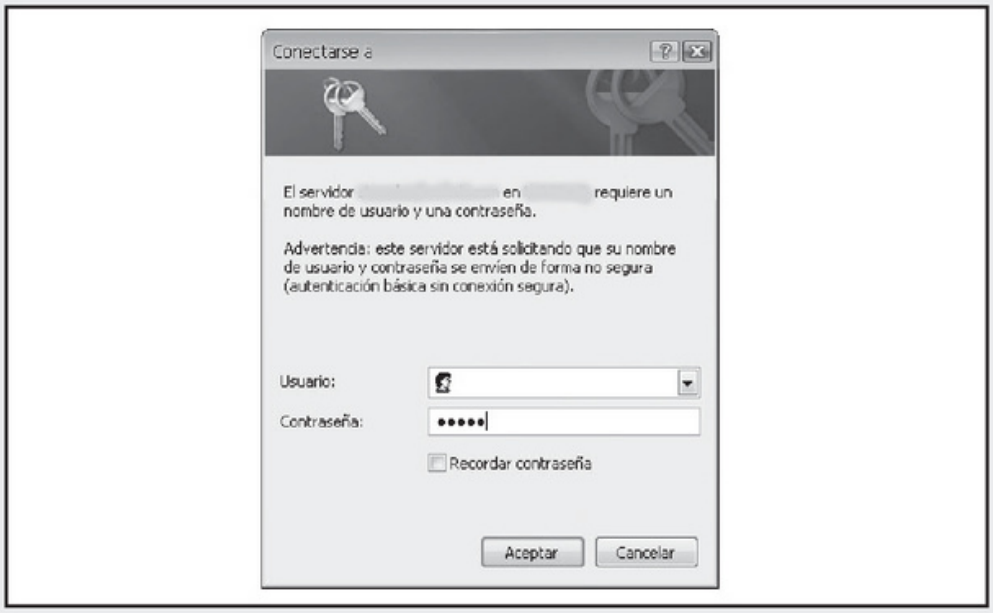
06 Si el archivo que usted bajó está en formato ZIP, haga doble clic en él y extraiga el contenido en una carpeta situada en el Escritorio de Windows. Nota: necesitará un programa para abrir y extraer los archivos contenidos en el archivo ZIP. Puede usar el popular **WinZip**, ingrese en **www.winzip.com** para bajarlo.



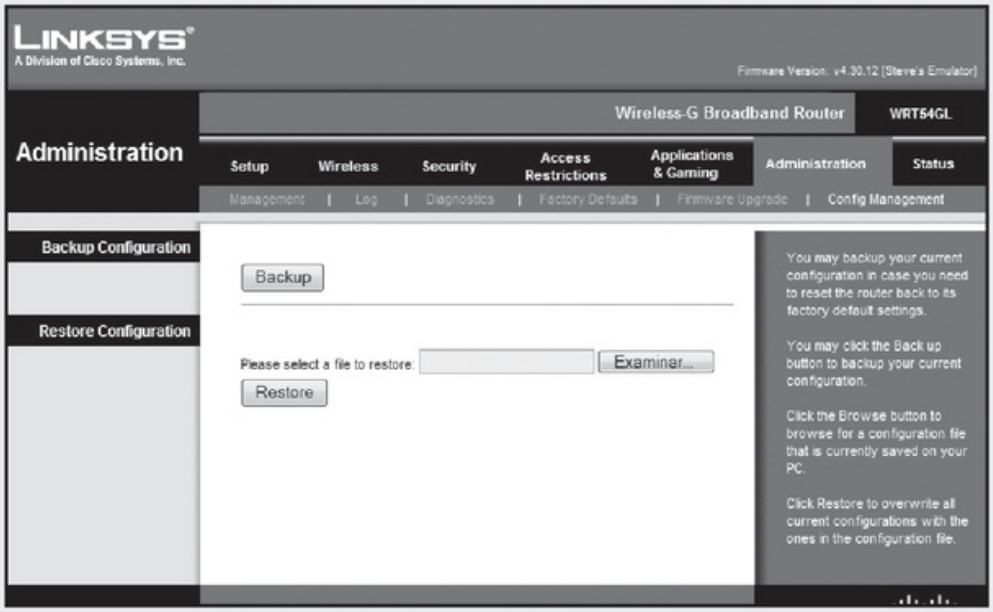
07 Realice una copia de seguridad de la configuración actual, para hacerlo verifique que el router esté encendido y conecte su computadora a uno de los puertos Ethernet en el router (1, 2,3 o 4) con el cable provisto (cable UTP).



08 Abra su navegador, por ejemplo Internet Explorer, e ingrese la dirección IP del router (por defecto la IP en la mayoría de los routers es 192.168.1.1) y luego presione Enter. Una ventana de diálogo preguntará por el usuario y la contraseña para ingresar a la configuración del router. Deje el nombre de usuario en blanco e ingrese su contraseña (por defecto, la contraseña que viene de fabrica es admin). Luego presione Aceptar.



09 Cuando la página de configuración del router aparezca, haga clic en Administration y luego en Config Managment del menú superior.



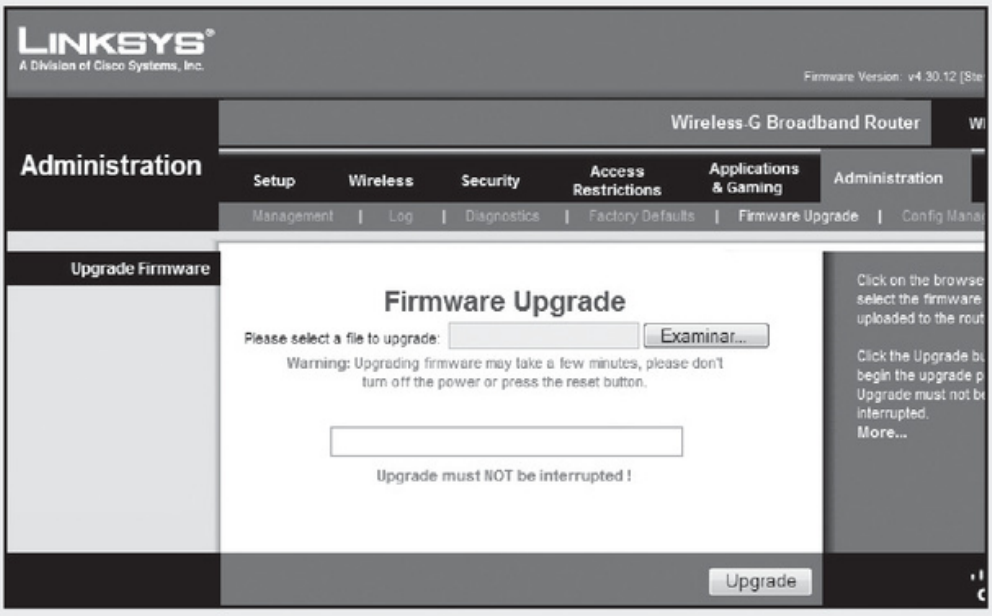
10

Una vez dentro de Config Management, mire en la sección Backup Configuration y haga clic en Backup. Presione Guardar en el cuadro de diálogo que aparece. Cuando se complete la descarga haga clic en Cerrar.

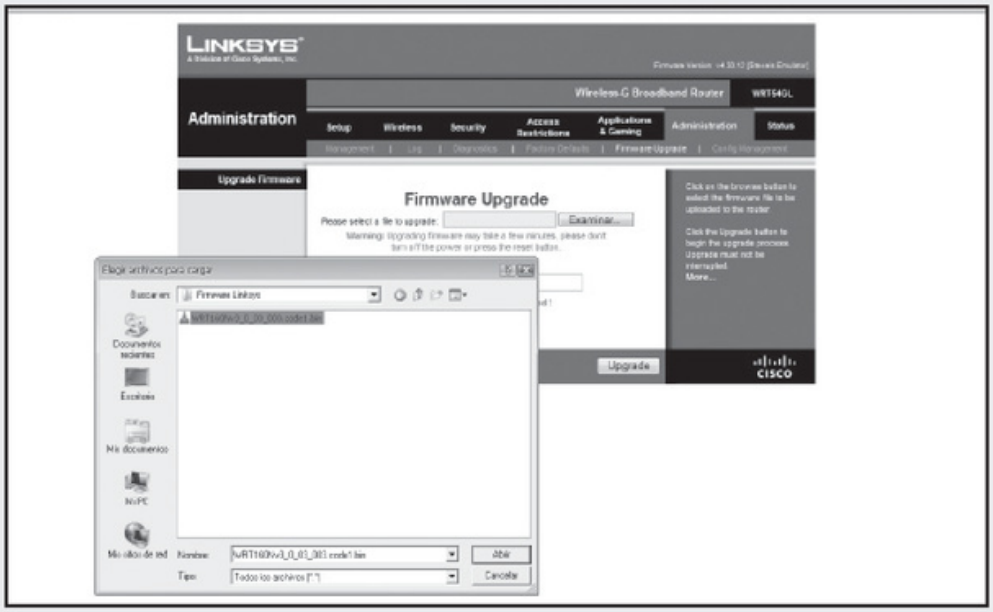


11

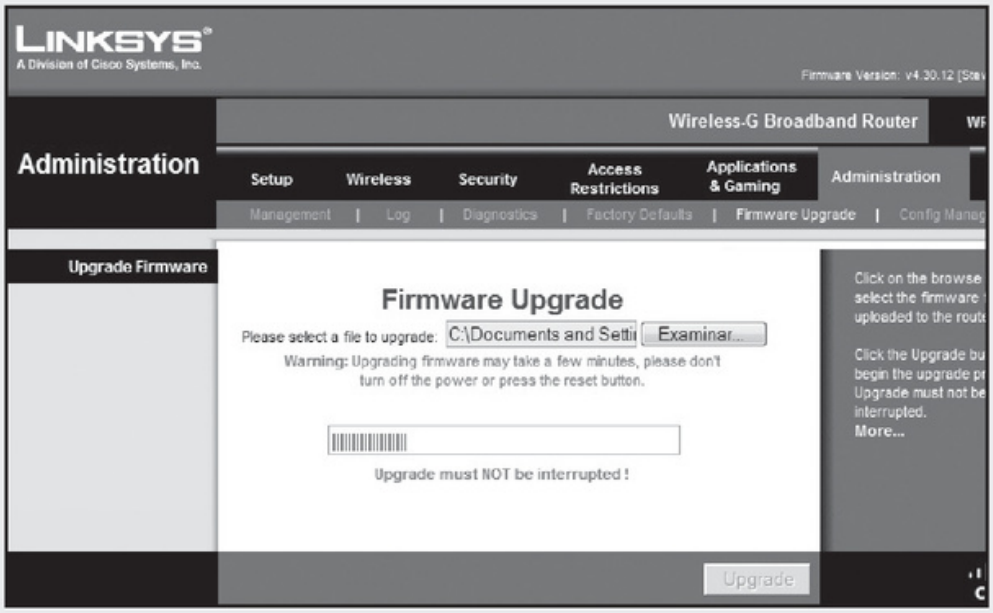
Una vez que completó la copia de seguridad de las configuraciones del router, realice la actualización del firmware. Vuelva a la página de administración haciendo clic en Administration en el menú superior para luego hacer clic en Firmware Upgrade.



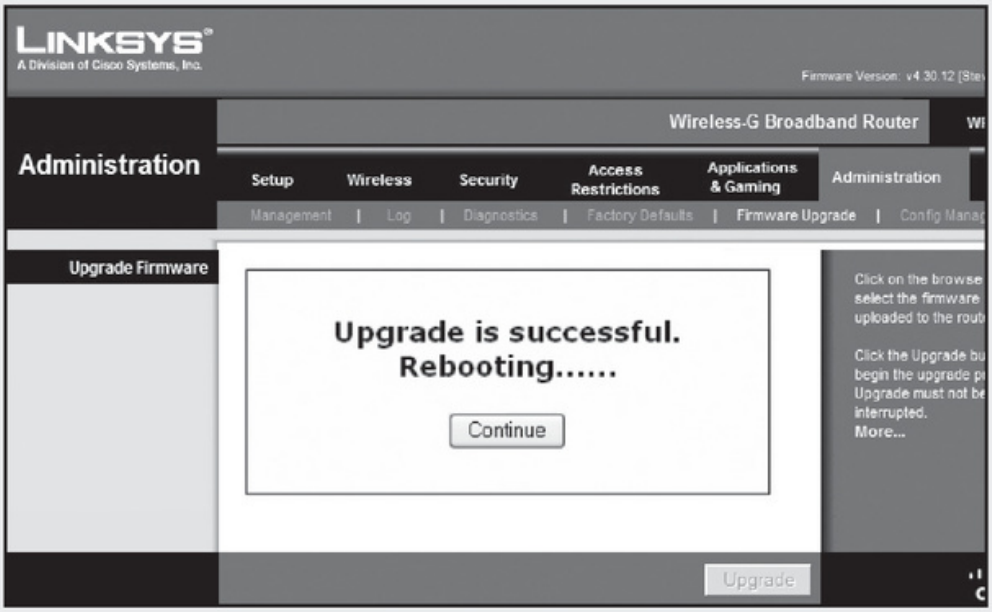
12 Para continuar, debe hacer clic en `Examinar` para buscar el archivo que descargó y descomprimió con extensión `.BIN`, que tiene todo lo necesario para actualizar el firmware de su router inalámbrico.



13 Presione `Upgrade` y la actualización comenzará. Una barra de estado mostrará el progreso, como se ve en la figura siguiente.



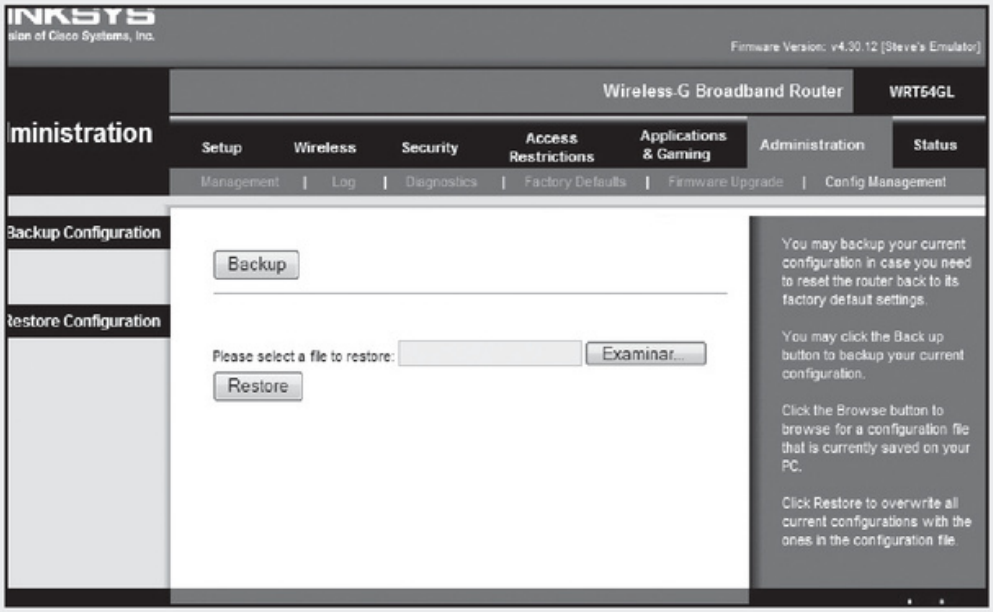
14 Si la actualización finalizó con éxito se mostrará el siguiente mensaje. Presione `Continue` para finalizar el proceso.



15 Complete la actualización del firmware cerrando Internet Explorer y realice un `reseteo` del router. Puede encontrar el botón de reset a la derecha de los puertos ethernet. También puede consultar su manual de usuario que especifica dónde se encuentra el botón de reset, en caso de poseer otro modelo de router.



16 Luego de resetear el router, deberá restaurar las configuraciones del router de la siguiente manera. Ingrese a la página de configuración del router como lo hizo en el punto 7, presione en `Administration` y luego `Config Management`. En la sección `Restore Configuration`, haga clic en `Examinar` para buscar su archivo de configuración previamente guardado.



17 Presione `Restore` para iniciar el proceso de restauración de la configuración en su router y así concluir son la actualización del firmware.

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 nuestra red. Se puede realizar este vínculo usando una conexión por cable o de forma inalámbrica. Para realizar 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 nuestra red configurados, cambiar y usar la conexión inalámbrica para administrar o modificar configuraciones de la red. La conexión por cable puede hacerse con:

1. Cable Ethernet que usa el protocolo utilizado en la Web (HTTP).

2. Cable Ethernet pero que usa un programa específico provisto por algunos fabricantes y que se basa en el protocolo SNMP (protocolo simple de administración de red).

3. Puerto Serie, en caso de que el dispositivo cuente con uno. Se usa algún software de comunicación serial como HyperTerminal de MS Windows que se se puede bajar de Internet.

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 11. El cable Ethernet usado para conectarnos se llama patch cord y consta de un cable UTP y conectores RJ45.

El cable de red, también llamado **patch cord** en general es de unos 3 metros de largo o un poco menos también.

FIRMWARE EN TODOS LADOS

El firmware evolucionó para poder estar presente en cualquier dispositivo con el cual interactuemos. Por ejemplo, en muchos modelos de automóviles se emplean computadoras a bordo y sensores para detectar problemas, así como control de los sistemas antibloqueo de frenos y lecturas de combustible, presión de neumáticos, etc. Esto ocurre desde 1996 aproximadamente y se hace presente hoy en día con muy fuerte énfasis en toda la industria, ya sea automotriz o dedicada a otro rubro, como puede ser la dedicada a los electrodomésticos.

Los cables de conexíon que no son patch cords resultan un poco más difíciles de conseguir en el mercado.



Figura 12. Si nuestro dispositivo permite conexión serie, usaremos un cable que tiene en un extremo una ficha RJ-45 y en el otro, uno o dos DB9 o B25.

Una vez que ingresemos a la configuración del punto de acceso desde el navegador, veremos la interfaz de usuario. Si bien las interfaces no son idénticas, varían según fabricantes y modelos, son similares. Esto permite reconocer elementos básicos a la hora de configurar nuestro dispositivo.

Debemos tener especial cuidado cuando vemos estas interfaces, ya que no todos los fabricantes hacen referencia a los mismos conceptos con las mismas palabras. Podemos pensar en los siguientes conceptos básicos para lograr comunicarnos con el punto de acceso:

- El cliente debe pertenecer a la misma subred IP. Esto significa que si nuestro número IP perteneciente a la computadora desde donde nos conectamos tiene el número 192.168.1.10, en general la subred se identifica como 192.168.0.X (donde X puede valer entre 1 y 254).
- Verificar en el manual del dispositivo la dirección IP por defecto del punto de acceso. Debemos modificar nuestra dirección IP según la IP del punto de acceso. Por ejemplo, si por defecto la IP del punto de acceso es 192.168.1.1 (en general siempre viene esta) y nuestra computadora tiene 192.168.1.10 entonces estamos en la misma subred y no necesitamos modificar nada.
- Si fuese necesario, debemos cambiar la dirección IP de nuestra computadora como corresponda.

• Como paso final, debemos abrir el navegador web e introducir la dirección IP del punto de acceso por defecto (192.168.1.1), podremos realizar la configuración desde la interfaz web. Debemos tener especial atención si se nos pide un usuario y contraseña, estos figuran en el manual del dispositivo.



Figura 13. La interfaz de los dispositivos D-Link que tenemos al usar el protocolo HTTP muestra un menú prolijo y posee ayudas para el usuario.

Cuando nombramos la posibilidad de configurar los dispositivos usando el protocolo SNMP estábamos haciendo referencia a utilidades o programas que desarrolla el propio fabricante y pone a disposición nuestra (también llamadas **utilidades propietarias**). No veremos ninguna de estas utilidades, ya que no se contemplan estos dispositivos en este libro.

Por último, si deseamos usar un cable serial, debemos considerar que será necesario tener acceso al lugar físico donde esté el dispositivo, ya que el cable serie se conecta en su parte posterior. Este método es el utilizado generalmente cuando necesitamos reconfigurar el punto de acceso y hemos olvidado la contraseña y no queremos restablecer la configuración de fábrica. En la gran mayoría de los casos podemos acceder al dispositivo usando el cable serial sin necesidad de la contraseña. No es común encontrar este conector en dispositivos hogareños por lo que no lo veremos en detalle y nos concentraremos en el acceso usando HTTP.

> EL CLIENTE DEBE PERTENECER A LA MISMA SUBRED IP



Figura 14. Podemos ver la parte de atrás del gabinete que se debe conectar al router .

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 en sus manuales). Por este motivo es común que nos asustemos ante tanta cantidad de opciones para configurar en un principio.

Si nuestro punto de acceso va a actuar como un puente inalámbrico que no realiza tareas de enrutamiento (esto significa que no provee de mecanismos como NAT, DHCP, entre otros que luego explicaremos), entonces solo será necesario verificar dos parámetros:

- SSID (*Service Set Identifier,* en español: Identificador de la red).
- Número de canal utilizado.

SSID INVISIBLE

Algunos puntos de acceso nos permiten desactivar el envío del SSID para así ocultar la red al público, lo que permite incrementar la seguridad de la red inalámbrica. Debemos ser precavidos y usar otro mecanismo de seguridad extra, ya que un usuario con conocimientos avanzados puede monitorear y capturar datos de la red para encontrar el SSID oculto.

De todas formas también se recomienda configurar otros parámetros que se refieren a la seguridad y los permisos de acceso, ya que con estos evitaremos que intrusos ingresen a nuestra red sin tener nuestro consentimiento.

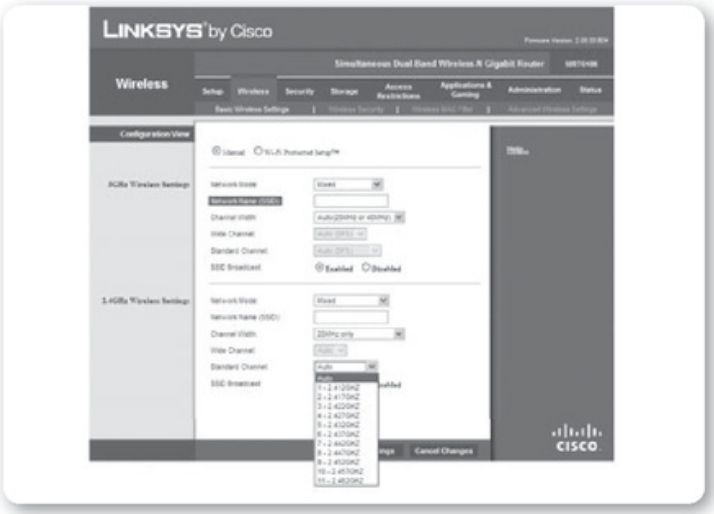


Figura 15. Dentro de las configuraciones básicas destacamos los parámetros SSID y el número del canal.

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 que tengamos plena seguridad al momento de implementar nuestra 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 estos para que podamos tener una idea general del concepto.

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 va a ser confeccionada nuestra red inalámbrica. Podemos realizar un escaneo de las frecuencias utilizadas por otras redes con algún software como Netstumbler (**www.netstumbler.com/downloads**) o inSSIDer (**www.metageek.net/products/inssider**), que nos permiten ver la información de otras redes inalámbricas y así evitar el uso del mismo canal en nuestra red. Esto reduce las posibilidades de interferencia en nuestra red inalámbrica.

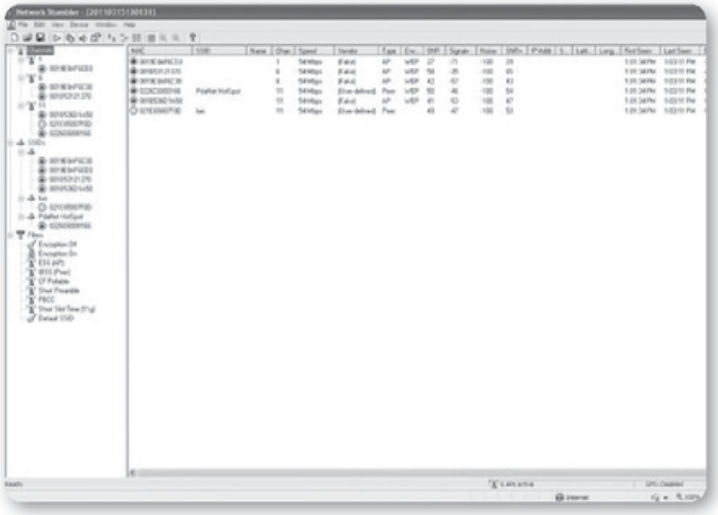


Figura 16. Netstumbler nos muestra de forma práctica los canales ocupados por redes y los respectivos SSIDs.

Netstumbler o inSSIDer ofrecen casi las mismas opciones.

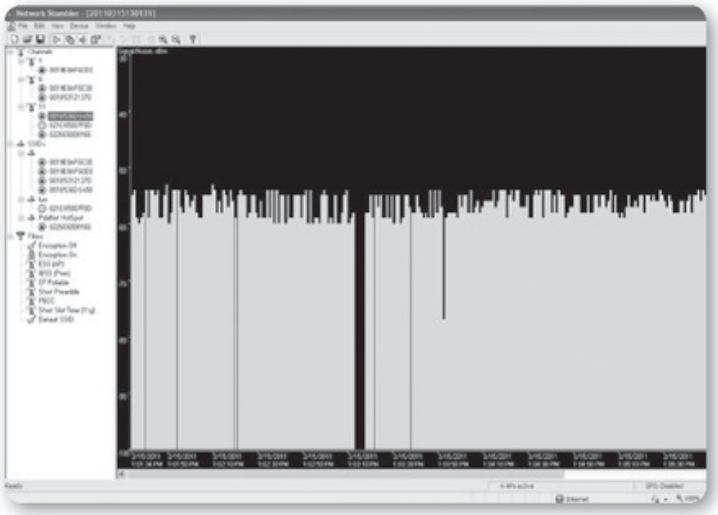


Figura 17. Al seleccionar un canal o SSID específico, Netstumbler nos muestra un gráfico del tráfico de datos en tiempo real.

Como información adicional a lo visto en el capítulo anterior, si usamos la norma IEEE 802.11b es recomendable utilzar 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 que nos convenga y esté disponible.

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 al que usamos nosotros.



Figura 18. Al momento de seleccionar el canal que vamos a utilizar, vemos que se especifica la frecuencia en GHz además del número de canal.

Es muy común encontrar que ciertos productos nuevos en el mercado poseen la opción de "auto" en estas configuraciones de canal. Si seleccionamos esta opción, se seleccionará una frecuencia de forma automática según el resultado de un escaneo del espectro realizado por el mismo dispositivo. De esta forma se detectan las frecuencias más congestionadas y, este modo de configuración automática, las evita.

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 nuestra 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 ciertos lugares este valor es 100 mW (20 dBm) y en otros, como EE.UU. o Canadá, el límite es 1 W. De todas maneras no deberíamos hacer uso abusivo de este parámetro, ya que usar más potencia que la necesaria aumenta las posibilidades de interferir con otros usuarios. Existen algunos dispositivos que no permiten cambiar la potencia de salida por estos motivos.

> LA GRAN MAYORÍA DE LOS PUNTOS DE ACCESO POSEEN LA OPCIÓN PARA CAMBIAR LA TASA DE TRANSMISIÓN

Debemos tener en cuenta que la potencia máxima se debe calcular considerando la ganancia de nuestra antena (si dejamos las antenas como vienen de fábrica en nuestro punto de acceso, esto no será necesario, lo implementaremos si usamos una antena diferente a la original). La suma de la potencia de salida en dBm y la ganancia de la antena en dBi es el parámetro que se conoce como PIRE (Potencia Isotrópica Radiada Equivalente o en inglés, EIRP). Veremos más de esto en el capítulo dedicado a las antenas. Si lo que deseamos es aumentar la capacidad total de nuestra red inalámbrica y agregamos puntos de acceso uno cerca de otro, la potencia que usemos tendrá que establecerse en el valor más bajo posible. Se hace así para disminuir el solapamiento y la interferencia. Modificar la orientación de las antenas puede minimizar la interferencia entre puntos de acceso.

Tasa de transmisión

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.

OVERCLOCKING DE POTENCIA

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



Figura 19. En general si vemos las configuraciones avanzadas de nuestro dispositivo encontraremos opciones más específicas.

Como se muestra en la figura, los valores varían según la norma que usemos. Para IEEE 802.11b, los valores puede estar en 11, 5.5, 2 o 1 Mbps; para IEEE 802.11g, varían.

Debemos saber que si al momento de seleccionar nuestra norma usamos la opción **mezcla,** vamos a tener la posibilidad de ver en el menú donde seleccionamos la tasa de transmisión todos los valores disponibles para nuestra norma seleccionada, incluyendo que la selección se realice de forma automática con la opción **auto**. Si el usuario no tiene los suficientes conocimientos para seleccionar una opción, recomendamos dejar auto.

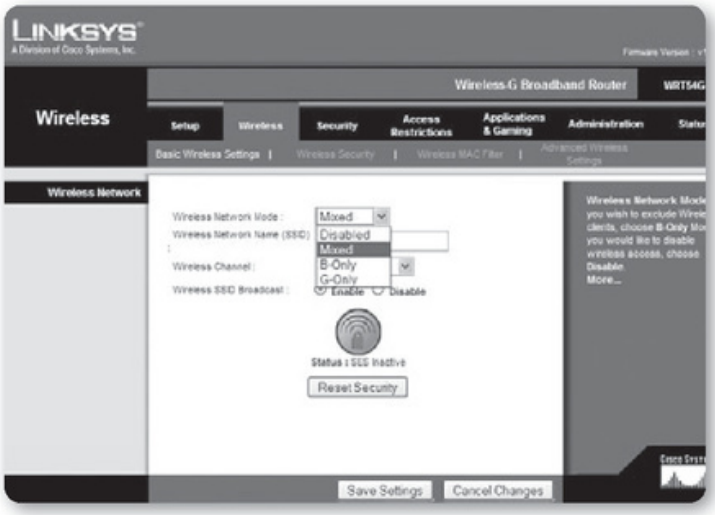


Figura 20. En la configuración básica podemos seleccionar una norma a utilizar o una mezcla de ambas.

Cuando nosotros realizamos el cambio de la tasa de transmisión valor, estamos modificando la técnica de modulación empleada para realizar la transmisión de datos. Es recomendable que definamos la mayor velocidad posible cuando configuremos este parámetro. Debemos tener en cuenta que si nuestra red inalámbrica va a extenderse sobre un área grande y sufrimos problemas de recepción, pérdida de datos, entre otros errores que veremos luego, podemos reducir la tasa de transmisión para lograr una señal que sea un poco más robusta y de mejor calidad.

Recomendamos realizar un ejercicio práctico y útil que consiste en variar los valores y tomar nota de los resultados, así podremos ver e identificar cuál es la tasa de transmisión que nos conviene.

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

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 (que son los tan nombrados modos infraestructura y ad hoc). ¡A no confundir conceptos!

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.



MODIFICAR EL FIRMWARE

Existen versiones modificadas no oficiales de firmware que son creadas por terceros y nos permiten tener nuevas características o usar funcionalidades ocultas. Esto implica hackear el firmware. Algunos ejemplos ocurren en las cámaras Canon, Access Point Linksys o ciertos reproductores de DVD, en los que se obtienen nuevas opciones de configuración. Un proyecto destacado es el **dd-wrt**.

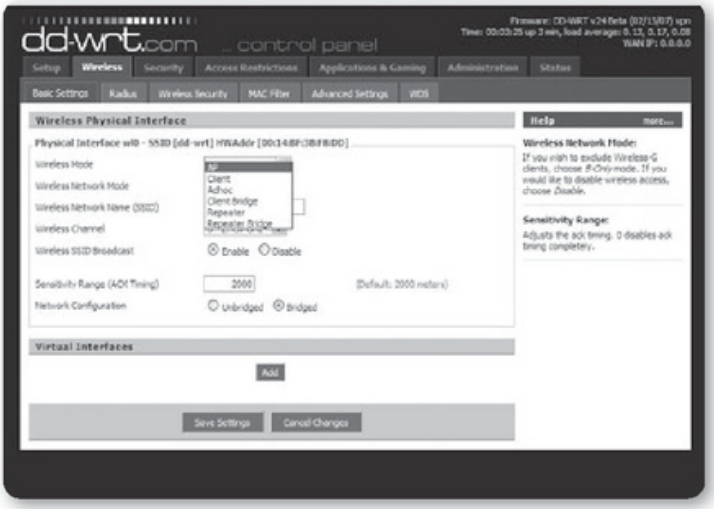


Figura 21. Un router con firmware dd-wrt, donde la opción Wireless mode hace referencia a las tareas que pueden realizar el dispositivo.

Cualquier punto de acceso puede funcionar como un puente que vincula la red cableada y la inalámbrica. Podemos decir que funciona como puente si solamente realiza este vínculo y nada más. En cambio, si además, se llevan a cabo funciones como enrutamiento y enmascaramiento (NAT), decimos que tenemos un enrutador inalámbrico funcionando en nuestra red.

NAT (*Network address translation*) o Traducción de direcciones de red es un mecanismo que hace de intermediario en una red. Se lo conoce también como enmascaramiento de IP. En esta técnica, las direcciones IP de origen o destino de la información enviada o recibida son reescritas, es decir sustituidas por otras (por este motivo se le llama enmascaramiento) para los usuarios dentro de una LAN.

Cuando varios usuarios comparten una conexión a Internet solamente poseen una única dirección IP pública que deber ser compartida. De esta forma los usuarios dentro de una red LAN utilizan direcciones IP reservadas para uso privado y será necesario un dispositivo que se encargue de traducir las direcciones privadas a esa única dirección pública de salida a Internet. De la misma forma, la información recibida por esa dirección pública será distribuida al usuario interno que la solicitó. Las direcciones IP privadas se seleccionan en rangos prohibidos para uso en Internet como: 192.68.x.x, 10.x.x.x, 172.16x.x, para nombrar algunos ejemplos.

El uso de NAT es muy común en domicilios o empresas con muchas computadoras en red y con un solo acceso a Internet.

Los modos, entonces, dependerán de si nuestro punto de acceso funciona simplemente como un puente o vínculo entre redes o si actúa como enrutador/NAT.

Podemos nombrar algunos modos típicos que encontramos en la mayoría de los puntos de acceso. Como dijimos antes, debemos prestar atención al nombre del modo ya que puede diferir entre fabricantes. Nombraremos aquí algunos modos típicos que encontramos en la mayoría de los puntos de acceso:

• **Punto de acceso**: también llamado en inglés **Access Point Bridging / Access Point Mode**. En este modo, el punto de acceso es un puente totalmente transparente. No realiza ninguna tarea en el medio y los datos pasan tal cual se envían. Así vincula el enrutador y los clientes inalámbricos de la red. Este modo es la configuración más simple para nuestro dispositivo.

• **Pasarela**: también se puede encontrar como **Gateway**, por su traducción en inglés. En este modo, nuestro dispositivo funciona como un enrutador inalámbrico entre una red LAN y los clientes inalámbricos. Realiza tareas de enrutamiento y enmascaramiento (NAT) para esos clientes. Nuestro dispositivo puede obtener del proveedor de acceso a la Red (ISP u otro) una dirección IP a través de **DHCP** (*Dynamic Host Configuration Protocol*).

El DHCP es un protocolo que permite a clientes de una red obtener de forma automática sus parámetros de configuración (dirección IP, mascara de red, entre otros). Este protocolo le permite al administrador de la red monitorear y distribuir de forma centralizada las direcciones IP necesarias entre otros parámetros. El punto de acceso también puede proveer direcciones IP a sus clientes, ya que cuenta con un servidor de DHCP dedicado para esto.



IMPRESIONES SIN CABLES

Con un **servidor de impresión inalámbrico** se comparte una impresora de red entre usuarios cableados o inalámbricos en la misma red y así no usamos una PC como servidor de impresión. Estos pequeños dispositivos permiten conectar una o más impresoras USB. Luego el servidor de impresión se conecta a nuestra red LAN de forma inalámbrica usando las tecnologías 802.11b/g y 802.11n.



Figura 22. La configuración del servidor DHCP se puede realizar dentro de las configuraciones básicas de cualquier dispositivo.

• **Puente punto a punto**: se puede encontrar, en algunos dispositivos, como **Point-to-Point bridge/Repeater mode**. En esta configuración usamos dos puntos de acceso para hacer un puente entre dos redes cableadas. Por supuesto que podemos seguir conectando usuarios al punto de acceso ya sea por medio de un cable o de forma inalámbrica sin embargo, debemos recordar que con esta configuración extendemos el área de cobertura de nuestra red de forma considerable.

No se realiza ninguna tarea extra y los datos pasan sin sufrir modificación alguna en su camino.

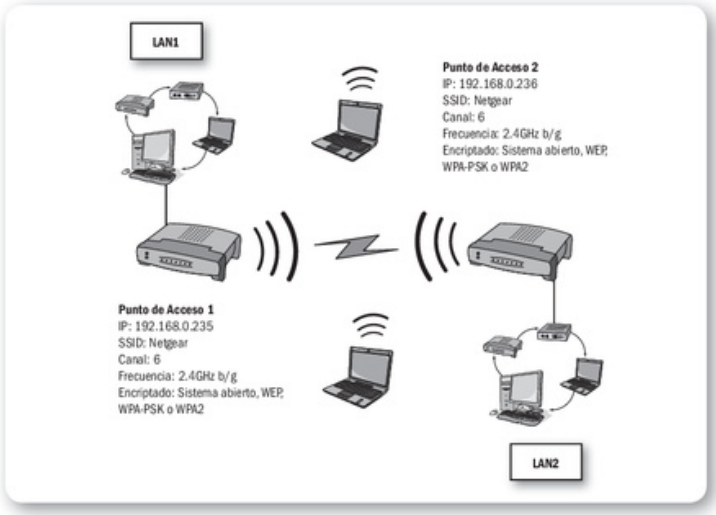


Figura 23. El modo Point-to-Point bridge/ Repeater mode. nos permite extender la red sin necesidad de cables.

• **Enrutamiento punto a punto:** este modo nos permite usar el punto de acceso como un enrutador inalámbrico entre dos redes LAN separadas. Lo podemos encontrar como **Point-to-Point routing/ Wireless Bridge Link** en algunos equipos.

• **Adaptador inalámbrico Ethernet**: la finalidad de este modo es poder usar un punto de acceso como una placa inalámbrica para aquellas computadoras donde no se soporten placas PCI, USB o PCMCI por algún motivo. Se puede conectar nuestra computadora al punto de acceso a través del puerto USB o Ethernet para así reconocerlo como un dispositivo y usarlo como si fuese una placa inalámbrica.

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 envía desde un dispositivo conectado a todos los demás dispositivos 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 milisegundos (ms).

EL SSID ES EL NOMBRE QUE ASIGNAMOS A NUESTRA RED LAN INALÁMBRICA

Simplemente definimos al SSID como una cadena de texto que diferencia las letras minúsculas de las mayúsculas, acepta hasta 32 caracteres alfanuméricos y además es usada en el proceso de asociación a una red inalámbrica. Pensemos que esta asociación es como enchufarnos al dispositivo.

Si los clientes desean comunicarse con un punto de acceso, entonces deberán usar el SSID durante la asociación (veremos esto más adelante). Este identificador es difundido por nuestro dispositivo en el **beacon** para así anunciar su presencia a los potenciales clientes.

Si nuestro dispositivo no posee medidas de seguridad para autorizar a nuestros clientes a conectarse (veremos estas medidas más adelante, pero podemos nombrar WPA, filtro MAC, entre otros), entonces cualquiera puede asociarse al punto de acceso y conectarse a la red de forma fácil y rápida.

Control de acceso al medio

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

• **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 nuestra casa, con estos beacons vamos a tener conocimiento de la existencia del punto de acceso sin ningún problema. Este valor se puede modificar pero no es recomendable salvo que se tenga conocimientos avanzados y una buena razón para hacerlo.

• **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 grabado 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 de forma 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 hoy en día. Aunque este mecanismo de encriptación

EXISTE UNA SEGUNDA GENERACIÓN LLAMADA WPA2

(o cifrado de datos) posee grandes falencias y muchos no lo consideran como una opción segura para asegurar sus datos, es común que un usuario con conocimientos intermedios lo use.

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

Existen alternativas al protocolo WEP como 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 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.

Un punto de acceso puede comportarse como AP o como puente, y así se logra que la red se extienda fácilmente. Todos los puntos de acceso de la red WDS deben configurarse para usar el mismo canal de radiofrecuencia y compartir las claves WEP o WPA en caso de implementarlas. La conexión de los clientes se hace en la capa 2, ya que se utilizan las direcciones MAC de las placas inalámbricas de origen

NAT O NO NAT

Cuando un punto de acceso es simplemente un "concentrador inalámbrico" y no soporta enrutamiento y enmascaramiento (NAT), la conexión de redes inalámbricas se restringe a solo las dos primeras capas del modelo OSI, que son la capa física y la capa de enlace. En cambio si soporta NAT también incluirá opciones relativas a la capa de red, capa 3 del modelo OSI.

y destino, las cuales gracias a WDS se guardan en dos campos de los datos que son transferidos.

Nosotros podemos usar WDS para proveer dos modos de conexión inalámbrica entre puntos de acceso:

• Un puente inalámbrico que solo nos permita la comunicación entre dos puntos de acceso sin posibilidad de que otro cliente de la red pueda acceder a la red.

• Un repetidor inalámbrico que nos permita que un punto de acceso se comunique con otros puntos de acceso y clientes inalámbricos.

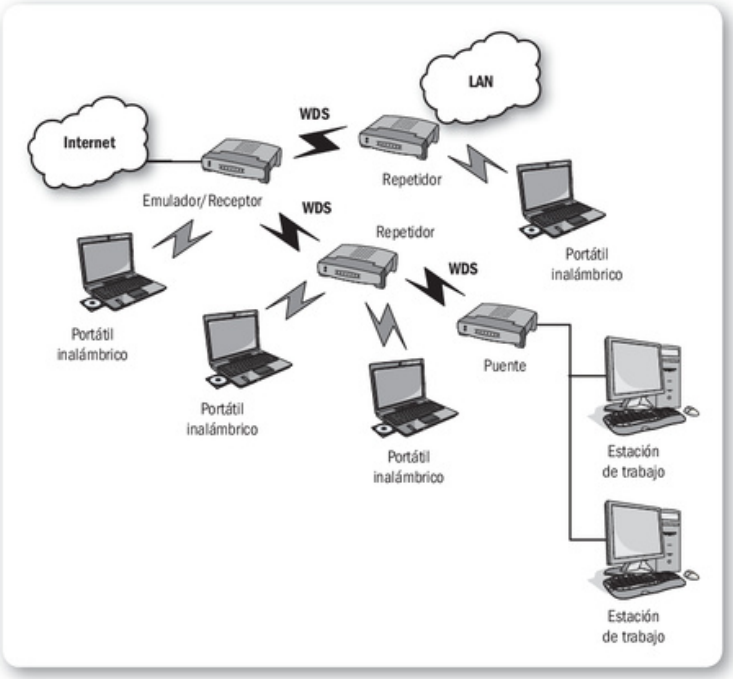


Figura 24. En este esquema podemos ver la implementación del sistema WDS.

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 extras 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:

TABLA 1

▼ 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 como pasarela. Es la dirección IP de 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 la de traducir nombres inteligibles para los humanos (como una dirección de una pagina 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. En esta tabla, podemos ver las opciones a 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, tiene total control sobre las configuraciones y sin problemas puede cambiar la contraseña de administrador y de esa forma dejarnos sin acceso a nuestro equipo inalámbrico. La única solución a 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 de nuestro proceso de configuración se encuentran en la capa de aplicación.



RESUMEN

Según lo visto en el capítulo, concluimos que cuando necesitamos instalar un punto de acceso o router inalámbrico será necesario que identifiquemos el hardware que vamos a utilizar y conozcamos qué tipo de red queremos implementar. 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 de atrás de los puntos
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 PC?
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?

*03 -

Configuración en Windows

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

- **Instalar clientes en Windows 102**
- **¿Qué hardware utilizar? 103**
  - Instalar el hardware es fácil 103
- **Configurar el hardware en Windows 111**
  - Configurar la red inalámbrica 126
  - Configurar la red para compartir 134
  - Configuración de red inalámbrica, modo infraestructura 139
- **Configuración de una red inalámbrica AD HOC 145**
  - Configuración de Internet en una red AD HOC 147
- **Resumen 149**
- **Actividades 150**

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) se desconoce por parte de nuevos usuarios de computadoras 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 esté encendida o no podremos avanzar.

• 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 nos puede causar algún problema. Para evitar esto, seleccionaremos solo un gestor de configuración y desactivaremos el otro. Recomendamos usar el gestor que MS Windows provee.

Planteamos esto ya que tendremos mayor soporte en caso de presentarse algún problema.



Figura 2. En la notebook de la imagen, el botón que habilita nuestra interfaz inalámbrica se encuentra en la parte superior del teclado.

¿Qué hardware utilizar?

Windows lidera el mercado en materia de sistemas operativos para usuarios hogareños, aquellos que no poseen mucha experiencia o los usuarios que necesiten una plataforma fácil de instalar y que funcione de manera estable. Las últimas versiones de Windows que salieron al 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 gran mayoría de los fabricantes (por no decir todos) dan soporte de sus productos para Windows. Así, cualquier hardware podrá utilizarse.

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

Instalar el hardware es fácil

Cuando instalamos nuestro hardware siempre es necesario tener los **drivers** (controladores) en nuestro sistema operativo correctamente configurados. Los drivers son programas que permiten que el sistema

operativo pueda controlar 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 este nuevo sistema operativo tiene soporte para gran cantidad de dispositivos. En caso de utilizar alguna versión anterior (Windows 98, Windows 2000, Windows XP, por ejemplo) o algún dispositivo viejo, se puede requerir un poco más de esfuerzo en la instalación.

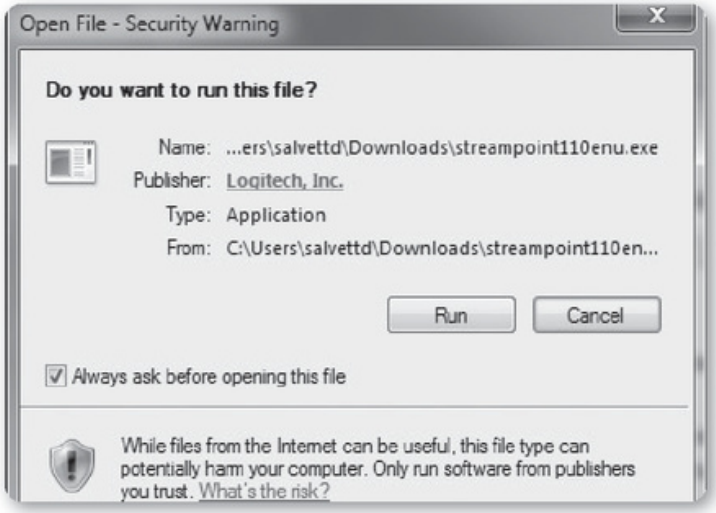


Figura 3. Cuando instalamos un driver se presenta una ventana donde se nos pregunta si queremos ejecutar el programa.

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

INSTALLSHIELD COMO HERRAMIENTA

Para crear instaladores de programas que nosotros desarrollamos, tenemos la posibilidad de usar **InstallShield**, una herramienta de software desarrollada por la empresa Stirling Technologies, que luego se llamó InstallShield Corporation. Se suele utilizar para software de escritorio, sin embargo, también se usa para administrar aplicaciones y programas en dispositivos móviles y portátiles. Se utiliza una interfaz amigable y fácil de manipular para crear in archivo ejecutable que realizará la instalación de nuestro programa en cualquier computadora.

instalación de programas adicionales, dependerá de cada caso en particular.

La forma más común de instalar un driver es por medio de un **InstallShield** o programa de ayuda para la instalación, que es distribuido en forma de archivo ejecutable (**.EXE**). Hacemos uso del sistema InstallShield cuando la instalación del driver implica la instalación de programas extras, como es el caso de drivers de placas de sonido, impresoras, placas de video, entre otros.

> CUANDO INSTALAMOS NUESTRO HARDWARE SIEMPRE ES NECESARIO TENER LOS DRIVERS

La instalación del driver consiste en ejecutar el instalador (archivo **.EXE**, que, en general, se llama **setup.exe**) y seguir una serie de instrucciones que aparecen en el proceso. Muchas veces se presentan opciones de instalación y configuración. Este mismo sistema se usa, por ejemplo, cuando se necesita expandir (o descomprimir) los drivers en un directorio específico. Con solo ejecutar un instalador podremos lograr tener nuestros drivers disponibles para luego usarlos.

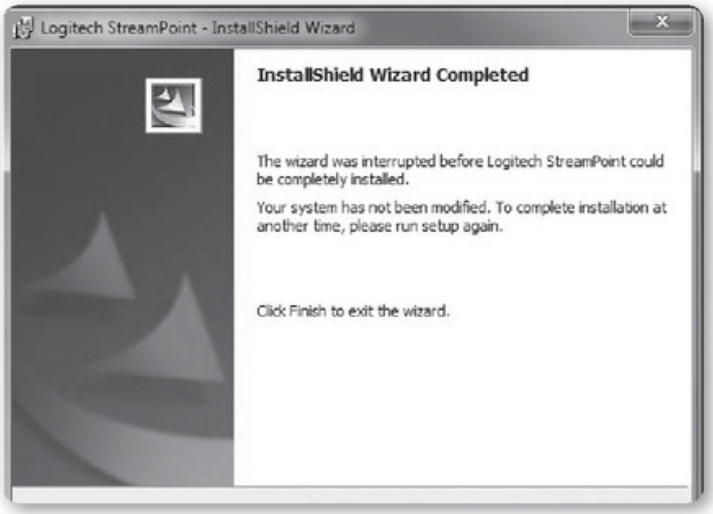


Figura 4. La ventana final nos confirma la correcta instalación del driver en el sistema operativo.

Otra forma de instalar un driver es mediante el reconocimiento automático del dispositivo y la búsqueda del controlador por parte del sistema **Plug and Play** o P&P (enchufar y usar). Esta tecnología permite que un dispositivo sea conectado a una computadora sin tener que configurar ni proporcionar parámetros a sus controladores. No debe entenderse como sinónimo de no necesitar controladores.

Funciona de la siguiente manera, debemos preinstalar los drivers en una carpeta específica que consideremos fácil de acceder, esto lo podemos hacer mediante el programa instalador, o bien en muchos casos descomprimiendo un archivo tipo **.RAR** o **.ZIP** en ese directorio.

Una vez que conectamos el dispositivo, el sistema P&P lo va a detectar e intentará localizar el controlador en nuestro sistema. Cuando el sistema P&P no encuentra el controlador, nos solicitará que ingresemos la ruta donde tengamos los archivos que hemos descomprimido. Una vez que especifiquemos la ruta donde se encuentran los controladores, estos se instalarán. Podemos usar esta metodología de instalación de driver cuando no es necesario instalar un software junto con los drivers.

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

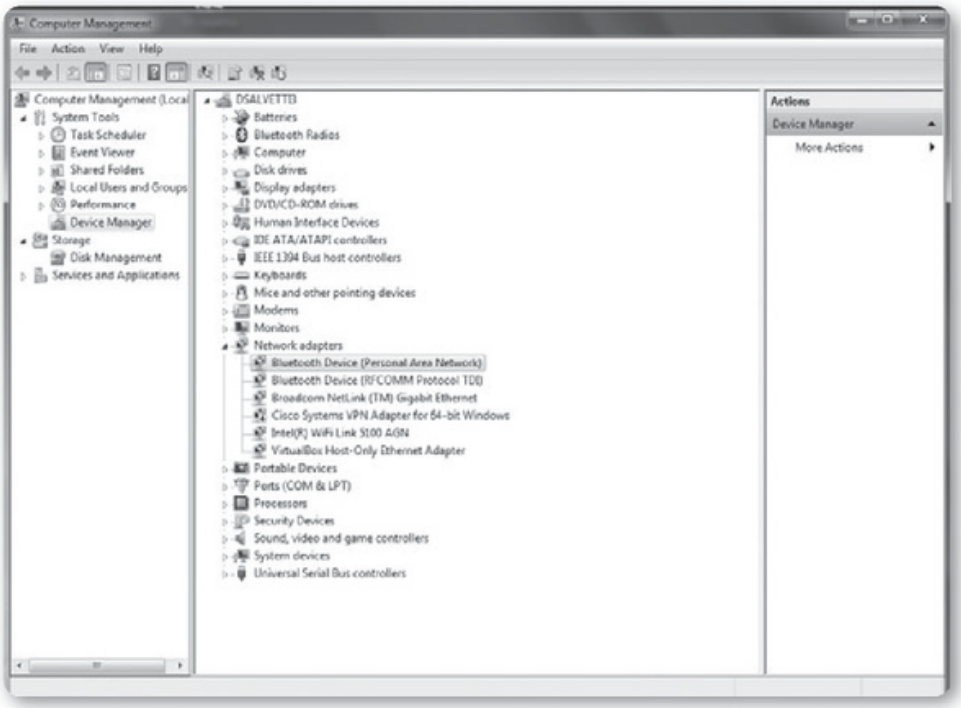


Figura 5. Hacemos **clic** con el botón derecho en el **icono de Equipo** (Computer) en el escritorio y seleccionamos **`Administrar`** (Manage).

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 driver.

Hay que prestar atención a nuestros drivers. Debemos 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. No contar con éste archivo puede causar problemas.

En todos los casos, usemos 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.

Las versiones actuales de Windows ya tienen herramientas especialmente dedicadas a redes inalámbricas. Por este motivo para la gran mayoría de los dispositivos USB o PCMCIA no será necesario instalar drivers dado que Windows ya los tiene disponibles. No es el caso de las placas PCI para computadoras de escritorio, donde sí es necesario instalar el driver que el fabricante nos facilita.

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

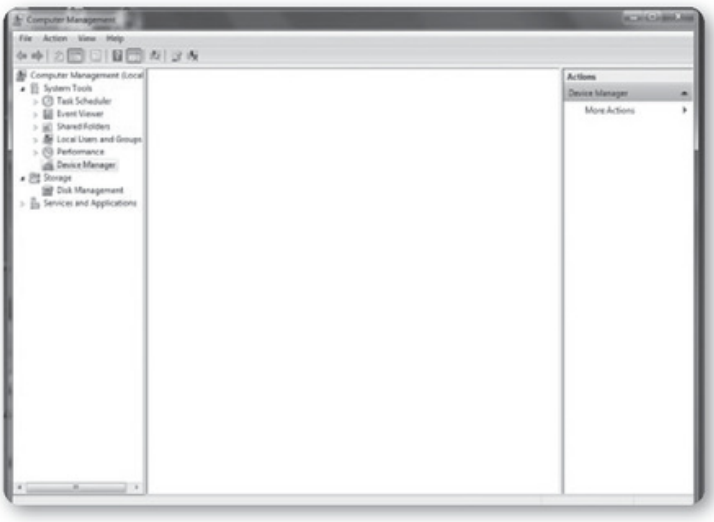


Figura 6. Windows nos informará que ha detectado e instalado automáticamente los drivers necesarios para nuestro dispositivo.

En caso de que ya tengamos acceso a Internet en nuestra computadora por medio de cable, podremos descargar la versión más reciente del driver disponible para nuestro sistema.

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 nuestra nueva placa inalámbrica. Este lugar vacío se llama **slot PCI** y se encuentra en nuestra placa base (**motherboard**). Veamos la figura siguiente.

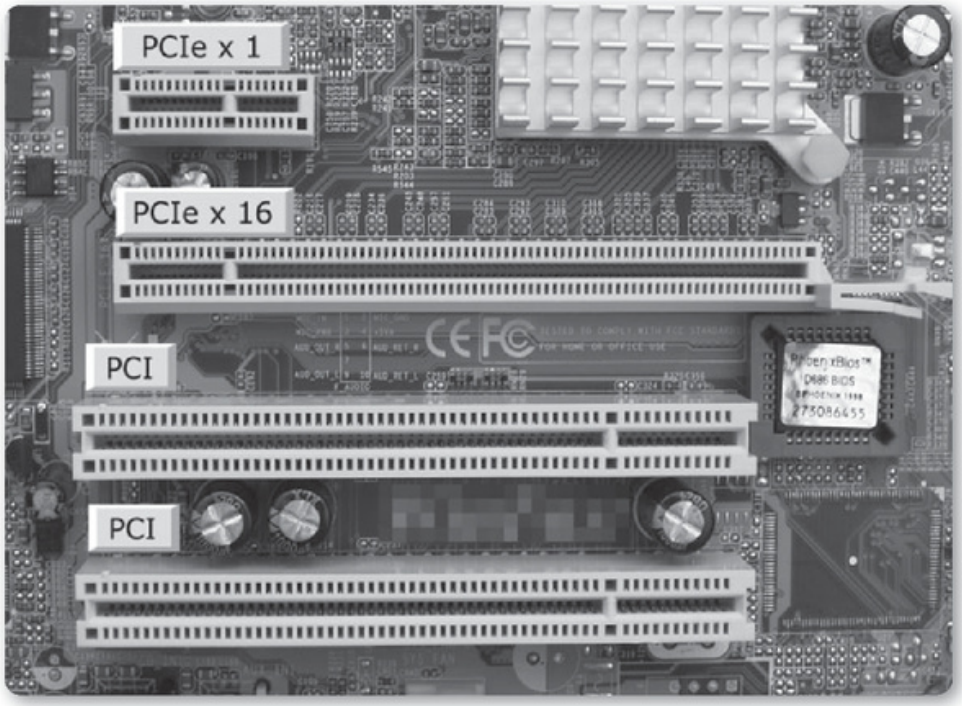


Figura 7. El esquema muestra las diferentes formas de los zócalos de expansión (también llamados slots).

MEZZANINE O PCI

PCI es una especificación para la interconexión de componentes en computadoras. El bus **PCI**, llamado también **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.

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, de red, entre otras). Los slots presentan diferente tamaño (como se puede observar en la figura) y a veces diferente color. Esto es así para distinguir la tecnología en que se basan.

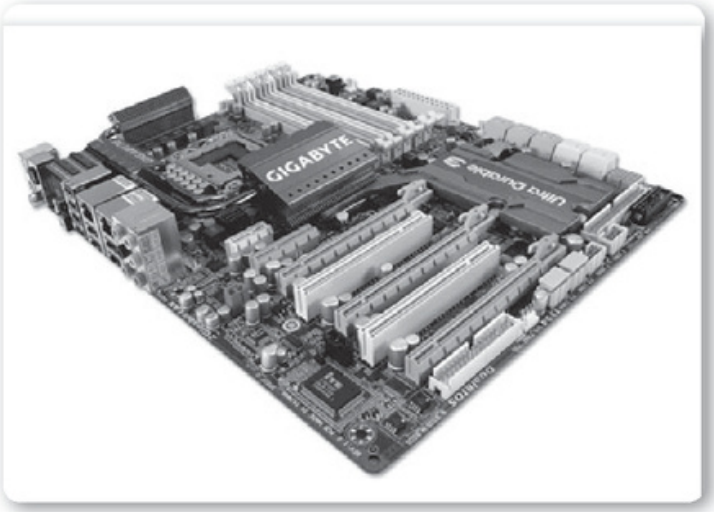


Figura 8. En los motherboards están diferenciados por color y tamaño los slots de expansión. El PCI mide unos 8,5 cm y generalmente es blanco.

Una vez conectada la placa PCI volveremos 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 este, podemos dejar que Windows instale el que corresponda. Tomemos, como ejemplo, la instalación de la placa PCI en una computadora de escritorio. Aunque esta instalación 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 y seguir algunas recomendaciones para no tener mayores inconvenientes.

En la próxima páginas, veremos algunos de los pasos básicos para instalar la placa PCI en nuestra computadora:

• Sería un buen comienzo que leyéramos el manual de instrucciones de la placa inalámbrica PCI antes de comenzar la instalación. Si es necesario, instalemos los drivers de la placa en el sistema operativo.

• Apaguemos nuestra computadora haciendo clic en el icono de Windows y luego en **Apagar** (*Shut Down*). Después desenchufemos la fuente de alimentación por seguridad.

• Si lo deseamos, para trabajar con mayor comodidad, podemos desenchufar los cables que están conectados en la parte de atrás de la PC (mouse, teclado, entre otros). Si creemos que no recordaremos cómo estaban conectados, hagamos un diagrama en papel de la conexión actual para que podamos seguirlo a la hora de reconectar todo.

• Ahora quitaremos la tapa del gabinete desatornillando los tornillos del costado. Es una práctica común utilizar una pulsera antiestática para evitar descargas eléctricas al manipular el gabinete. Si bien es improbable que suceda si tenemos la alimentación de la red eléctrica desconectada, es algo que puede ocurrir.

• Una vez que quitamos la tapa, debemos identificar los slots PCI en nuestra placa madre. Tengamos en cuenta que si no existen slots vacíos, tal vez tengamos que quitar alguna vieja placa PCI en desuso.

• Conectemos nuestra placa PCI inalámbrica en el slot vacío. Si en el slot nunca fue conectada una placa entonces tendremos que quitar una pequeña chapita de metal que es por donde saldrá la antena de nuestra placa. Esta pequeña chapa se desatornilla. Recomendamos guardarla para tapar espacios vacíos cuando no tengamos placas conectadas en los slots. Para colocar la placa, presiónela hasta que todos los conectores hayan encastrado bien. No presione muy fuerte porque corre el riesgo de estropear la placa madre.

• Aseguremos la placa PCI al gabinete con un tornillo y cerremos el gabinete, verificando que todo esté en su lugar.

• Enchufemos nuevamente la computadora y arranquemos el sistema operativo. Si no desea conectar todos los cables de la parte de atrás, es importante que por lo menos conecte el teclado y el mouse. Muchas veces puede ocurrir que no inicie la PC, en la gran mayoría de los casos es porque no se conectó el teclado o el monitor.

• Cuando inicie Windows 7 se detectará un nuevo hardware conectado en nuestra computadora. Instalemos los controladores, según vimos anteriormente como paso final.

Hacemos una última aclaración con respecto a las placas inalámbricas para las computadoras de escritorio. Muchas computadoras actuales ya traen incorporado en la placa madre (**motherboard**) una placa inalámbrica. Por lo tanto no es necesario instalar otra placa inalámbrica PCI para conectarse a una red, simplemente debemos consultar el manual de la placa madre e identificar cómo se habilita. Los motherboards actuales poseen drivers de instalación que realizan todas las configuraciones necesarias en Windows. De esta forma, nuestra placa inalámbrica incluida en el motherboard puede operar sin problemas bajo este sistema operativo y nos ofrece conexión inalámbrica a redes.

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, Windows siempre intentará conectarse a la red inalámbrica que tenga la señal más intensa. Nos va a solicitar confirmación antes de concretar la conexión a una red que no tenga contraseña de seguridad. 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 tendremos la lista de las redes inalámbricas detectadas.

DIFERENCIA ENTRE BSSID Y ESSID

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 con estas siglas tan parecidas.

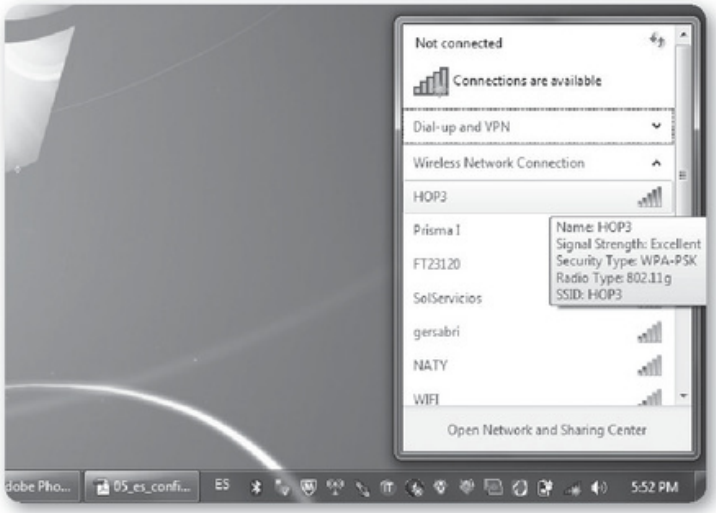


Figura 9. En los iconos, vemos el correspondiente a la conexión de red sin color y con un signo de admiración ya que no estamos conectados.

Si dejamos el puntero del mouse sobre alguna de las redes, podremos ver información básica y útil de la red, como el SSID, el método de cifrado que utiliza la red 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 porque permite que cualquiera se conecte.

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 por ejemplo WEP/WPA, cuando identifiquemos y seleccionemos su SSID y nos conectemos, aparecerá una advertencia de que la red es insegura y, por consiguiente, nuestros datos podrán estar en riesgo de ser capturados por terceros.

Debemos tener especial cuidado en este tipo de conexiones inseguras ya que nuestros datos viajarán sin protección por el espectro de frecuencia en que opera la red.

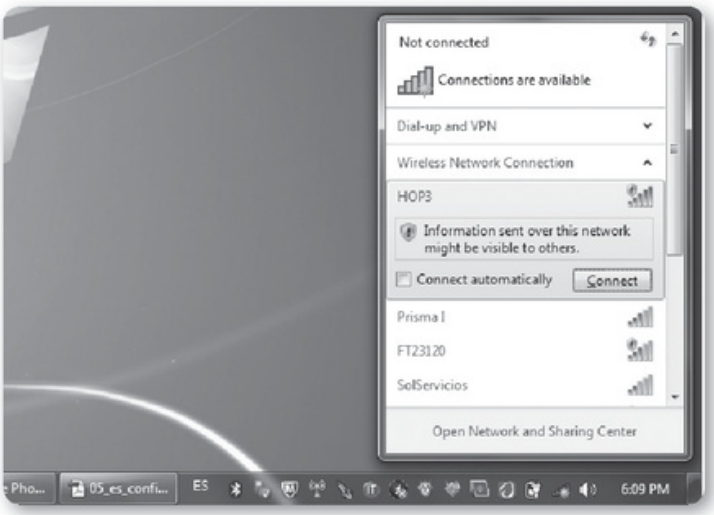


Figura 10. Cuando la red no posee contraseña, nos informarán que al conectarnos, nuestros datos pueden ser vistos por intrusos.

Si nuestra red tiene seguridad por contraseña (configurada en el punto de acceso) necesitaremos tener conocimiento de la clave antes de que nos podamos conectar. La clave de seguridad debería ser la misma con la que se configuró el punto de acceso que se utiliza en la red, recomendamos consultar el manual del equipo.

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



Figura 11. Cuando nuestra red tiene contraseña, se comparte la clave o contraseña de red entre el punto de acceso y sus clientes.

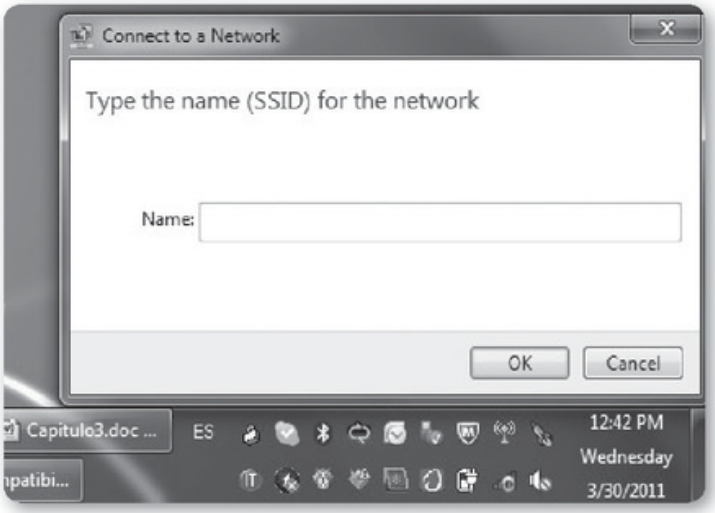


Figura 12. Si nuestra red oculta el SSID por cuestiones de seguridad, tendremos que ingresarlo cuando nos conectemos a la red.

El sistema operativo Windows Seven nos ofrece detalles de nuestra red una vez que estamos conectados.

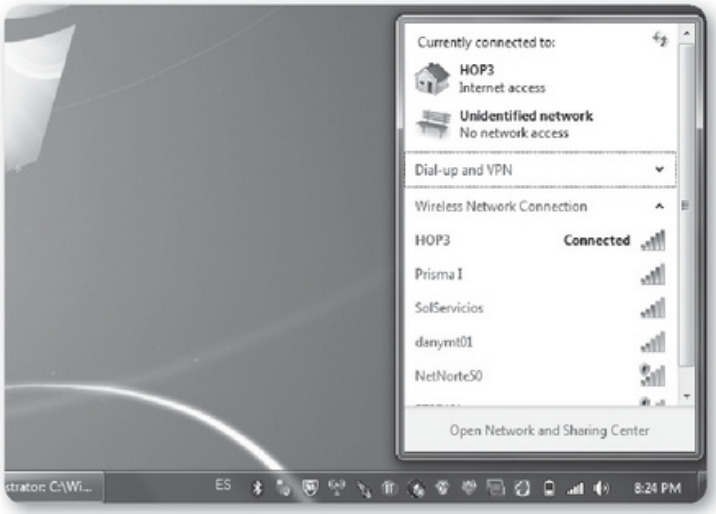


Figura 13. Cuando estamos conectados, si hacemos un clic sobre el icono, en la barra de menú, de la red inalámbrica veremos el estado.

Configurar opciones de TCP/IP

Vamos a verificar y ajustar las opciones de TCP/IP. En esta instancia, podremos obtener una IP dinámica a través del uso del protocolo DHCP o fijar, de forma manual, una dirección IP estática para nuestra placa inalámbrica. 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 conectados 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 denomina **dirección IP dinámica**. Si la dirección no varía se denomina **dirección IP fija**.

Además podemos 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, nuestro router, por ejemplo.

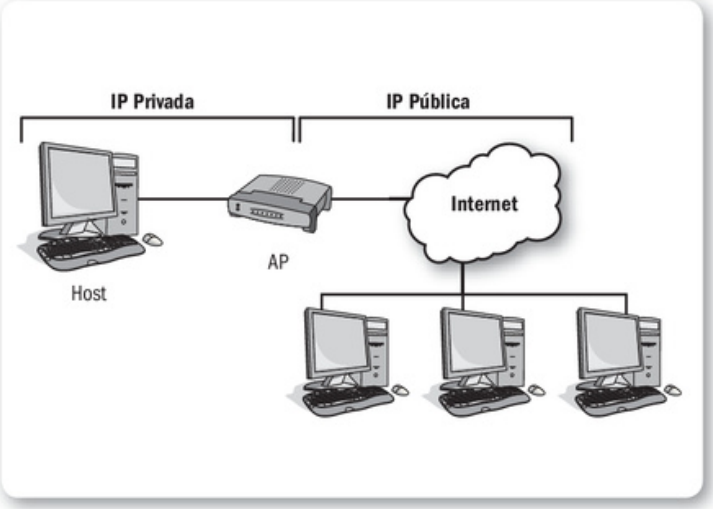


Figura 14. Diferenciamos IP privada y pública tomando como referencia el acceso a la red de redes (Internet).

• IP privada: es la dirección que tiene una computadora o un dispositivo de red (esto 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, 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 aparece 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 IPs van a ser iguales. En caso de tener una red vinculada a un router (u otro dispositivo de red), estas IPs serán diferentes, según la configuración de la red.

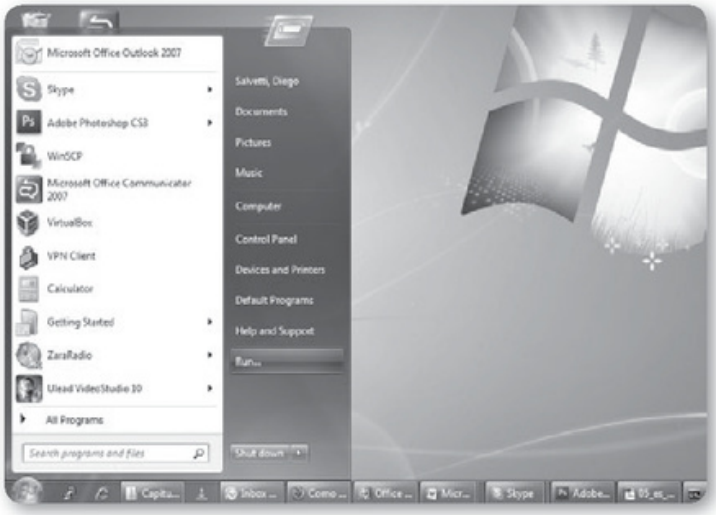


Figura 15. Desde la opción Ejecutar (Run), el sistema operativo Windows nos permite ejecutar comandos.

Si ingresamos al sitio **www.ip2location.com** vamos a poder obtener nuestra IP pública entre otros datos de nuestro proveedor de Internet o ISP, esto es muy útil en ciertas ocasiones.

ASIGNACION DE IP POR DHCP

Sin **DHCP**, cada dirección IP debe configurarse manualmente en los clientes y si 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.

A continuación veremos de qué forma podemos obtener nuestra IP privada con los comandos básicos de Windows. Esto nos ayudará cuando en capítulos posteriores aprendamos un método para la resolución de problemas en nuestra red.

• 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 realizar desde una consola y, muchas veces, esta es la única manera de realizarlo.

Una función que **ipconfig** posee y es bastante importante 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 escribimos **cmd** como se muestra en las figuras siguientes.

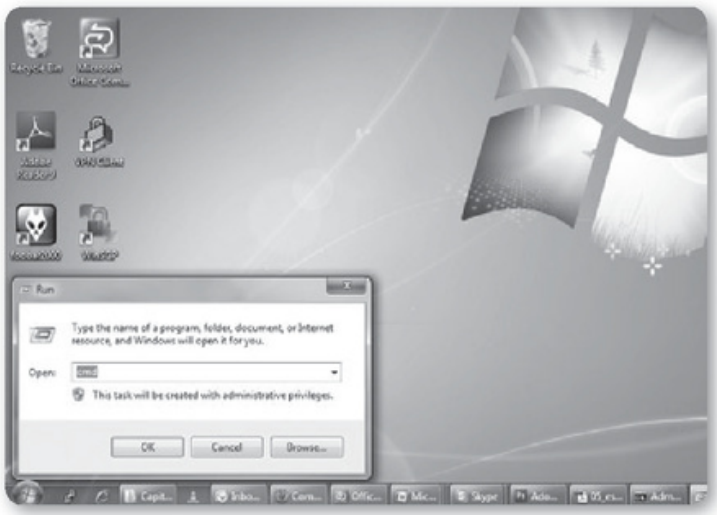


Figura 16. Podemos abrir programas directamente desde esta aplicación ingresando su nombre.

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, como dirección IP asignada en nuestra placa de red instalada.

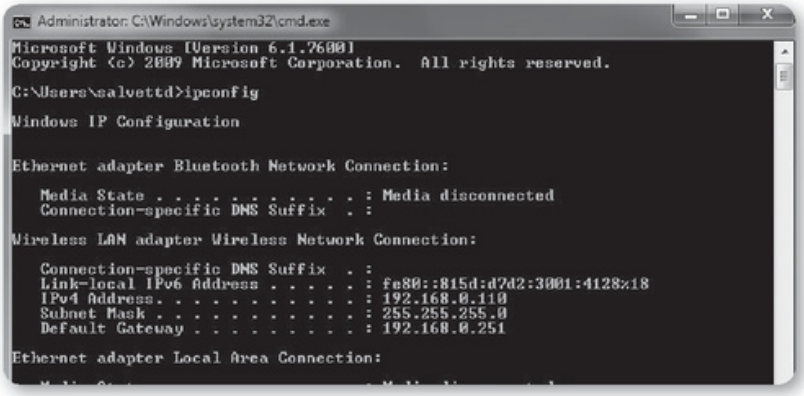


Figura 17. Ejecutar **ipconfig** muestra los detalles de la placa inalámbrica así como también la placa Ethernet (o por cable).

Si queremos obtener más información con este comando, ejecutamos en la consola de nuestro equipo **ipconfig /all**.

Si la IP fue obtenida por DHCP, se mostrará el tiempo durante el cual esta IP es válida y transcurrido este tiempo la IP expira. Si esto sucede, el DHCP automáticamente asignará una nueva IP. Este tiempo figura como **Concesión obtenida** o **Concesión expirada** (*Lease obtained* o *Lease expires*) en la configuración.

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, 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 direcciones 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 esa IP 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 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) en este capítulo).

Renovar la dirección IP suele ser una solución cuando debido a cortes de electricidad (por ejemplo), nuestro router entra en conflicto con la dirección 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 nuestra red o tal vez evitamos el trabajo de reiniciar nuestra propia computadora reiteradas veces.

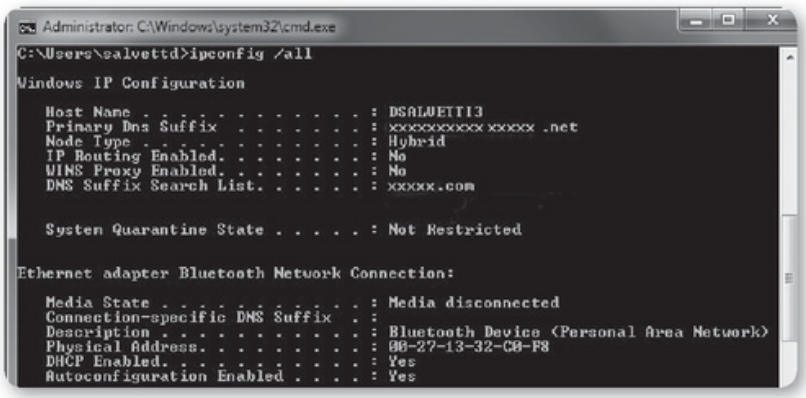


Figura 18. Este comando nos provee información como nombre de host, IP privada, dirección de la puerta de enlace, entre otros.

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

ipconfig /release

Seguido de un:

ipconfig /renew

CONOCER IP PÚBLICA

Si necesitamos 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 consultar los siguientes sitios: **www.my-ip.es**, **www.cualesmiip.com**, **www.cual-es-mi-ip.net**, **www.obtenerip.com.ar**, **www.vermiip.es**, **www.mi-ip.cl** que proveen esta información sin costo.

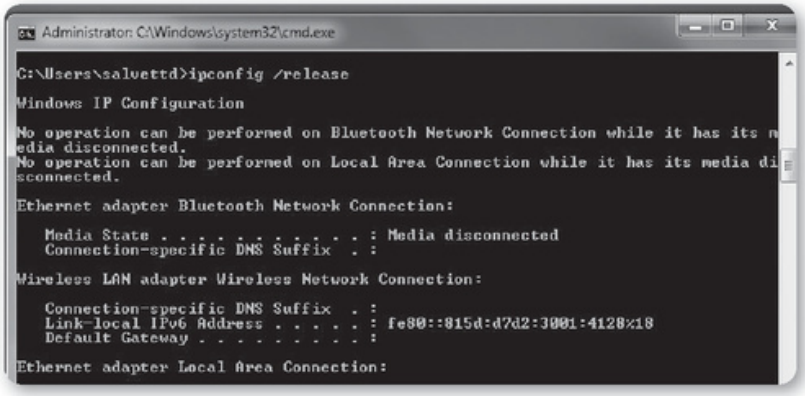


Figura 19. Si obligamos a ipconfig a renovar la dirección IP estaremos asignando una nueva dirección IP valida.

Poder trabajar con la consola del sistema operativo es una gran ventaja para ejecutar comandos.

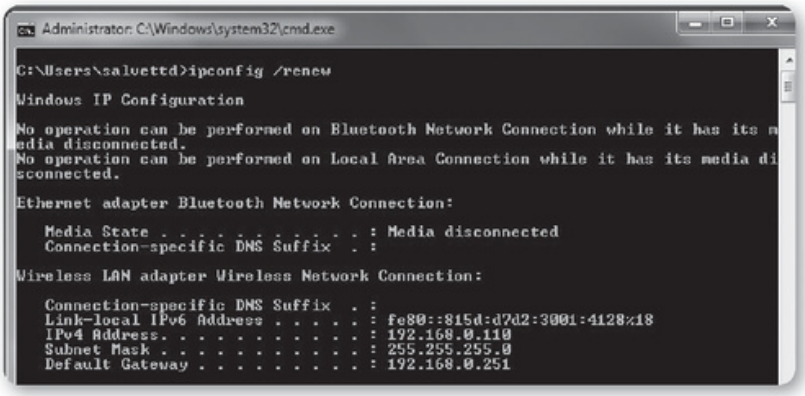
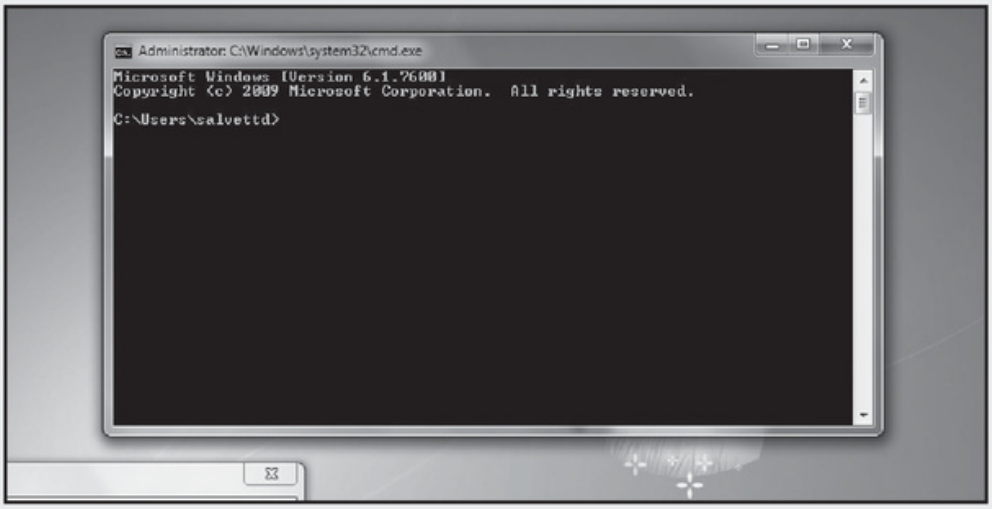


Figura 20. Luego de liberar la dirección IP, ejecutar **`ipconfig/renew`** nos permite obtener una nueva IP.

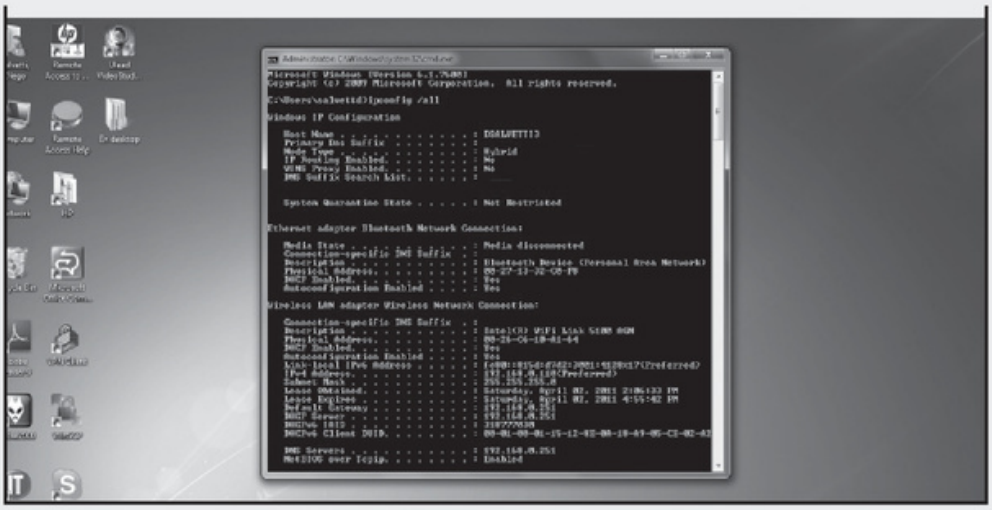
Para fijar de forma manual una dirección IP estática, podemos seguir unos pasos para realizarlo. Tengamos en cuenta que esta es solo una forma de realizar esta asignación y existen otras que no veremos ahora. Antes de comenzar, escribamos en un papel cuáles son las configuraciones que tenemos en estos momentos (esto es en caso de que su red ya esté configurada). Si algo no sale como lo planeamos siempre podremos volver a la configuración inicial si la tenemos.

CONFIGURACIÓN DE IP ESTÁTICA

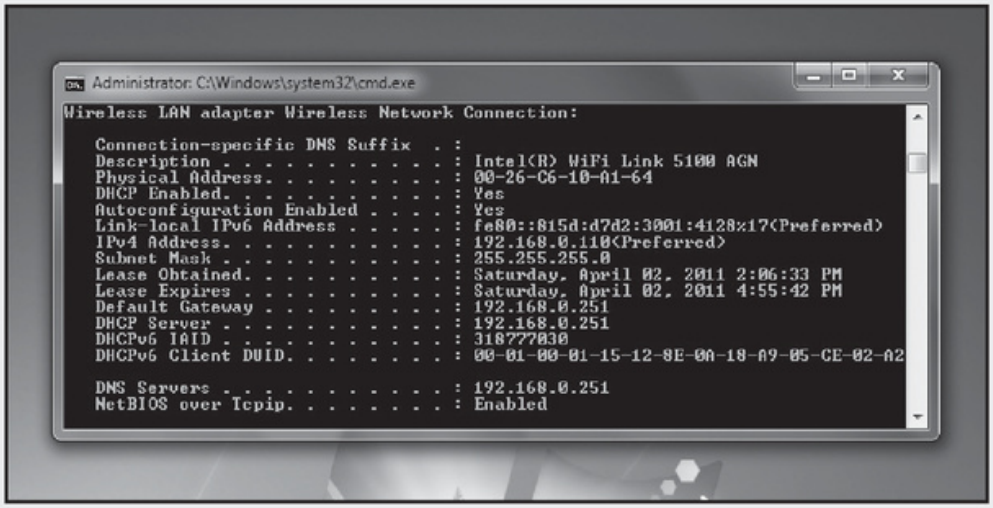
01 Copie la información que actualmente posee para su placa inalámbrica. Puede saltear este paso si no posee ninguna configuración previa para su dispositivo inalámbrico. Abra una consola como se mostró anteriormente haciendo clic en `Inicio` y luego en `Ejecutar` (o Run) y escriba `cmd`.



02 Para continuar y con el fin de ver los parámetros de la placa inalámbrica debe escribir `ipconfig /all` y presione la tecla `Enter`. Esto nos mostrará la configuración actual de todos los dispositivos de red.



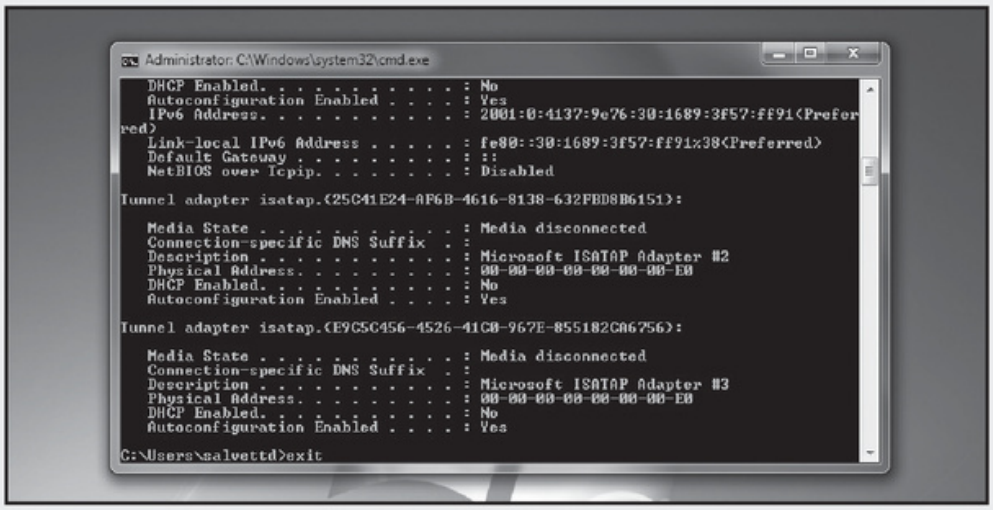
03 Identifique la información relevante correspondiente a su placa inalámbrica. Puede que tenga muchas líneas de información, pero lo importante es que vea las líneas correspondientes a IPv4 Address, Subnet Mask, Default Gateway y DNS Servers. Todos estos parámetros pueden estar descriptos para más de un adaptador, por eso tenga certeza de que está mirando el correcto. Puede subir en la pantalla con la rueda del mouse.



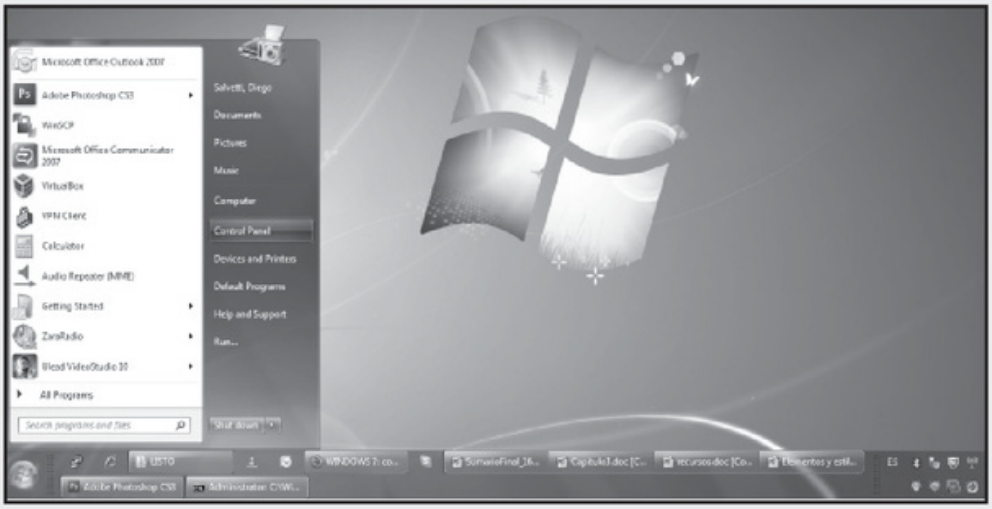
04 Tome nota de los parámetros que identificó. Usted tiene que anotar:

* Dirección IPv4 (IPv4 Address)
* Máscara de subred (Subnet Mask)
* Puerta de enlace predeterminada (Default Gateway)
* Servidores DNS (DNS Servers)

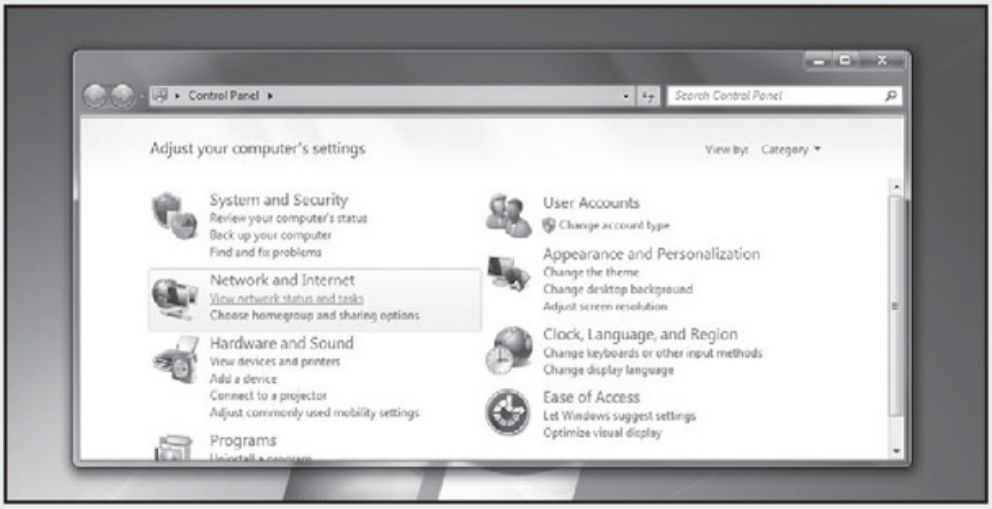
Asegúrese de escribirlos correctamente. No mezcle los datos. Tómese su tiempo. Cierre la consola cuando termine (puede escribir `exit` para cerrarla).



05 Abra el panel de control para seleccionar su dispositivo de red. Vaya a `inicio` y haga clic en `Panel de control` (`Control Panel`).



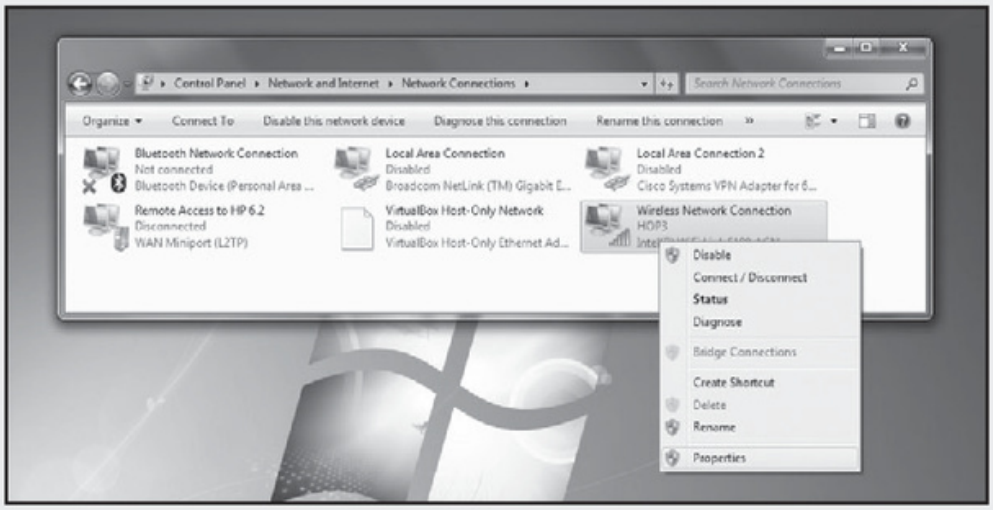
06 Haga clic en `Ver el estado de la red y tareas` (`View network status and task`) para ir a la configuración del adaptador de red inalámbrica.



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.

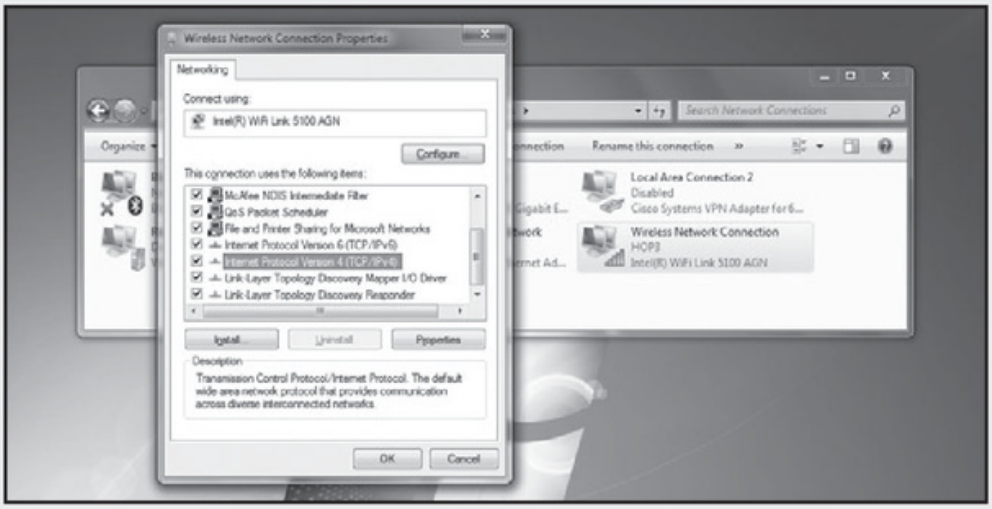


08 Haga clic con el botón derecho del mouse sobre su adaptador de red inalámbrica y luego clic en `Propiedades` (`Properties`). Sólo los adaptadores habilitados tienen colores. Los iconos en colores grises significan que el adaptador está deshabilitado, debe estar atento a esto.



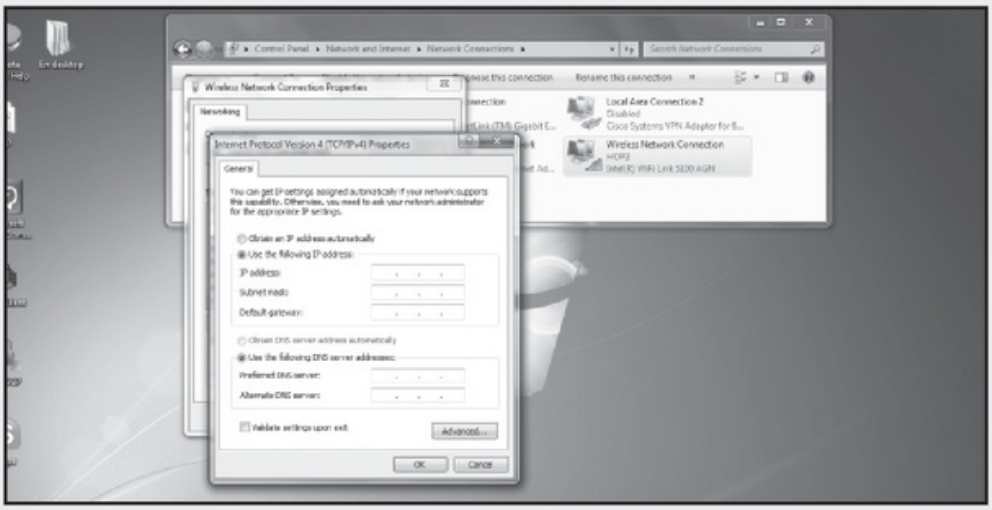
09

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, usted deberá seleccionar 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. Para finalizar ingrese los valores de Servidores de DNS. Haga clic en Ok para cerrar las ventanas y finalizar la configuración de la IP estática.



Tengamos en cuenta que la dirección IP que seleccionemos debe ser similar a la dirección 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, nosotros 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 otro dispositivo de la red. Todo dispositivo que esté conectado a la red deberá tener su propia dirección IP.

> LA DIRECCIÓN IP QUE SELECCIONEMOS DEBE SER SIMILAR A LA DIRECCIÓN IP DEL ROUTER

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 (se lo preguntamos). De todas formas también podemos hacer uso de cualquier servidor de DNS. Por ejemplo **Google** provee el servicio de DNS público de forma 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 son varias pero en general se refieren a un mal servicio, interrupciones, filtrado de contenido escaso, lentitud en la respuesta, entre otros. A causa de estos motivos nacieron los servidores DNS gratuitos en la red.

Configurar la red inalámbrica

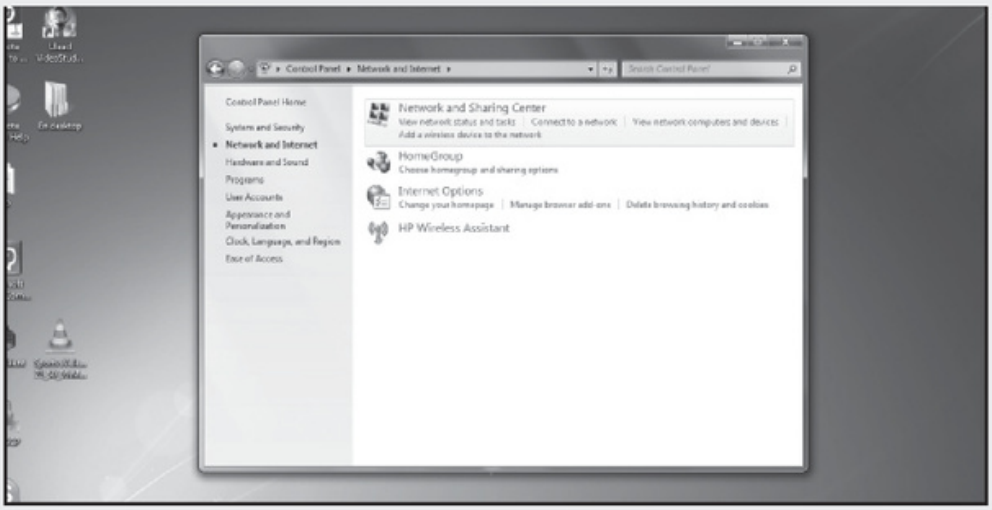
Muchos podemos estar acostumbrados a configurar una red inalámbrica, o tal vez nunca configuramos una y esta es nuestra primera vez. Sea cual sea el caso, veremos ahora cómo se configura una red inalámbrica en el sistema operativo Windows 7, que puede variar un poco si comparamos el mismo procedimiento con versiones de Windows anteriores a este nuevo sistema operativo.

CONFIGURAR LA RED INALÁMBRICA

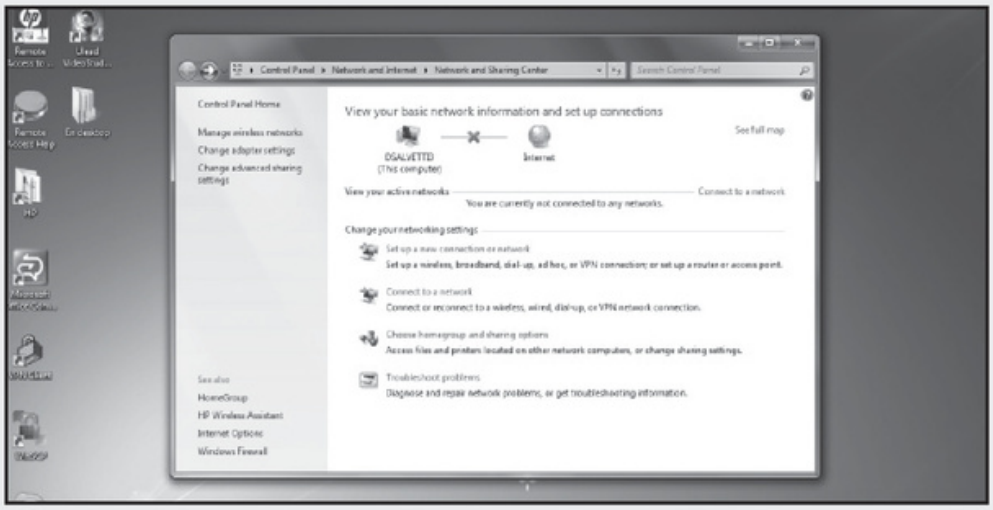
01 Lo primero que debe hacer es acceder al Centro de Redes y recursos compartidos de Windows. Para ingresar, haga clic en el menú `Inicio`, luego en `Panel de Control` y ahí en `Redes e Internet` (`Network and Internet`).



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 en nuestro equipo.



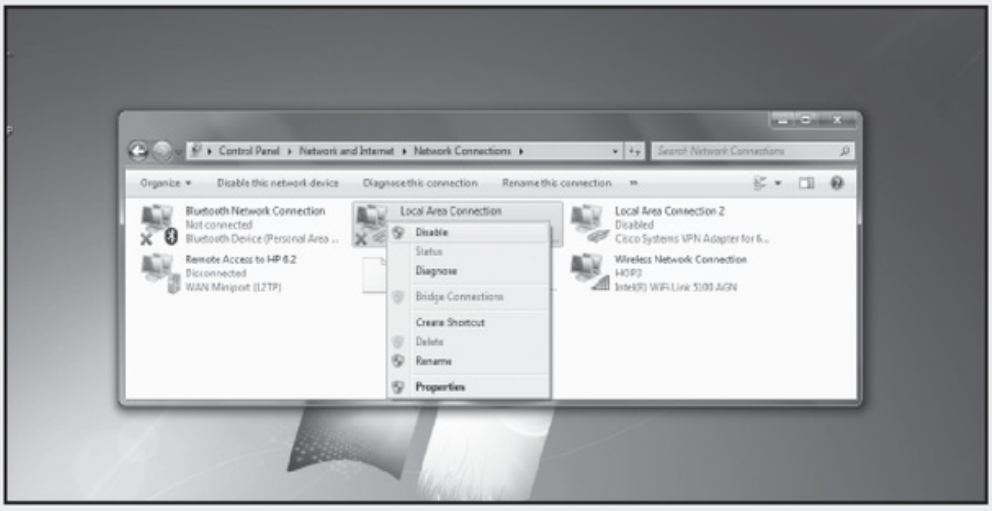
03 Dentro del Centro de redes y recursos compartidos tendrá tres opciones básicas de las cuales se verán sus descripciones en detalle: Administrar redes inalámbricas (Manage wireless networks), Cambiar configuración del adaptador (Change adapter settings) y Conectarse a una red (Connect to a network), como muestra la figura.



04 Ingrese a Cambiar configuración del adaptador y verá una ventana como muestra la siguiente imagen. En esta ventana podemos diferenciar entre los adaptadores habilitados y deshabilitados. Simplemente debe fijarse en los iconos de los adaptadores, los que están en color son los habilitados y los que están en colores claros o grises están deshabilitados (no pueden usarse).



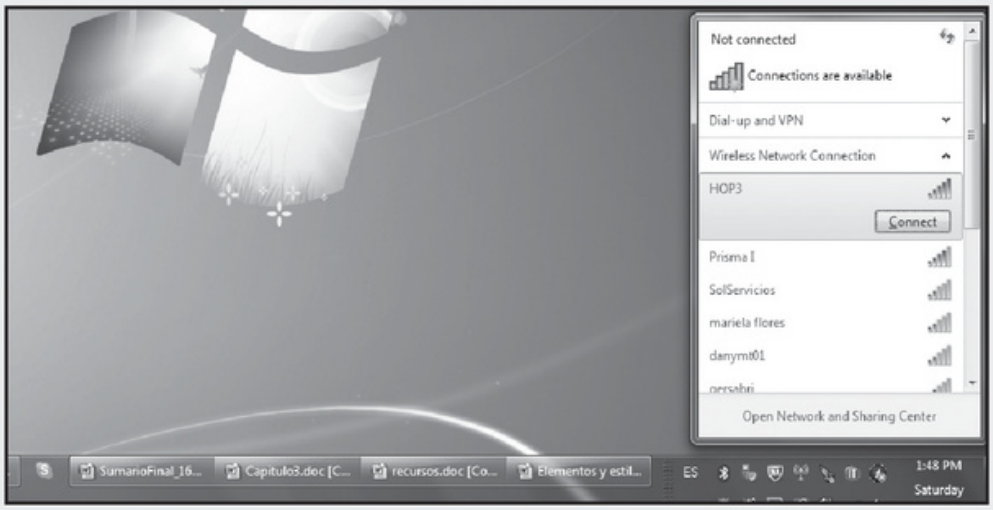
05 Si desea evitar confusiones a la hora de llevar a cabo el proceso de configurar una red inalámbrica, puede optar por desactivar las conexiones de área local u otras conexiones que no sean inalámbricas. Para hacerlo solo tiene que situarse sobre el ícono del adaptador y hacer clic con el botón derecho.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



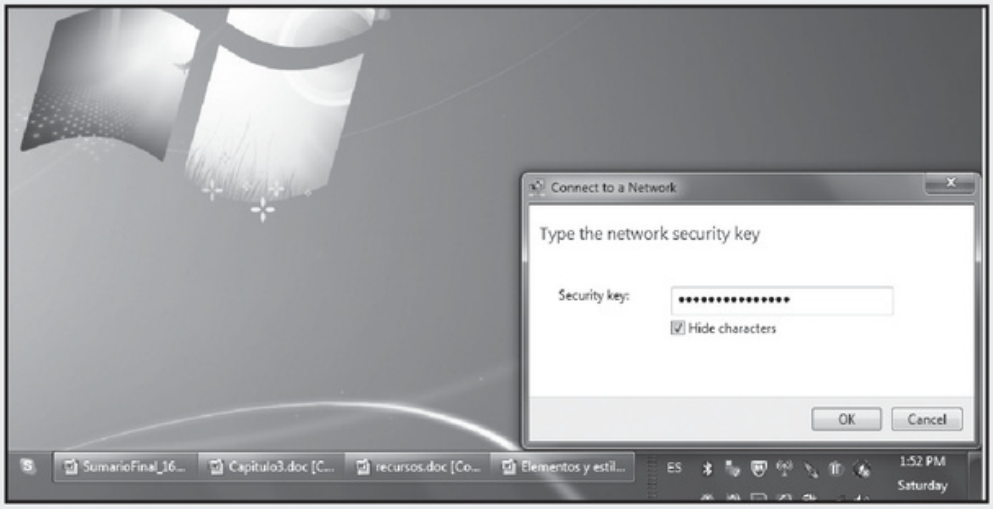
06 Llegado este punto, vuelva al Centro de redes y recursos compartidos (paso 2) y haga clic sobre la opción `Conectarse a una red`. Una vez realizado esto se abrirá el **Escaner de redes inalámbricas** en la parte inferior derecha de nuestro escritorio, tal como lo muestra la imagen.



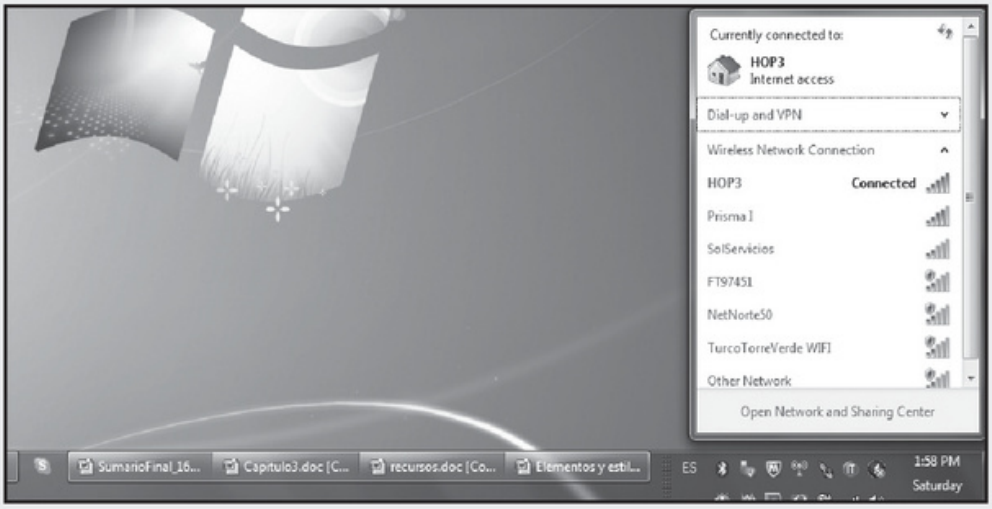
07 Ahora busque su red en el cuadro que muestra todas las redes inalámbricas que están dentro del alcance de su adaptador de red. Si hace clic sobre el nombre (o SSID) de la red tendrá la opción de conectarse como lo muestra la imagen.



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` (`Hide characters`) para ocultar su contraseña. De la misma forma, si no tiene seleccionada esa opción, su contraseña será visible en el cuadro de diálogo mientras la ingresa.



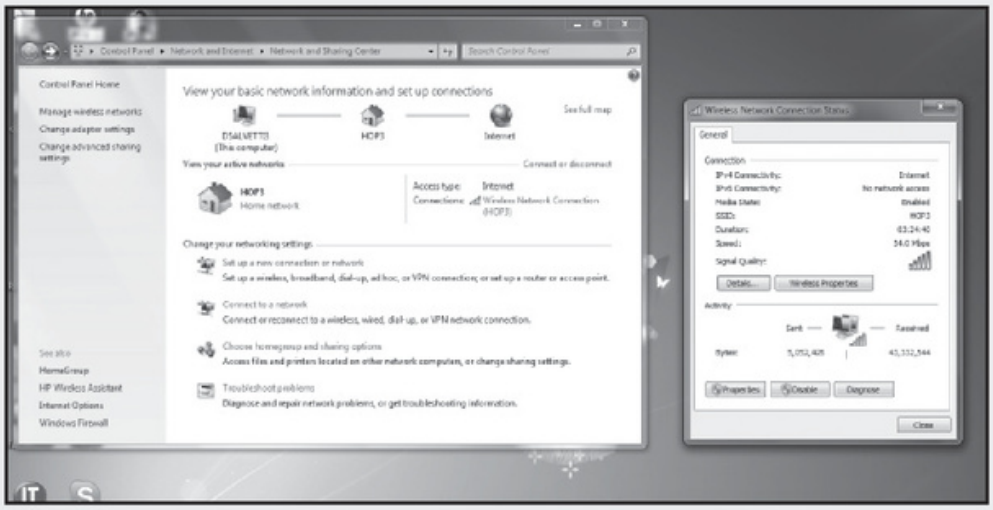
09 Si todo fue bien, estará conectado a la red inalámbrica y podrá verificar esto haciendo clic en el icono que muestra pequeñas barras en blanco en la parte inferior derecha del escritorio. El nombre de la red, en este caso HOP3, aparece resaltado y junto el estado de Conectado (Connected) confirma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



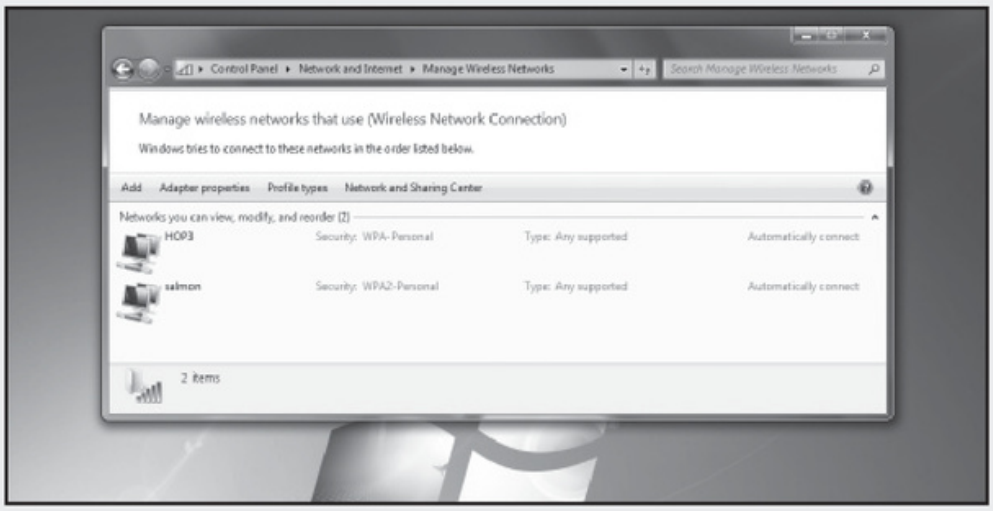
10 Vuelva al Centro de redes y recursos compartidos. Ahora puede ver en la parte central de la ventana que posee una conexión activa. Haga clic sobre el nombre de su red en la opción Conexiones (Connections) como muestra la imagen.



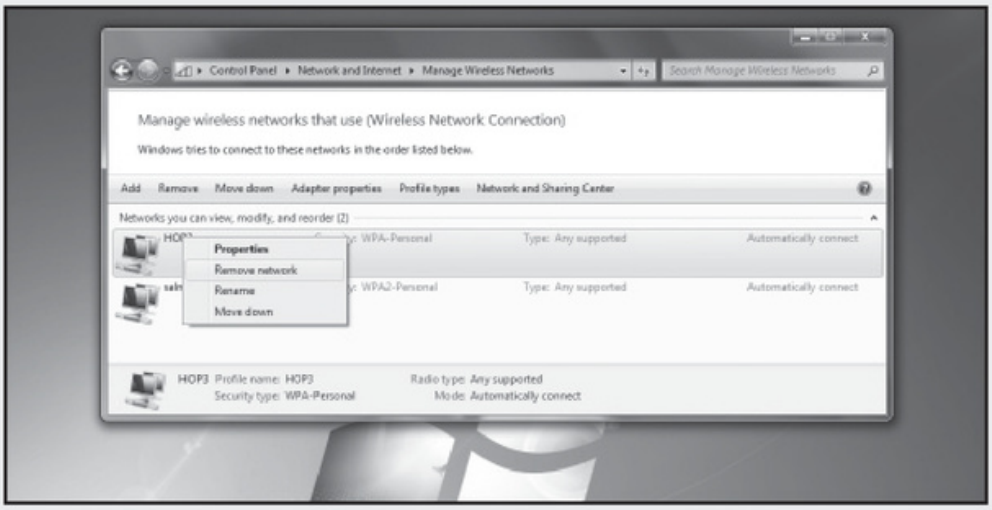
11 Se abrirá la ventana de Estado de su conexión inalámbrica (Wireless Network Connection Status) donde puede ver los parámetros más importantes de su red. Puede hacer clic en Detalles para obtener mayor información, si lo desea. El icono en Calidad de Señal (Signal Quality) le informa de manera práctica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



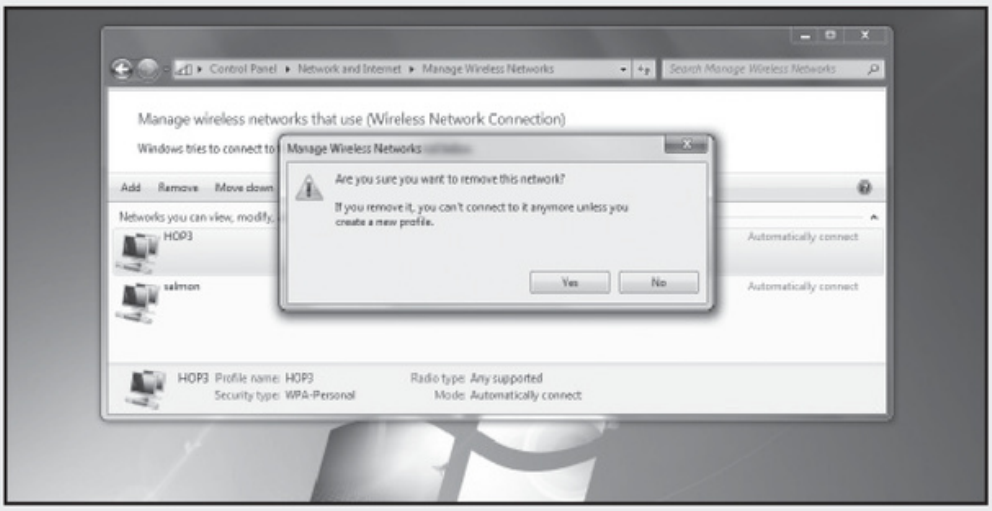
12 Cierre las ventanas anteriores y diríjase nuevamente al Centro de redes y recursos compartidos. Ahora haga clic en Administrar redes inalámbricas (Manage wireless networks) y verá la imagen siguiente. En esta ventana puede ver los Perfiles de redes (en este caso de redes inalámbricas), que son las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



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 red). A veces se necesita borrar los perfiles para evitar problemas y errores de la conexión causados por configuraciones existentes que no se usan. Haga clic con el botón derecho y seleccione `Quitar red` (`Remove network`) para eliminar el perfil.



14 Un cuadro de diálogo se abrirá y solicitará que confirme si usted 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. No se preocupe, que Windows creara el perfil de forma automática la próxima vez que se conecte a esa red (siempre que ingrese parámetros, como la contraseña, correctamente).



Configurar la red para compartir

Para compartir recursos entre computadoras que estarán conectadas a la misma LAN, tenemos que crear una red en el sistema operativo. Para iniciar las configuraciones tenemos que tener certeza de que nuestras placas de red en los clientes estén instaladas y correctamente configuradas. Además de los puntos de acceso que tengamos,verificaremos el buen funcionamiento de la conexión inalámbrica de cada PC. Es una práctica común configurar una clave para cada computadora cuando uno va a compartir recursos en red. En Windows 7 se hace mucho énfasis en todo lo relacionado con la seguridad, por este motivo, recomendamos configurar una clave de inicio de sesión para nuestra computadora. Para hacerlo nos vamos al **Panel de Control** y hacemos clic en la opción **Agregar o quitar cuentas de usuario** del menú **Cuentas de Usuario** (*User accounts*). En la nueva ventana podemos hacer clic en **Crear nueva cuenta de usuario** o **cambiar la configuración de una cuenta actual.**



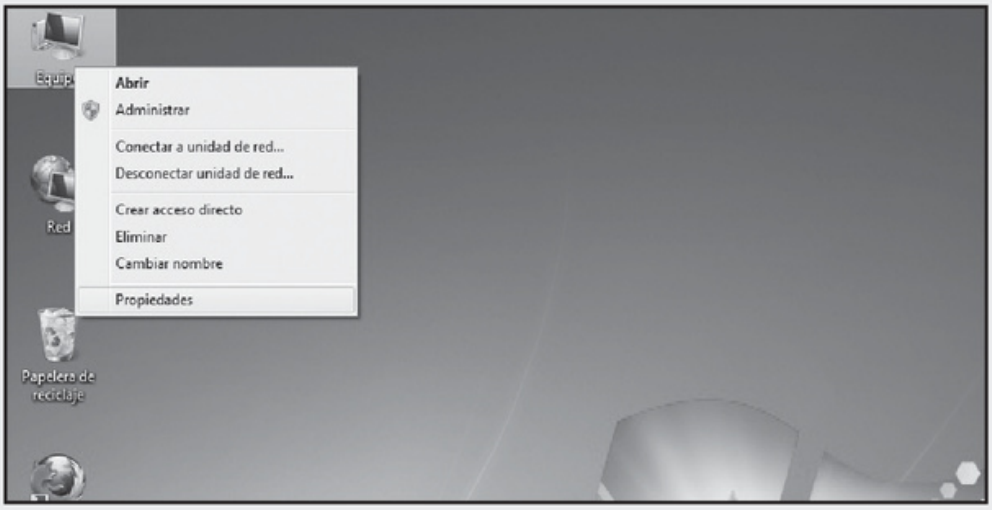
Figura 21. En la configuración de cuentas de usuario podemos cambiar las contraseñas, así como la imagen de nuestra cuenta.

PERFIL EN MEMORIA USB

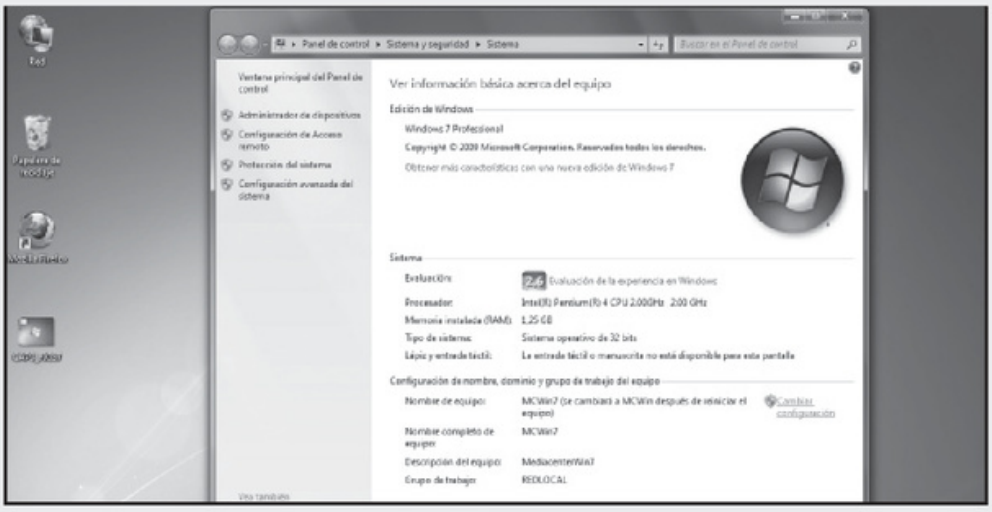
Tener el perfil de nuestra red en una memoria USB nos facilita instalar nuevas computadoras en nuestra red. Para hacerlo, seleccionamos nuestra red y hacemos clic derecho, seleccionamos **Propiedades** y en la pestaña Conexión hacemos clic en **Copiar este perfil de red a una unidad Flash USB**, seguimos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

CONFIGURAR LA RED PARA COMPARTIR

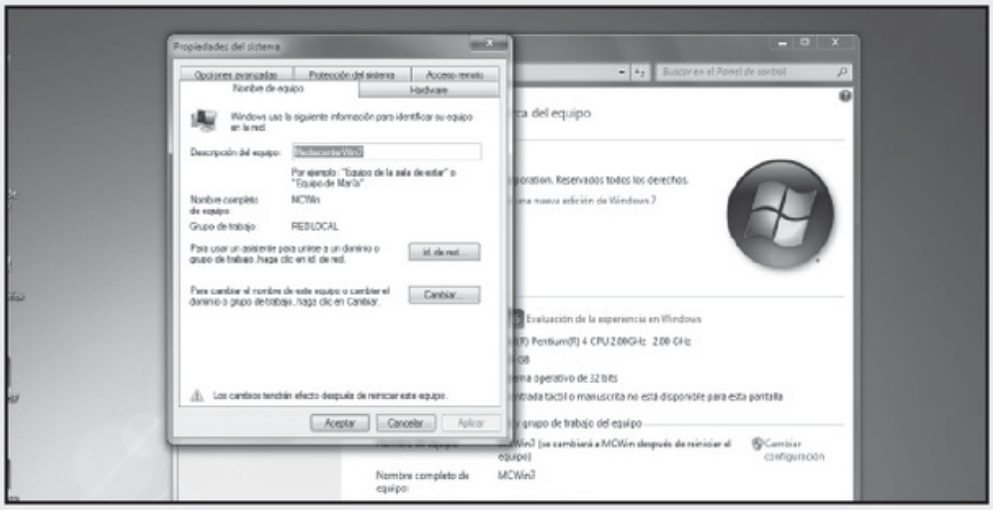
01 Diríjase al icono de Equipo (Computer) en su Escritorio y haga clic con el botón derecho del mouse. Seleccione Propiedades para abrir una ventana que mostrará información básica sobre su computadora.



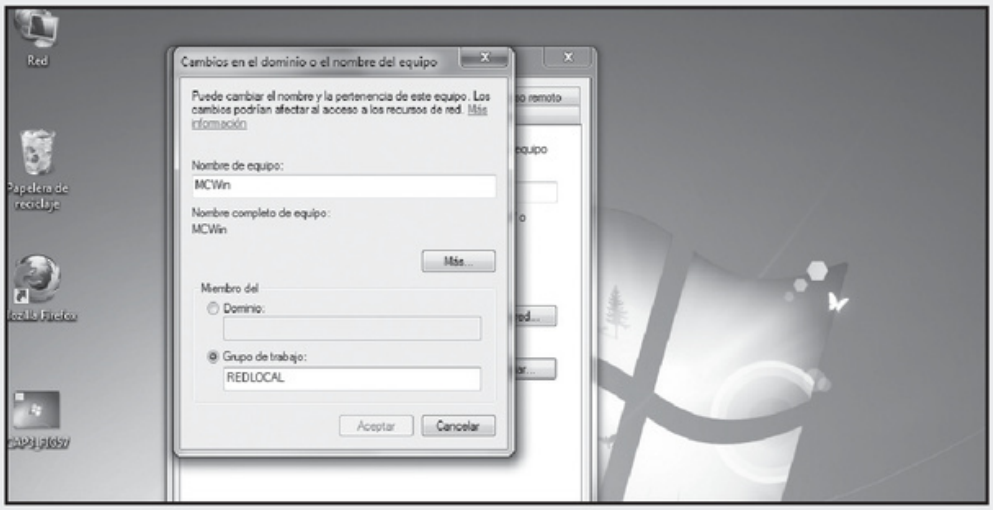
02 En esta ventana usted puede ver información sobre su hardware en la sección de Sistema (System) y datos sobre su grupo de trabajo. Además en la parte inferior se encuentra el número de producto de su Windows. Haga clic en Cambiar configuración (Change Settings), que se encuentra dentro de la información de grupo, a la derecha como muestra la imagen.



03 La nueva ventana mostrará las propiedades del sistema. En la pestaña Nombre del Equipo (Computer name) haga clic en Cambiar para modificar su configuración. Si usted desea puede agregar una descripción del equipo en ese campo para identificar su computadora en la red.



04 En este momento tiene que ingresar el identificador de su computadora en la red. Haga esto en Nombre de Equipo (Computer name) y además seleccione la opción Grupo de Trabajo en la parte Miembro de y escriba el nombre del grupo de trabajo que todos los miembros usarán, por ejemplo REDLOCAL. Hagaclic en Aceptar y luego un mensaje confirmará que tuvo éxito. El sistema solicitará que se reinicie la máquina.



05 Luego de reiniciar su computadora, ingrese nuevamente al `Panel de control`. Haga clic en `Redes e Internet`. Se abrirá una ventana como muestra la imagen. Debe hacer clic en `Grupo Hogar` (`Home group`) para poder cambiar la configuración de su red para compartir recursos.



06 Windows solicitará que seleccione qué ítems desea compartir en su red. Puede compartir Imágenes, Música, Videos, Documentos e Impresoras. Seleccione lo que necesite compartir y haga clic en `Siguiente`.



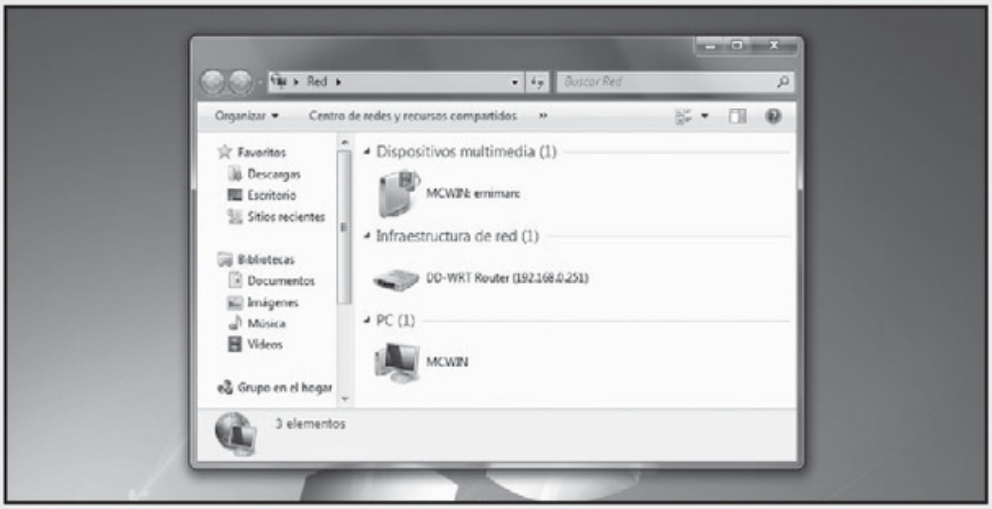
07 Para finalizar, el sistema operativo le recomendará usar una contraseña que debe anotar. Usará la contraseña para tener acceso a los archivos e impresoras de otros equipos que previamente agregará a su grupo de trabajo. Haga clic en `Finalizar` para terminar la configuración.



08 Si desea cambiar la contraseña por otra que usted quiera, vaya a `Panel de Control`, luego a `Grupo hogar` y haga clic en `Cambiar contraseña`. Ingrese la contraseña deseada y Windows luego le confirmará el cambio. Recuerde que su contraseña debe ser de 8 caracteres como mínimo y puede incluir letras y números.



09 Podrá ver los equipos compartidos si hace clic en el icono de Red (Network) en su escritorio, bajo el título Infraestructura de 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 formada por el punto de acceso y los usuarios ubicados dentro del área de cobertura se llama **Conjunto de servicio básico** o **BSS.** Decimos que se forma una

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.

célula. Cada BSS lo identificábamos con un BSSID (identificador de BSS) propio de cada célula.

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.



Figura 22. La figura muestra el cable UTP categoría 5 extendida que comúnmente encontramos en las redes cableadas.

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 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

INTERFAZ PCI

Con el objetivo de buscar alternativas al obsoleto bus **VESA** que tenía deficiencias, en 1992 la compañía Intel lideró la creación de un grupo de fabricantes de hardware que trabajaron en un nuevo estándar, el bus **PCI** (Peripheral Component Interconnect). Las primeras placas **PCI** aparecieron en 1993 con el lanzamiento de los procesadores Pentium.

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 nuestra placa de red, 192.168.1.10. Este vínculo lo realizamos por medio del **cable UTP**, que trae nuestro punto de acceso o uno similar que tengamos.

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**. Escribiremos la dirección IP estática 192.168.1.10 y la máscara de subred se completará automáticamente. No necesitaremos ningún otro parámetro, por lo tanto presionaremos en **Aceptar** para grabar la configuración y cerrar la ventana.

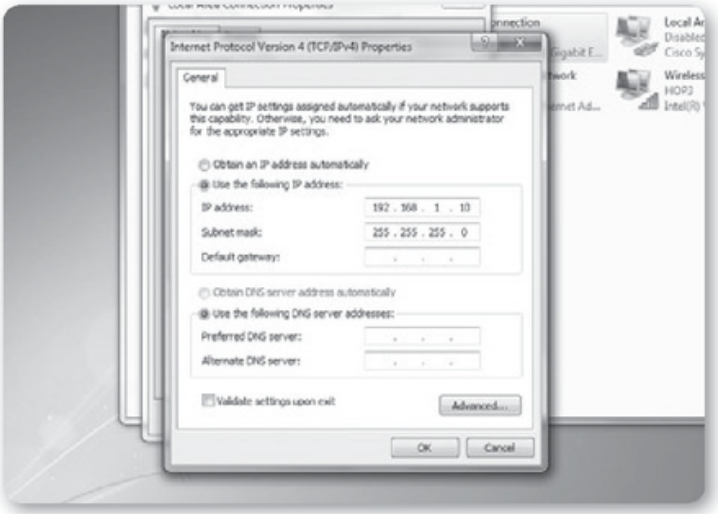


Figura 23. En este caso no necesitaremos configurar la puerta de enlace o DNS, solo una dirección IP en la misma subred.

Ahora abriremos el navegador web para ingresar a las configuraciones de nuestro 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 (recuerde que si el dispositivo nunca fue configurado, esta información viene por defecto y puede consultar su manual para obtener estos datos

de acceso). 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 realizaremos el proceso de configuración sin hacer uso de este asistente.

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** y cerrar la ventana.

Ahora ingresamos los parámetros para nuestro punto de acceso:

- SSID: escribimos el nombre que identificará a nuestra red. Usaremos HOP3 que es el nombre de la red en este ejemplo.
- Wireless channel: cambiamos el canal a 5.
- Wireless Network mode: vamos a usar G-only para trabajar a mayor velocidad con la norma IEEE 802.11g.

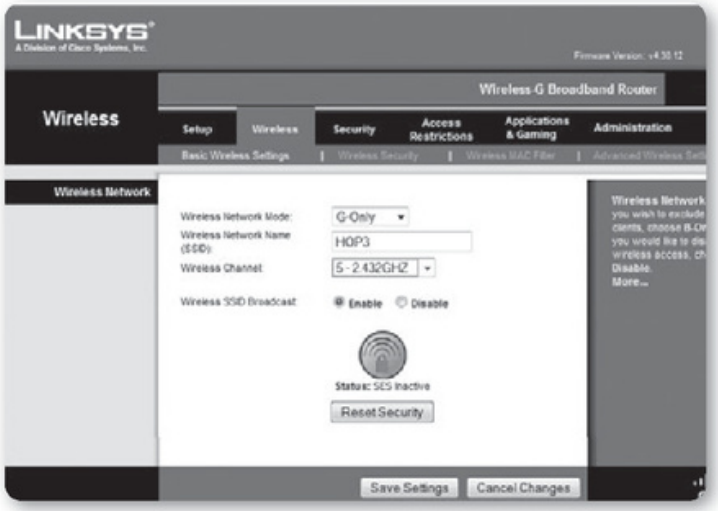


Figura 24. Podemos emitir nuestro SSID o no seleccionando **Enable** o **Disable** en la opción Wireless SSID Broadcast.

PCI NO ERA ESTÁNDAR

PCI 1.0 no era un estándar aprobado oficialmente por las autoridades de estandarización, solo era una especificación a nivel componente. PCI 2.0 fue el primer estándar establecido para conectores y ranuras de motherboards, se lanzó en 1993 y luego en 1995 salió el **PCI 2.1**. En 2004, el estándar **PCI Express serial**, que ofrece mejoras, se comenzó a incluir en motherboards para reemplazar a **PCI**.

En la pestaña **Wireless Security** de la imagen siguiente podemos configurar una contraseña de seguridad. Seleccionamos **WPA** o **WEP** e ingresamos la contraseña deseada en el campo **WPA Shared Key**.

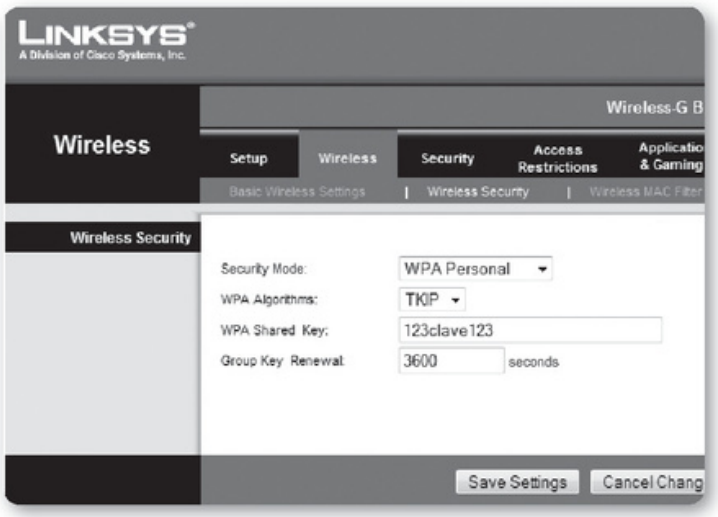


Figura 25. El campo WPA Algorithms permite modificar el algoritmo de encriptación que usará el AP para nuestra contraseña.

Hacemos clic en el botón **Save Settings** (guardar configuración) para aplicar los cambios. El equipo se reinicia y ya tenemos configurado nuestro punto de acceso en nuestra red.

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 conocimientos.

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 estoy 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 **Aceptar**.

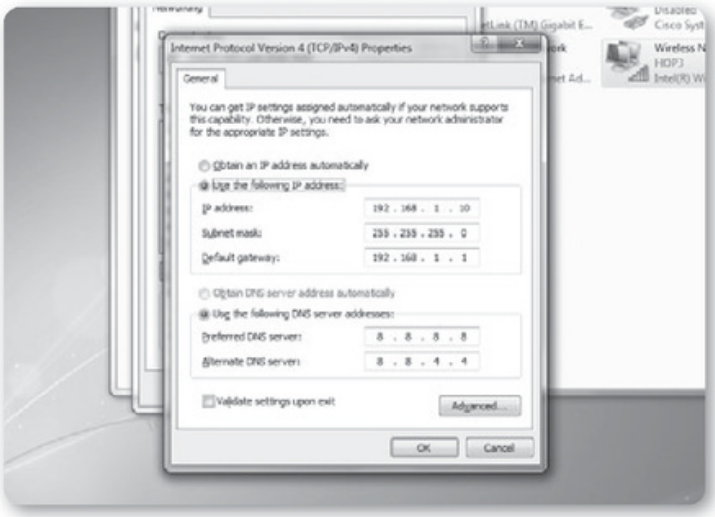


Figura 26. Podemos usar cualquier servidor de DNS. Nuestro ISP puede facilitarnos esos datos si no queremos usar DNS públicos.

Solo resta que nos conectemos a la red inalámbrica que hemos creado en el punto de acceso. Para hacerlo buscamos el icono de notificación de redes en la parte inferior derecha de la pantalla donde hacemos clic. Seleccionamos el nombre de nuestra red y hacemos clic en **Conectar**. Recordemos que se nos solicitará la contraseña si configuramos esto en el AP.

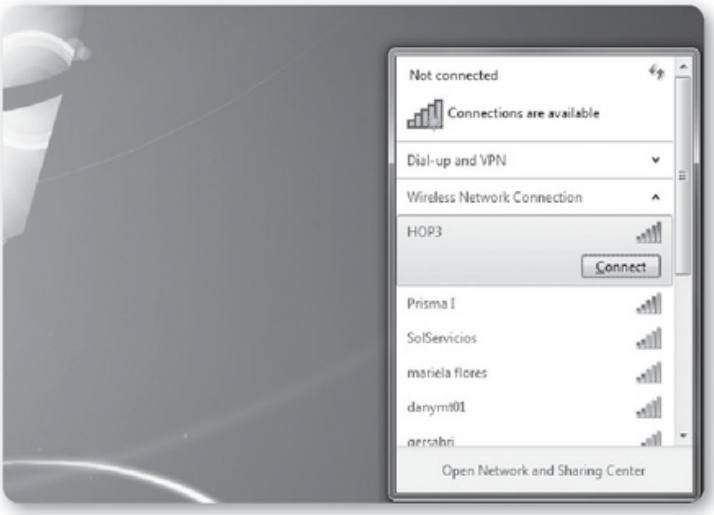


Figura 27. Si hacemos clic en el icono de redes veremos la lista de redes disponibles que detecta nuestra placa inalámbrica.

Una vez confirmada la correcta conexión a nuestra red, podemos apreciar en la ventana de conexiones inalámbricas que estamos vinculados a nuestro punto de acceso. Si alguna vez fuera necesario cambiarnos de red inalámbrica, nos podemos desconectar simplemente haciendo clic en la red a la que estamos conectados y luego presionando **Desconectar** desde la barra de menu.

Configuración de una red inalámbrica AD HOC

Una conexión ad hoc es una conexión temporal entre computadoras y dispositivos usada para un fin específico como, por ejemplo, compartir archivos o participar en juegos en red de varios jugadores. Además, es posible compartir temporalmente una conexión a Internet con otros usuarios de la red ad hoc. De este modo los usuarios no tienen que configurar sus propias conexiones a Internet. Las redes ad hoc solo pueden ser inalámbricas, de modo que cada cliente deberá contar con una placa de red inalámbrica correctamente instalada y configurada para unirse a esta red.

En este tipo de configuración no usamos un punto de acceso, lo único que debemos configurar son las placas de red inalámbricas de las computadoras que deseamos conectar. Como mínimo deberán ser 2 computadoras. En todos los clientes configuraremos una dirección IP estática de forma manual en el mismo segmento de red (o sea, en la misma subred de trabajo). También cada computadora tendrá un nombre de equipo y un grupo de trabajo en común.



DESCONEXIÓN AUTOMÁTICA

Una red **ad hoc** se elimina automáticamente después de que todos los usuarios se desconectan de la red o cuando la persona que la configuró se desconecta y sale del área de cobertura de los otros usuarios de la red. Todo esto ocurre salvo que el creador de la red decida convertirla en una red permanente al momento de crearla y guardar la configuración.

Básicamente, en un cliente configuraremos la red inalámbrica (se comporta como un AP) y las otras se conectarán a esta.

Vamos al **Centro de redes y recursos compartidos** y hacemos clic en **Administrar redes inalámbricas** (*Manage wireless networks*). En esta ventana seleccionamos **Agregar** (*Add*)

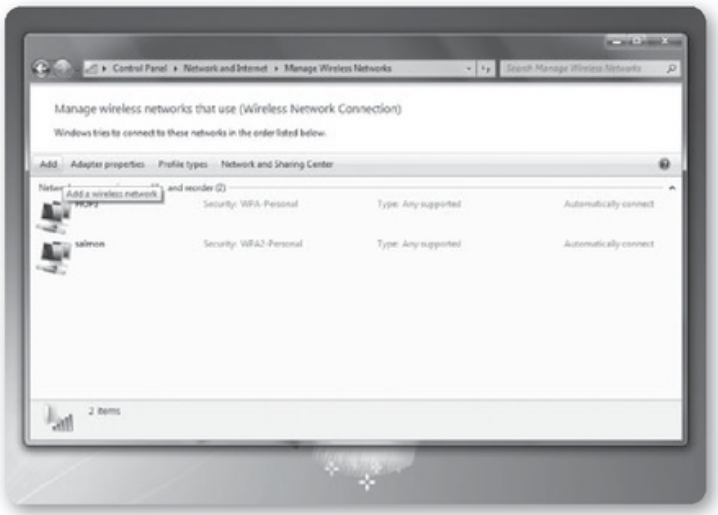


Figura 28. Crearemos nuestra red ad hoc en la misma ventana que nos permitía modificar los perfiles de nuestras redes.

En la nueva ventana que se abre hacemos clic en **Crear una red ad hoc** (*Create an ad hoc network*) y seguimos el asistente de instalación. Es muy sencillo y solamente nos preguntará el nombre de la red (SSID), el tipo de seguridad (podemos seleccionar WPA, WEP o sin seguridad) y, en caso de usar contraseña, tendremos que ingresar una palabra clave. Tildamos la opción **Guardar esta red** y hacemos clic en **Siguiente**.Luego de que se configure la red, aparecerá el aviso de confirmación de la correcta creación de nuestra red ad hoc. Además Windows nos informa que ingresando al Centro de redes y recursos compartidos, seleccionando la opción **Cambiar configuración de uso compartido avanzado** (*Change advanced sharing settings*) podemos configurar nuestro sistema para compartir archivos.

> LA PUERTA DE ENLACE ES LA DIRECCIÓN IP DE NUESTRO PUNTO DE ACCESO

Ahora solo resta conectarnos a la red ah hoc creada (buscar el nombre de red o SSID que ingresamos) e introducir la contraseña (si es que configuramos la seguridad para nuestra red).

Configuración de Internet en una red AD HOC

Ahora veremos cómo compartir la conexión a Internet por medio de una red ad hoc entre dos computadoras. Pongamos como ejemplo el siguiente escenario. Supongamos que tenemos dos computadoras (PC1 y PC2) y una conexión por cable a Internet. Ambas computadoras tienen placas inalámbricas instaladas y configuradas funcionando, pero no tenemos un dispositivo inalámbrico (router o AP). Lo que queremos es que ambas computadoras tengan acceso a Internet por medio de la única conexión cableada existente. Vamos a solucionarlo usando la conexión por cable a la PC1 y creando una red ad hoc en esta. Luego vamos a configurar la PC2 para que se conecte a la nueva red ad hoc creada.

1. Empecemos por conectar el cable que nos provee Internet a la placa de la PC1. Verifiquemos que tengamos conexión a Internet por medio de este vínculo cableado.

2. Ahora hagamos clic en el ícono de Windows (**Inicio**), escribamos **Ver conexiones de red** (*View network connections* si es que tenemos el sistema operativo en inglés) y presionemos **Enter**.

3. Identifiquemos nuestra conexión de área local (conexión cableada a Internet) y la conexión inalámbrica. En nuestro caso, para la PC1, la conexión cableada a Internet se llama Conexión de área local y la placa inalámbrica se llama Conexión de red inalámbrica.

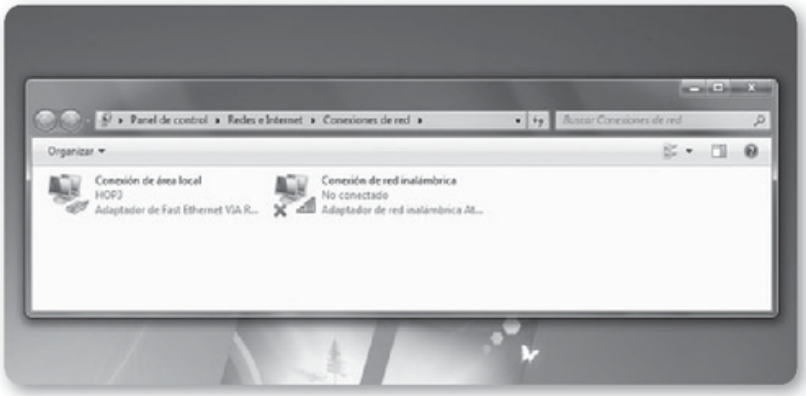


Figura 29. Tengamos en cuenta que los nombres de nuestras conexiones pueden cambiar en otros equipos.

4. Hacemos clic derecho con el mouse sobre la conexión cableada y seleccionamos **Propiedades**, entre las opciones que tenemos.

5. En la nueva ventana que se abre tendremos dos pestañas, hacemos clic en **Uso compartido** (*Sharing*). Tildamos la opción **Permitir que los usuarios de otras redes se conecten a través de la conexión de Internet de este equipo** (*Allow other network users to connect through this computer´s Internet connection*). Presionamos en **Aceptar** para guardar la configuración y continuar.

6. Ahora vamos a crear la red ad hoc como vimos anteriormente. Tengamos en cuenta el nombre de red usado y si configuramos o no una contraseña de acceso a la red.

7. Hagamos clic en el icono de redes en la esquina inferior derecha para asegurarnos que estamos conectados a la red creada (llamada PRUEBA) en la PC1 de este ejemplo.

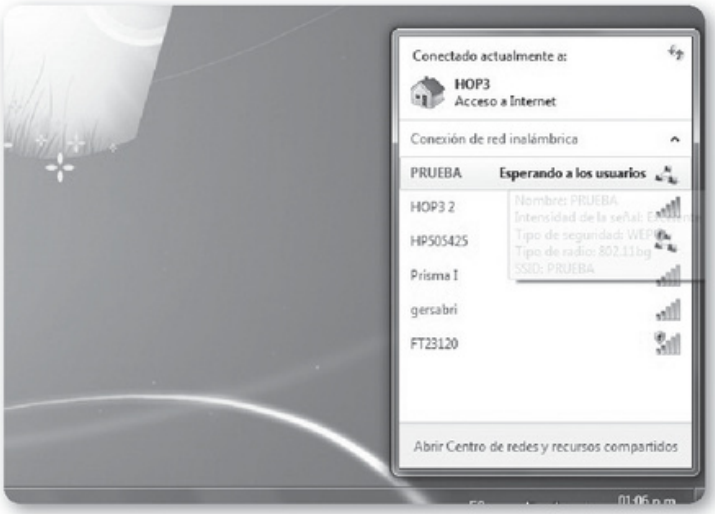


Figura 30. Nuestra red ad hoc figura con el estado de conectado y esperando usuarios.

INTERNET PARA TODOS

Cuando configuramos una red **ad hoc** en nuestra computadora, compartimos la conexión a Internet y si, a continuación, alguien se conecta a nuestra computadora con otro usuario (usando el cambio rápido de usuario de Windows 7), seguiremos compartiendo la conexión a Internet, aunque no tuviésemos la intención de hacerlo con esta persona. Hay que estar atentos a estos cambios para poder administrar nuestros recursos correctamente.

8. Terminamos las configuraciones en la PC1 y procedemos a configurar la PC2. Vamos al icono de redes en la PC2 e identificamos el SSID de nuestra red ad hoc.

9. Seleccionamos la red y hacemos clic en **Conectar**. El sistema operativo nos solicitará que ingresemos la contraseña, si configuramos una en el paso correspondiente.

Cuando terminemos de compartir los recursos, podremos deshabilitar la configuración, creada para compartir Internet con la red ad hoc, en la PC1. Si no realizamos esto, nuestra conexión inalámbrica no funcionará en la PC1. Para deshabilitar la configuración, seguimos los pasos 1 al 5 para la PC1, pero debemos destildar la opción **Permitir que los usuarios de otras redes se conecten a través de la conexión de Internet de este equipo** (*Allow other network users to connect through this computer´s Internet connection*).

Con estos simples pasos podemos compartir la conexión de Internet entre dos o más computadoras creando una simple red ad hoc.



RESUMEN

Vimos varios temas en este capítulo, primero hablamos del hardware necesario y podemos concluir que el principal punto a tener en cuenta para la instalación de hardware 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: modo infraestructura y modo ad hoc. En este último, configuramos la red para compartir la conexión a Internet.

Actividades

TEST DE AUTOEVALUACIÓN

1	¿Cuáles son las dos situaciones en las que debemos prestar especial atención cuando estamos por instalar el cliente inalámbrico?
2	¿Cuáles son las tres formas que describimos en el texto para instalar los drivers de nuestra placa inalámbrica?
3	¿De qué manera se identifican los zócalos de expansión en un motherboard?
4	¿Qué evitamos usando una pulsera antiestática cuando abrimos nuestro gabinete?
5	¿Cómo podemos ver información básica de las redes disponibles?
6	¿De qué manera llamamos a 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 obtenemos al ejecutar el comando ipconfig en una consola?
9	¿Por qué motivo podríamos querer cambiar nuestros servidores de DNS y usar DNS públicos y gratuitos?
10	¿Si queremos compartir temporalmente archivos entre dos computadoras, qué tipo de red configuraremos, ad hoc o infraestructura?

*04

Seguridad en la red

Estudiaremos los principales conceptos sobre seguridad informática, partiremos de conceptos básicos 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. Nos dedicaremos a conocer las amenazas más frecuentes que pueden afectar nuestra red.

▾ **¿Seguridad inalámbrica? 152**

▾ **¿A que llamamos seguridad de la información? 154**

Confidencialidad 157
Autenticación 158
Integridad 158
Disponibilidad 159
No repudio 160

▾ **Seguridad de la información + WLAN 160**

Atributos de seguridad 161
Confidencialidad en WLAN 162
Autenticación en redes inalámbricas 168
Integridad de datos en WLAN 173
Disponibilidad en WLAN 174
No repudio en redes inalámbricas .. 175

▾ **Las 10 amenazas más comunes 175**

▾ **Resumen 177**

▾ **Actividades 178**

¿Seguridad inalámbrica?

La utilización del aire como medio de transmisión de 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 esta forma se estaría interceptando nuestra red inalámbrica.

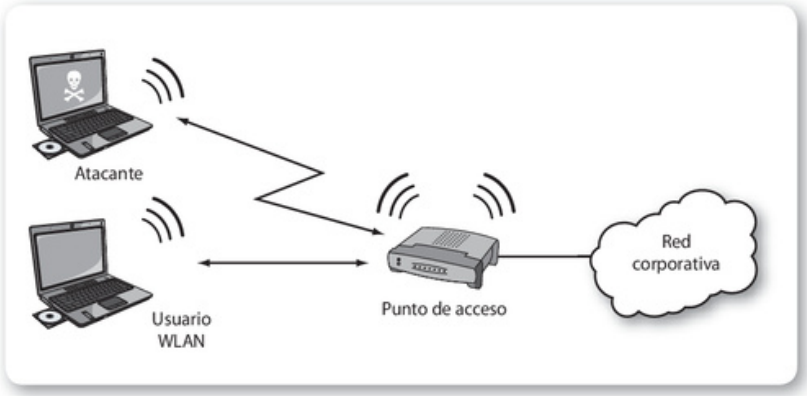


Figura 1. El atacante de una red inalámbrica tiene en sus manos información privada que no le pertenece al ingresar a nuestra red.

EMULADOR DE MÁQUINA ENIGMA

Para simular el funcionamiento de una máquina de escribir **Enigma** se puede ingresar en **http://enigmaco.de/enigma/enigma.swf**, donde usando tres rotores podemos ver el camino que recorre cada letra. Al teclear el texto, este es automáticamente cifrado (o descifrado) y se permite configurar las claves, los rotores y sus posiciones iniciales.

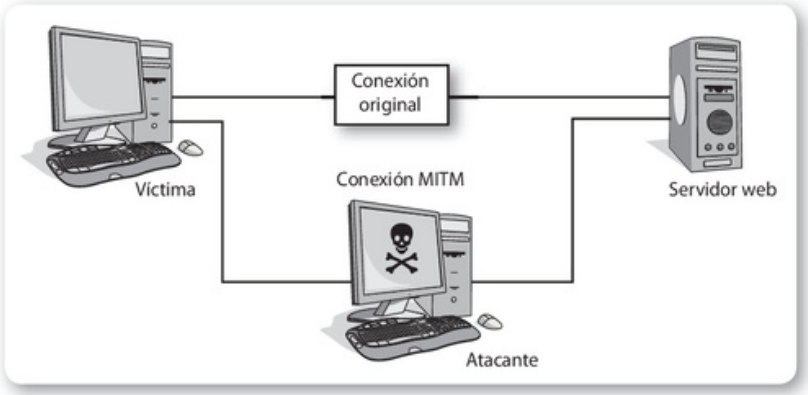


Figura 2. Vemos cómo el atacante recibe la información que intercambian las victimas sin que estas se den cuenta.

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 (en general 2.4 GHz).

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 ofrece servicios o comparte archivos en la red. Algo muy utilizado también es la posibilidad de duplicar las direcciones IP o MAC de clientes legítimos de la red.

Cualquier punto de acceso puede estar expuesto a un ataque de **fuerza bruta** (*brute force attack*). Este es un término utilizado en criptografía, que se define como un procedimiento para recuperar una clave probando todas las combinaciones posibles hasta encontrar la que permite el acceso. Estos ataques demandan gran cantidad de tiempo, ya que se utiliza un método de prueba y error. Así una configuración incorrecta o descuidada de nuestro punto de acceso dejará el camino libre para que nuestra red inalámbrica sea invadida por personas que no tienen autorización.

No podemos definir la palabra **seguridad** sin tener en cuenta el ámbito en el que nos estamos manejando. Esta palabra abarca un amplio rango de campos dentro y fuera del ámbito de la informática o computación. Se puede hablar de seguridad cuando describimos las

medidas de seguridad en una ruta o cuando decimos que un nuevo sistema operativo que vamos a utilizar en nuestras computadoras es seguro contra virus. En realidad se desarrollaron varias disciplinas para abordar cada uno de los aspectos de la seguridad.

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 la información en redes inalámbricas**.

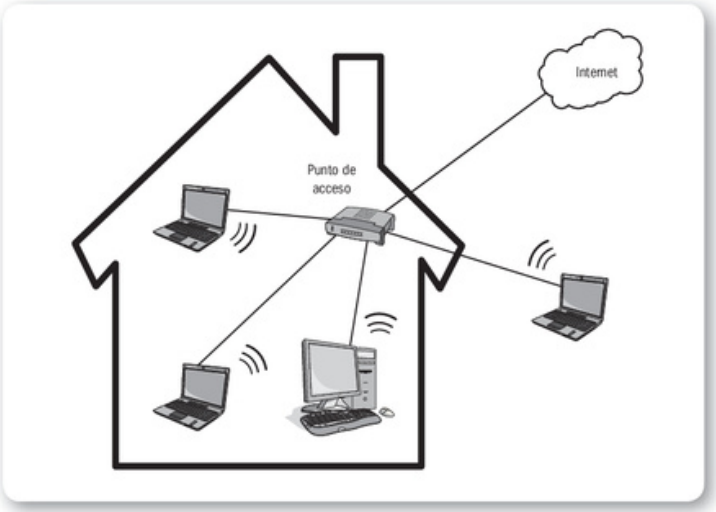


Figura 3. Nuestro enfoque de la seguridad nos dará las pautas para proteger la información que estamos intercambiando en nuestra red.

¿A qué llamamos seguridad de la información?

Decimos que la **seguridad de la información** abarca todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permiten proteger la información. Se busca mantener tres aspectos básicos, que son la **confidencialidad**, la **disponibilidad** y la **integridad** de la información.

Es común que confundamos el concepto de seguridad de la información con el de **seguridad informática**. Este último solamente se encarga de la seguridad en el medio informático, por medio de estándares.

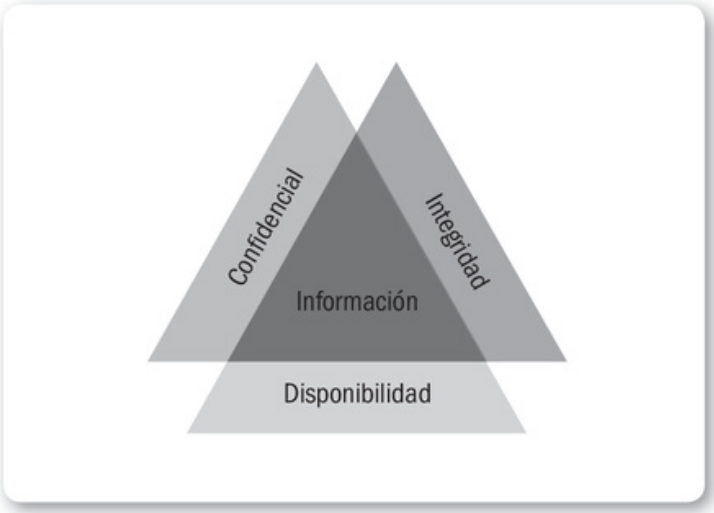


Figura 4. Una buena estrategia de seguridad se basa en mantener la confidencialidad, la disponibilidad y la integridad de los datos.

El manejo de la seguridad de la información se basa en la tecnología.

Si nos situamos en el ámbito de una empresa, proteger la información es indispensable para obtener ventajas y poder sobre otras personas o empresas. A la información se la conoce como:

- Crítica: es indispensable para la operación de la empresa.
- Valiosa: es un activo de la empresa con alto valor.
- Sensitiva: debe ser conocida por las personas autorizadas.

Existen dos palabras importantes en la seguridad informática que son:

- Riesgo: es todo tipo de vulnerabilidades o amenazas que pueden ocurrir sin previo aviso y provocar pérdidas en la empresa.
- Seguridad: es una forma de protección contra los riesgos.

Los términos **seguridad de la información**, **seguridad informática** y **garantía de la información** son usados con frecuencia como sinónimos y aunque su significado no es el mismo, todos tienen una misma finalidad al proteger la confidencialidad, la integridad y la

MÁQUINA ENIGMA

La protección de la información siempre fue un ideal a alcanzar por el hombre. En la Segunda Guerra Mundial, Alemania utilizó mucho a Enigma, una máquina de escribir que tenía un mecanismo de cifrado rotativo. Era fácil de manejar y supuestamente inviolable. La maquina electromecánica de cifrado rotativo fue un invento militar.

disponibilidad de la información. Entre estos términos existen algunas diferencias sutiles que radican principalmente en el enfoque, las metodologías utilizadas y las zonas de aplicación.

La seguridad de la información se refiere a la confidencialidad, integridad y disponibilidad de la información y datos, independientemente de la forma que los datos puedan tener (por ejemplo, medios impresos, electrónicos, audio u otras formas).

Se involucra también la implementación de estrategias que cubran los procesos en donde la información es el activo principal. Las estrategias deben establecer políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo la información.

La seguridad es un proceso continuo de mejora por lo que las políticas y controles establecidos para la protección deberán revisarse y adecuarse ante los nuevos riesgos que aparezcan. De esta forma los reduciremos y en el mejor de los casos lograremos eliminarlos por completo.



Figura 5. El análisis de los resultados de nuestra seguridad es la base para poder mejorar las políticas planteadas.

De manera sintética decimos que la gestión de la seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información. Si alguna de estas características falla no estamos ante nada seguro y nuestro sistema correrá serios riesgos en su seguridad.

Confidencialidad

La confidencialidad es la propiedad de asegurar que la información no sea divulgada a personas, procesos o dispositivos no autorizados. Un ejemplo sería analizar cuando se lleva a cabo una transacción de tarjeta de crédito en Internet. En esta transacción se requiere que el número de tarjeta de crédito sea transmitido desde el comprador al comerciante y del comerciante a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el **cifrado** del número de tarjeta y los datos que contiene la banda magnética durante la transmisión. El problema aparece si una parte no autorizada obtiene el número de la tarjeta de alguna forma, así se habría producido una **violación de la confidencialidad**.



Figura 6. Sitios como PayPal.com o Moneybrookers.com nos permiten realizar operaciones con nuestra tarjeta de crédito de forma segura.

Hay muchas formas en las que la pérdida de la confidencialidad de la información se manifiesta. Cuando se publica información privada, cuando perdemos un pen drive con información privada o inclusive cuando alguien mira por encima de nuestro hombro cuando tenemos

información confidencial en una pantalla (e-mail, cajero automático, etc.). Estos y muchos otros casos pueden constituir una violación de la confidencialidad. Nuestro objetivo es estar atentos y solucionar estos inconvenientes.

Autenticación

Es una medida de seguridad diseñada para establecer la validez de una transmisión, mensaje o remitente. También podemos considerar que es un medio para verificar la autorización de un individuo para recibir categorías específicas de información.

Así la autenticidad nos garantiza que quien dice ser el Sr. X es realmente el Sr. X. Es decir, que implementamos mecanismos para verificar quién está enviando la información.

Integridad

Dado que es necesario proteger la información contra la modificación no permitida del dueño, implementamos la característica de conservar la integridad de la información. Así, buscamos mantener los datos libres de modificaciones no autorizadas.

La violación de la integridad se presenta, por ejemplo, cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra datos importantes que forman parte de la información privada de una empresa.

Cuando se trabaja en una red, debemos comprobar que los datos no sean modificados durante su transferencia. La integridad de un mensaje la podemos obtener, por ejemplo, adjuntándole otro conjunto de datos de comprobación de la integridad: la **firma digital**.



PERDER INTEGRIDAD

La integridad también se refiere a la corrección y completitud de los datos en una **base de datos**. Esta puede perderse añadiendo datos no válidos (por ejemplo, al pedir un producto inexistente) o modificando datos existentes con un valor incorrecto. Además un fallo en el suministro de energía puede hacernos perder datos y así la integridad de estos.

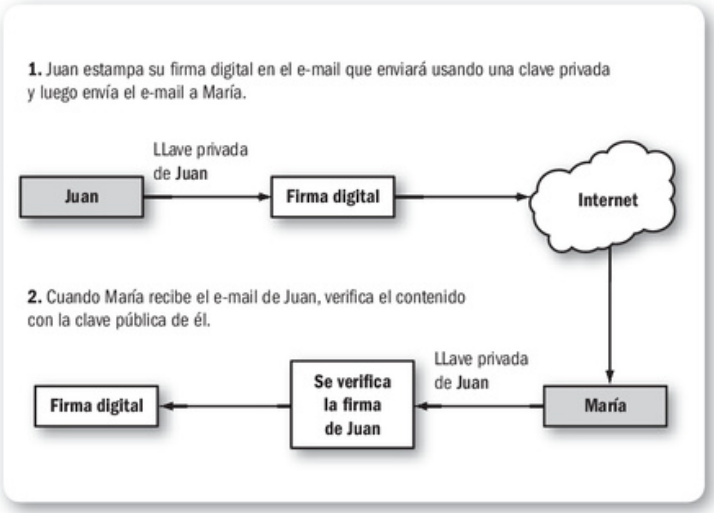


Figura 7. La firma digital es uno de los pilares fundamentales de la seguridad de la información hoy en día.

De forma resumida, podemos decir que una función de **hash** es un algoritmo matemático que nos da un resultado B al aplicarlo a un valor inicial A. En informática, una función o algoritmo hash es un método o función para generar claves o llaves que representen de manera casi unívoca a un documento, archivo o similar.

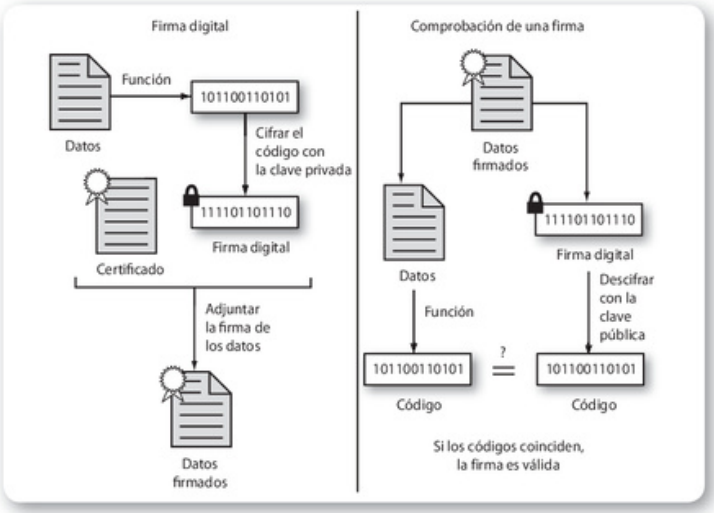


Figura 8. Esquema de comprobación de la firma digital usando funciones específicas.

Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean procesos, personas o aplicaciones.

Podemos decir que es el acceso oportuno y confiable a datos y servicios de información para usuarios que tengan acceso autorizado.

Tener sistemas que estén disponibles en todo momento y evitar interrupciones del servicio debido a cortes de energía, fallas de hardware y actualizaciones del sistema nos garantizan **alta disponibilidad** de la red. En nuestro caso, garantizar la disponibilidad implica también la prevención de ataques a la red inalámbrica como el tan famoso ataque de **denegación de servicio** (DoS).

No repudio

El **no repudio** (*non-repudiation*) evita que el emisor o el receptor nieguen la transmisión de un mensaje. Con esta expresión hacemos referencia a la capacidad de afirmar la autoría de un mensaje o información, evitando que el autor niegue la existencia de su recepción o creación. Por ejemplo, cuando se envía un mensaje, el receptor puede comprobar que efectivamente el supuesto emisor envió el mensaje. De la misma forma, cuando se recibe un mensaje, el emisor puede verificar que el supuesto receptor recibió la información. Así, se puede probar la participación de las partes en una comunicación.

Seguridad de la información + WLAN

El concepto de seguridad de sistemas de información lo definimos 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, etapa de procesamiento o tránsito. Además, la protección contra la negación de servicio a los usuarios autorizados o la provisión de servicio a usuarios no autorizados. Por último se incluyen las medidas necesarias para detectar, documentar y contabilizar esas amenazas. La seguridad inalámbrica la presentamos desde el punto de vista de la seguridad de los sistemas de información. Teniendo en mente los cinco atributos de seguridad podremos implementar y diseñar redes 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 capa usa únicamente la funcionalidad de la capa 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)

Recordemos que solamente estamos examinando los mecanismos de seguridad en las capas 1 y 2. Otros mecanismos de seguridad de nivel 3 y superiores son parte de la seguridad implementada en las capas de red o aplicación. Muchos se estarán preguntando ¿qué es el **cifrado** en el nivel de enlace? Bien, básicamente podemos decir que es el proceso de asegurar los datos cuando son transmitidos entre dos nodos de una red instalados sobre el mismo enlace físico (también podemos considerar el caso de dos enlaces diferentes mediante un repetidor, por ejemplo, un satélite). Con este cifrado a nivel de enlace, cualquier otro protocolo o aplicación de datos que se ejecute sobre el mismo enlace físico queda protegido de intercepciones.

El proceso requiere una clave secreta compartida entre las partes y un algoritmo previamente acordado. En caso de que el transmisor y el receptor no compartan el medio de transporte, la información debe ser descifrada y cifrada nuevamente en cada uno de los nodos en su camino al receptor. El cifrado en este nivel de enlace se usa en caso de que no se aplique un protocolo de mayor nivel.

En nuestro estándar IEEE 802.11, el algoritmo de cifrado más conocido es el llamado Privacidad Equivalente a Cableado o **WEP** (*Wired Equivalent Privacy*). Desde hace mucho tiempo está probado que WEP es inseguro, hoy en día existen otras alternativas como el protocolo **WPA**, que veremos más adelante en este capítulo.

Confidencialidad en WLAN

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

Nuestro objetivo es asegurar 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 (*Wi-Fi Protected Access*) son los estándares usados por la mayoría de los dispositivos inalámbricos hoy en día. Analizando estos dos estándares, WPA es muy superior en todos los aspectos y debemos usarlo siempre que sea posible.

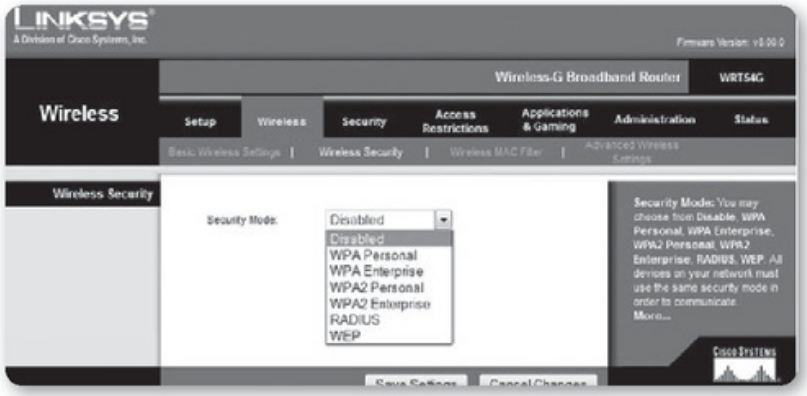


Figura 9. En redes inalámbricas existen dos métodos básicos de cifrado WEP y WPA, que podemos elegir.

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 original 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 por cualquier persona.

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 a este protocolo como obsoleto. Originalmente usaba claves de codificación de 40-bit de longitud, que luego fueron extendidas a 104-bit por preocupación en los estándares de seguridad. Esto último más que una solución fue un arreglo sobre la marcha, ya 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.

No fueron solamente las fallas de diseño las que hicieron que WEP fuera obsoleto. La falta de un sistema de manejo de claves como parte del protocolo también contribuyó para su fracaso. WEP no tenía incluido sistema alguno para solventar esto. La clave usada para codificar o decodificar se distribuía de forma muy simple. Solamente había que teclear manualmente la misma clave en cada dispositivo de la red inalámbrica y se tenía acceso.

Si tenemos un secreto y lo compartimos con muchos, deja de ser un secreto. De todas formas tener una red con WEP es mejor que tenerla sin ningún tipo de protección, por lo menos usando esta codificación tendremos a nuestros vecinos fuera de nuestra red.

Luego de WEP, aparecieron varias extensiones de carácter propietario que resultaron también inadecuadas, por ejemplo **WEP Plus** de Lucent y **WEP2** de Cisco (todas obsoletas al día de hoy).

Luego de WEP, nacen WPA y WPA2

WPA (Acceso Protegido Wi-Fi) 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 WEP 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 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, al WPA2 se le 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*). Este protocolo cambia claves dinámicamente a medida que el sistema es utilizado por el usuario.

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, 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**

RADIUS (acrónimo en inglés 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 es 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.

Con este tipo de servicio estamos permitiendo que las organizaciones centralicen su autentificación, autorización y administración.

A continuación, vamos a ver un poco más en detalle todo esto. Definimos tres tipos de entidades:

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

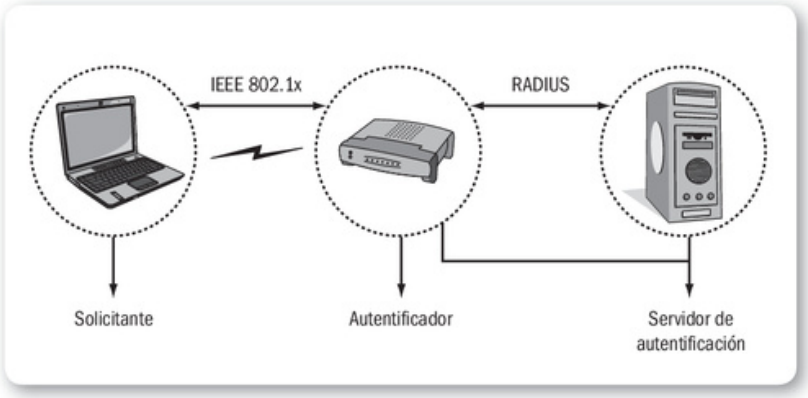


Figura 10. Ejemplo de una red inalámbrica donde hacemos uso de WPA-RADIUS. Podemos identificar las entidades que actúan.

Describamos el proceso de autentificación para este modo de funcionamiento de WPA. Analicemos en un gráfico cómo se realiza este

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 y se pueden bajar de Internet.

proceso, además veamos a modo informativo los mensajes que se intercambian para concretar la autenticación. Los protocolos que aparecen y no tratamos no los consideramos como fundamentales para el objetivo de este libro y por eso no los desarrollamos.

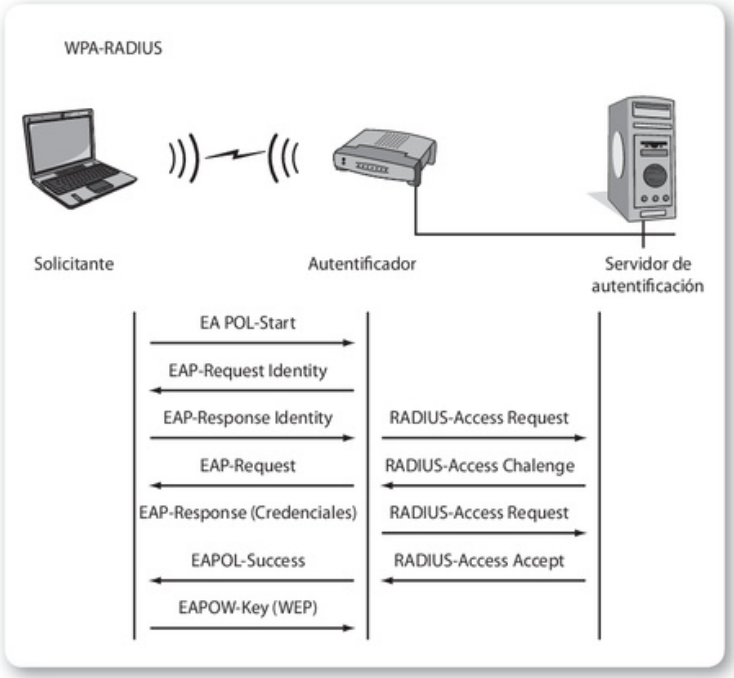


Figura 11. Ejemplo de una red inalámbrica donde hacemos uso de WPA-RADIUS. Podemos identificar los protocolos que actúan.

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 autentificación en tramas de gestión (paquetes de información que se envían para realizar ciertas 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 envía la identidad del cliente al servidor de autentificación mediante **EAP** (*Extensible Authentication Protocol*).

7) El cliente y el servidor de autentificación establecen un diálogo mediante el protocolo EAP de inicio.

8) Finalizado este diálogo, el solicitante y el servidor de autentificación comparten una clave de sesión que nunca ha viajado por la red hasta este momento.

9) El servidor de autentificación 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 de la red.

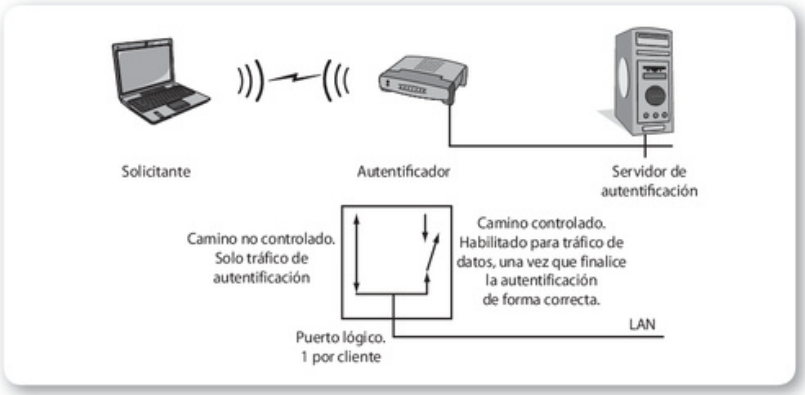


Figura 12. Vemos el esquema equivalente en el proceso de autentificación si usamos WPA-RADIUS.

• **WPA-PSK** (*Pre Shared Key*)

Destinado para entornos en los que no hay disponible un servidor de autentificación y en los cuales no es necesario llegar al mismo nivel de seguridad que los usados en las comunicaciones corporativas. Podemos hacer uso de este modo en nuestros hogares, oficinas pequeñas o en lugares donde la seguridad no es un tema demasiado importante para nosotros.

El principio de funcionamiento de este sistema 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, no hay un mecanismo estándar para modificar esta clave secreta compartida.

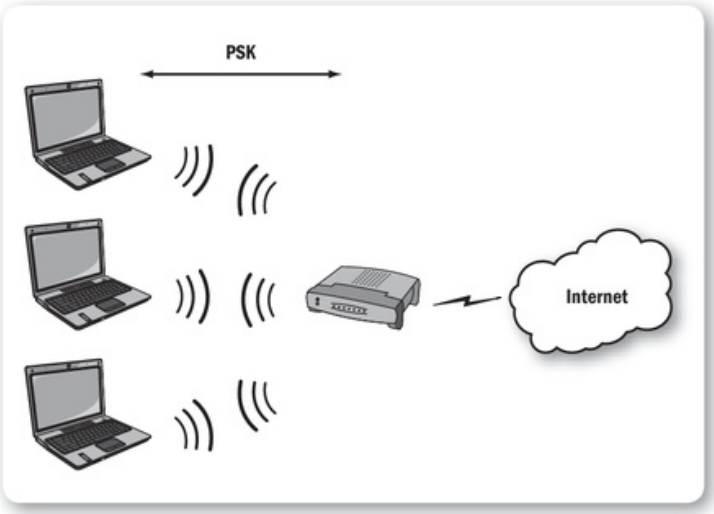


Figura 13. Pasar de WEP a WPA-PSK en una red supone actualizar el firmware, activar WPA-PSK e introducir la contraseña.

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, podemos afirmar que WPA2 es la versión certificada del estándar 802.11i. La Alianza Wi-Fi 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 a 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 a la red).

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 autentificación 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



OPCIÓN SEGURA

Si tenemos una red inalámbrica y necesitamos seguridad, optemos por **WPA2 (AES)** o en su defecto **WPA (TKIP)**. Los dispositivos que actualmente se encuentran en el mercado poseen estas opciones o por lo menos le permitirán seleccionar **WPA**. Evite usar el protocolo **WEP**, ya que no servirá de mucho en estos días y es facilmente violable su algoritmo.

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 deben asociar con un punto de acceso. Esto fue considerado por muchos fabricantes de equipo como una mejora de seguridad. Mientras 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 (**Wi-Fi Inspector**, por ejemplo) detecte la asociación que provenga de otro punto de la red cuando esto oportunamente ocurra.

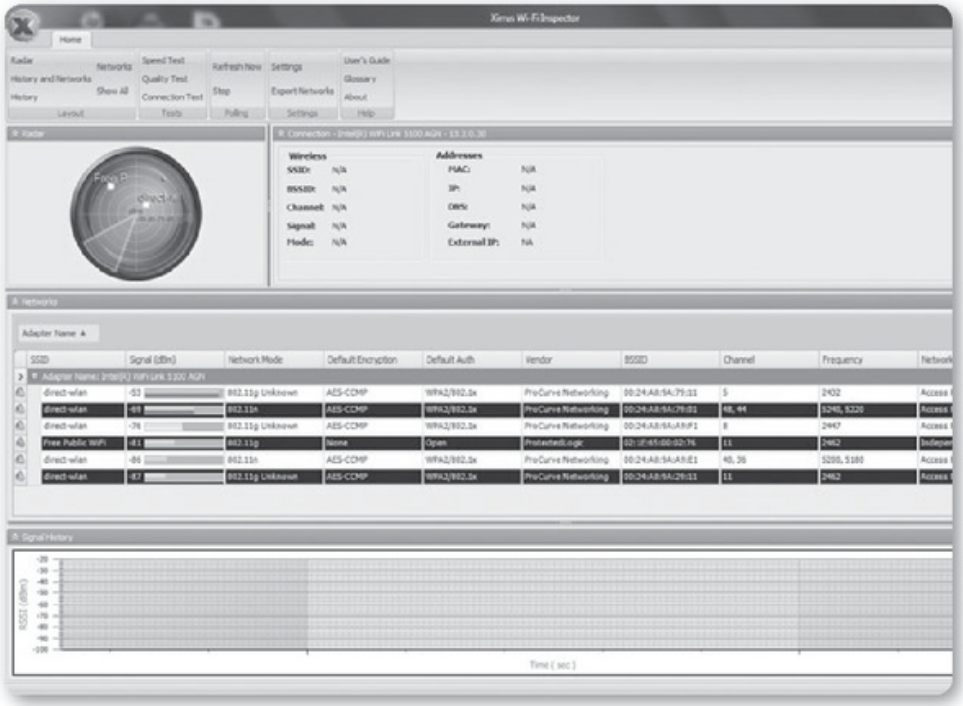


Figura 14. El programa Wi-Fi Inspector nos permite monitorear las redes cercanas aunque la SSID no sea visible a simple vista.

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. 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. La otra realidad más fuerte es que las direcciones MAC en casi cualquier red inalámbrica pueden ser fácilmente modificadas o **clonadas**, y de esta forma obtener una MAC de una entrada válida en el punto de acceso.



Figura 15. En las opciones del punto de acceso podremos 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 la dirección IP). Cuando el cliente tiene la dirección IP, todas las solicitudes HTTP se capturan y se envían al portal cautivo. Así, el cliente es forzado a identificarse en una página web de la empresa proveedora.

Los portales cautivos son responsables de verificar la validez de la contraseña y luego modificar el acceso del cliente Esto se realiza una vez que fue configurado correctamente todo el sistema y sus políticas de seguridad.



Figura 16. Esquema de funcionamiento de un portal captivo con autenticación en tres pasos.

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 trafico 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, desde el dispositivo del cliente inalámbrico.

PORTALES CAUTIVOS EN TU PC

Los portales cautivos se usan sobre todo en lugares con redes públicas (plazas, hospitales, entre otros). El objetivo de estos 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 para esto es FirstSpot, cuyo sitio web se encuentra en **http://patronsoft.com/firstspot**, que viene desarrollándose desde el año 2002 y ofrece una solución fácil de utilizar que nos da control total sobre nuestro punto de acceso.

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.

En los primeros años, WEP intentaba cumplir con esta premisa. Desafortunadamente, el mecanismo de integridad implementado llamado **CRC** (Código de redundancia cíclica) resultó inseguro. Utilizar un mecanismo inseguro permite que el tráfico de información sea alterado sin que se note nada.

> DEBEMOS RECORDAR QUE LA INTEGRIDAD DE DATOS MEDIANTE WEP ES OBSOLETA

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.

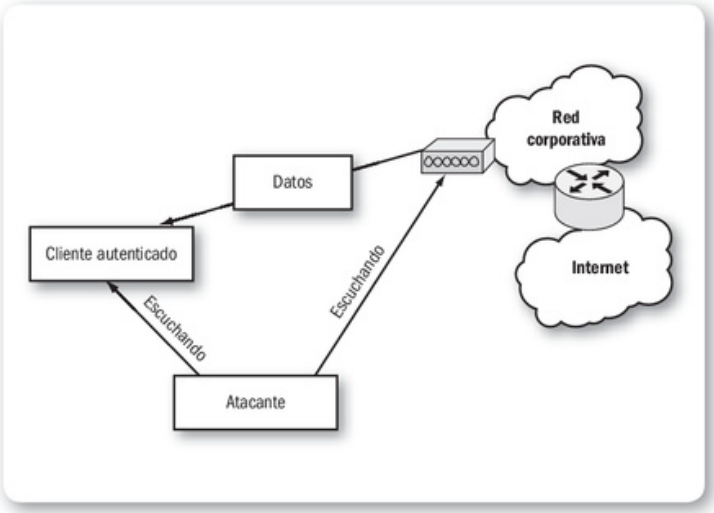


Figura 17. En un ataque de reinyección, el atacante espera de forma silenciosa hasta obtener información útil.

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.

TABLA 1

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

Tabla 1. En la tabla vemos el resumen de autenticación y cifrado en WPA y WPA2 (modo 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 la red. 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, 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. 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.



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 forma se puede revisar la información y 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 o similares.

• Ataque de denegación de servicio: como ya dijimos, en estos ataques se niega el uso de los recursos de la red a los usuarios legítimos.

• 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 pueden ser los expedientes, archivos, papeles con información confidencial, etc.). En general, los ataques a computadoras se inician con información obtenida de una fuente física que expone información sensible o privada de una empresa, por ejemplo.

En la tabla que se encuentra a continuación, veremos las diez amenazas de seguridad más relevantes en redes inalámbricas, la descripción de cada una y plantearemos de forma sintética recomendaciones a seguir para cada una de estos frecuentes peligros.

TABLA 2

▼ 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	Autentificación	Riesgo de acceso no autorizado a su red inalámbrica.	Implementar WPA2. No depender solo de un esquema de autentificación basado en MAC. No publicar la SSID.
4	Autentificación	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.

▼ N°	▼ PARÁMETRO	▼ DESCRIPCIÓN DE AMENAZA	▼ POSIBLE SOLUCIÓN
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	Autentificación 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__: 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

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 hacen 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 carecemos de medidas de seguridad en nuestra red, ¿de qué forma puede quedar expuesta nuestra información frente a intrusos?
2	¿En qué se basa una buena estrategia de seguridad?
3	¿Cómo podemos mejorar las políticas de seguridad planteadas?
4	Nombre algunas formas en las cuales la pérdida de la confidencialidad de la información se manifiesta en nuestra vida.
5	¿Qué garantías no da la autenticación?
6	¿Qué se entiende por cifrado o codificación a nivel de enlace?
7	¿Cuáles fueron las fallas que provocaron la obsolescencia del protocolo WEP?
8	¿Cuáles son los modos en que puede usarse el protocolo WPA/WPA2?
9	¿Es conveniente dejar de difundir el SSID para incrementar la seguridad de la red?
10	¿Qué objetivo tiene la implementación de un portal cautivo en la red inalámbrica?
11	Describa la autentificación en tres pasos implementada por un portal cautivo.
12	¿Cuál es el nombre del mecanismo, explicado en este capítulo, de integridad implementado en WEP que resultó totalmente inseguro?
13	¿En qué consiste el ataque por repetición?
14	¿Qué se recomienda implementar para lograr integridad en una red inalámbrica?
15	¿Qué realiza el ataque por intercepción?

*05 –

Resolver problemas

En este capítulo nos adentraremos en la resolución de los problemas de nuestra flamante red inalámbrica. Si bien pueden existir variedad de dificultades, trataremos de enfocarnos en un método que nos ayudará a identificar qué ocurre cuando se presenta un problema en la red. Evitaremos con esto usar el clásico reinicio de los dispositivos, al que tan acostumbrados nos tienen ciertos sistemas operativos.

Veremos cómo aislar, identificar, priorizar y resolver problemas, que una vez diagnosticados, solucionaremos con herramientas comúnmente usadas por administradores de redes.

- **Enfoque metodológico 180**
- **Pasos fundamentales a verificar 182**
  - Tensión eléctrica estable 182
  - Actualizaciones 186
- **Nuestro método 186**
  - Delimitar el problema 186
  - Encerrar la causa del problema 189
  - Planear la solución 190
  - Corroborar los resultados 197
  - Documentar los resultados 198
  - Caso práctico 200
- **¿Cuáles herramientas usar para resolver problemas? 201**
  - Escenarios prácticos 203
- **Resumen 205**
- **Actividades 206**

Enfoque metodológico

Basándonos en el modelo OSI, que venimos estudiando desde el primer capítulo, analizaremos capa por capa en busca de la causa del 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 rápido 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 de nuestra red con un plan, la causa y la posible solución van a ser más simple de encontrar.

Tomemos un ejemplo práctico para mostrar la metodología en la resolución de problemas en una red inalámbrica. Un usuario que maneja una aplicación para cargar datos de inventario en la página web de su ferretería tiene problemas para que le tome los datos ingresados. Lo primero que hará es quejarse de que la **aplicación** está fallando (estaría mirando la capa 7 del modelo OSI), pero si indagamos un poco más el tema podemos ver que el problema puede estar en otra capa inferior. Por ejemplo, podríamos decir que la señal inalámbrica no está llegando a su notebook (problema en la capa 1 de OSI) o tal vez no tiene una dirección IP asignada por el DHCP (capa 3 de OSI).

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. Vemos la Pila de protocolos del modelo OSI comparada con TCP/IP, separados por capas. El modelo TCP/IP es más simple.



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

Es posible que existan muchos y diferentes tipos de problemas en una red de estas características.

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 tarea más difícil de su trabajo. De todas formas, no tenemos que temerle a los problemas que se presentan día a día en las redes. Si poseemos un método práctico y buena dosis de paciencia vamos a lograr resultados óptimos. Todo va a depender de nuestra habilidad para analizar el problema y así encontrar la forma óptima de resolverlo con ciertos conocimientos.

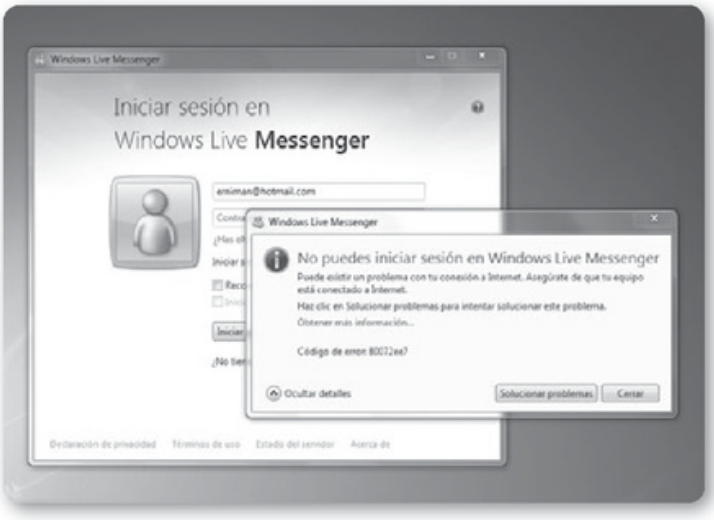


Figura 3. Aplicaciones como Windows Live Messenger no brindan información específica al momento de un problema.

Una vez que tengamos realizado el diagnóstico del problema, la identificación de los recursos afectados y además conozcamos el camino a seguir para llegar a esos recursos, la corrección del problema es algo directo y sencillo. Debemos tener presente que antes de dar el diagnóstico se debe aislar la verdadera causa que originó el problema de factores irrelevantes existentes.

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 problema de forma organizada y metódica, recordando que estamos buscando la causa, no síntomas.

Es común identificar los problemas por sus síntomas, pero no la causa auténtica. Por esto, aprenderemos a descartar rápidamente la mayor cantidad de hipótesis que identifiquemos. Así, podremos centrarnos en los puntos donde puede estar la causa original del inconveniente.

Pasos fundamentales a verificar

Antes de describir nuestro método para resolver problemas, vamos a desarrollar un par de conceptos a tener en cuenta. De esta forma nos aseguraremos que todos los dispositivos implicados están correctamente conectadas y funcionando además de tener la última versión de firmware instalada.

Tensión eléctrica estable

En los nuevos aparatos electrónicos que conforman nuestro equipamiento inalámbrico (por ejemplo, los puntos de acceso), 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, un bajón en la corriente o por alguna desconexión del equipo, puede producirnos un daño irremediable a las partes del aparato inalámbrico.

Por ejemplo, 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 deñarse. De esta forma el dispositivo quedará inutilizado y deberemos reemplazarlo .

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 que utilizamos.

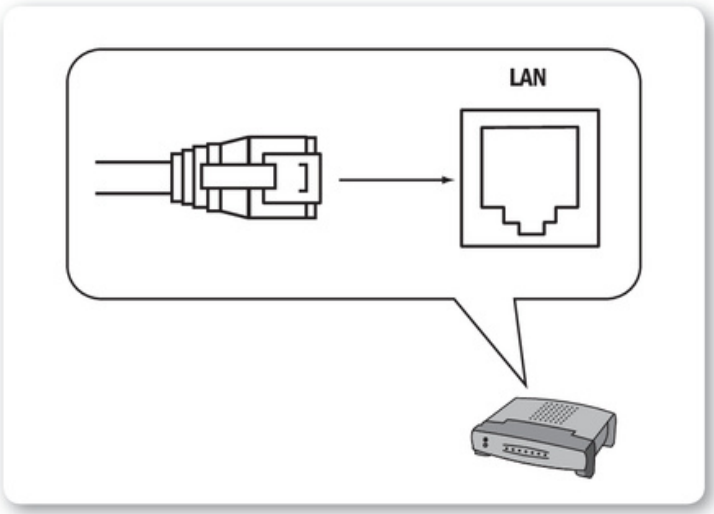


Figura 4. Recordemos que en el puerto Ethernet de nuestro AP conectamos el cable UTP con ficha RJ45 perteneciente a la red LAN.

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



Figura 5. Muchos dispositivos inalámbricos identifican el puerto a la red cableada con un color y la inscripción Ethernet.



Figura 6. Algunos fabricantes copian la parte estética de fuentes originales pero usan diferentes valores de tensión y corriente.

Podemos sufrir deterioros similares en la parte electrónica de nuestro equipo si usamos un transformador que no es el original o está defectuoso. Si alimentamos el punto de acceso, por ejemplo, con muy bajo o alto voltaje corremos el riesgo de dañar el dispositivo. Recordemos que cada fabricante tiene su propio diseño y en general varían en muy poco las fuentes de alimentación (**transformadores**). De esta forma es muy fácil confundirse con otros dispositivos y usar un transformador inadecuado para el nuestro. Los equipos suelen tener protección interna para esto, sin embargo, mejor estar prevenidos y prestar atención.



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



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

Si tenemos muchos equipos en nuestra 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 9. Es una práctica muy buena etiquetar todos los cables en nuestra red, en esta imagen vemos el ejemplo para un cable UTP.

Existen normas de telecomunicaciones que recomiendan la forma en que deben etiquetarse ciertos equipos. Nosotros podemos basarnos en esos ejemplos y realizar nuestro propio etiquetado de red. Resulta una buena práctica para mantener la seguridad en nuestros equipos.

Actualizaciones

Al hablar de actualizaciones siempre nos referimos a los equipos que traen software incorporado (microcódigo) y que llamamos **firmware** (describimos esto 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 generalmente existen nuevas versiones para usar (se puede consultar el sitio web del fabricante del equipo para comprobar la disponibilidad de la nueva versión). Nosotros, como usuarios del equipo, tenemos la responsabilidad de mantenerlo actualizado con la más reciente versión de firmware. Si tenemos el último firmware instalado en nuestro equipo optimizaremos las prestaciones y confiabilidad, además de corregir posibles fallas (también llamadas **bugs**) de funcionamiento.



Nuestro método

Basaremos nuestro método para resolver problemas en la red inalámbrica en cinco pasos fundamentales:

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 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 ayudará a resolver el inconveniente. Las personas que hacen uso de la red diariamente estaban cuando el problema no existía y luego cuando apareció y, seguramente, recordarán cuáles fueron los sucesos que consumaron en el problema.

Para ayudar a identificar el problema, **anotemos** en una lista la secuencia de eventos que nos describen los usuarios. En caso de que nosotros mismos seamos los usuarios, tratemos de recordar qué ocurrió antes del problema. Una idea útil es hacer un formulario con una serie de preguntas que ayudarán a organizar las anotaciones. Algunos ejemplos de preguntas a realizar son:

- ¿Cuándo notó el problema o error por primera vez?
- ¿Sabe si el equipo fue movido a otra habitación últimamente?
- ¿Conoce si ha habido cambios en el software o hardware en el último tiempo días o semanas?
- ¿Le ha sucedido algo al lugar donde habitualmente se conecta? ¿Se ha derramado algún liquido o similar sobre el teclado?
- ¿Recuerda cuándo ocurrió exactamente el problema? ¿Durante la tarde, a la mañana? ¿Luego de mandar un **e-mail**?
- ¿Sabe si se puede reproducir el error?
- ¿Cuál es específicamente el problema?
- ¿Puede describir los cambios que se manifestaron en su computadora o en el equipo (punto de acceso, etc.)?

Aunque no tengamos muchos conocimientos técnicos, formular estas preguntas puede ser extremadamente útil a la hora de recopilar información (siempre y cuando hagamos buenas preguntas).

Ciertas observaciones pueden ser indicios que nos servirán para identificar la causa original del problema. A modo de ejemplo, podemos decir que las siguientes sirven como pistas para identificar el problema de forma general:

- La red no funciona o funciona muy lenta
- No puedo imprimir un documento
- El programa para cargar el inventario no funciona
- Estaba conectado al **chat** y perdí la conexión
- No me puedo conectar a Internet

Si seguimos haciendo preguntas vamos a lograr acotar el problema. Depende de la habilidad para obtener información de cada uno el éxito de estas preguntas. Las siguientes preguntas y sus posibles respuestas nos muestran nuevos ejemplos a seguir para delimitar el problema encontrado:

- ¿Los problemas ocurren todo el tiempo o en ciertos lapsos? Cuando el hardware comienza a fallar se hace visible con síntomas intermitentes.
- ¿El problema afecta a todos los clientes inalámbricos o solamente a uno? En caso de estar afectado solo un cliente inalámbrico, entonces es muy probable que el problema exista en su computadora.
- ¿Se hicieron actualizaciones automáticas del sistema operativo? Ciertos cambios en el sistema operativo pueden causar problemas.
- ¿Cuándo el problema ocurre, es para todas las aplicaciones (**MSN, Skype**, etc.) o solamente en una en particular? En caso de aparecer en una sola aplicación deberemos centrarnos a investigar en ella.
- ¿Anteriormente ocurrió algún problema similar? En caso de ser afirmativa la respuesta debemos revisar la documentación en busca de la posible solución. Si no existe documentación, preguntemos si alguien recuerda (o si nosotros recordamos) cómo fue solucionado el problema.
- ¿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 (otro punto de acceso, una impresora, etc.)? Debemos verificar que, en caso de ser afirmativa la respuesta, los nuevos dispositivos estén configurados correctamente y funcionando.
- ¿Existen diferentes marcas de fabricantes en los equipos implementados en la red? Es posible que exista alguna incompatibilidad entre fabricantes de equipos. Debemos consultar en Internet.



CONEXIÓN NULA

Si tenemos problemas en la conexión de red, donde se informa que la **Conexión es limitada o nula**, y no podemos ingresar a Internet, entonces existe un problema. La causa es un **virus** o **adware** (programa que se ejecuta, muestra o baja publicidad) que borró o modificó registros. La herramienta **ICRepair Tool** lo repara **http://internet-connection-repair-tool.uptodown.com**.

• ¿Alguien instaló un nuevo **software** en la computadora que tiene problemas antes de que ocurra el error? Muchas veces las instalaciones de nuevos programas pueden ocasionar errores en las aplicaciones. Revisaremos cualquier aplicación instalada antes de que ocurra el error.

• ¿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, trate de hablar con la persona que intentó arreglar el problema.

Encerrar la causa del problema

El objetivo de este segundo paso es poder 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 problemas que consideramos más difíciles de resolver. Decimos que un problema es sencillo de resolver cuando, por ejemplo, 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 nuestra lista a una o dos categorías.

> EL OBJETIVO DE ESTE SEGUNDO PASO ES PODER AISLAR O IDENTIFICAR LA CAUSA ORIGINAL DEL PROBLEMA

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 tenemos.

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 formas más usadas para resolver estos problemas es realizar nuevamente los eventos que ocasionaron el inconveniente. Como ayuda extra, podemos solicitar al usuario que nos detalle lo que estaba realizando antes y en el momento de que ocurrió el error. Si el error se presenta de forma intermitente podemos solicitar nos llamen cuando aparezca el inconveniente en la red y mientras tanto que nadie toque nada (nos referimos a no instalar nuevas aplicaciones, por ejemplo). Así, vamos a poder ver el error manifestarse.

Planear la solución

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

Pensaremos un plan para identificar y resolver los problemas basándonos en el conocimiento actual. Iniciaremos 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 a tener en cuenta es **anotar** lo que realizamos en cada paso, de esta forma estaremos **documentando** cada acción realizada y su resultado. Cuando en un futuro se nos presente un problema y nosotros identifiquemos algún síntoma similar, podremos consultar la documentación para así resolver el inconveniente.

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, vamos a poder recorrerla en busca de soluciones a nuestro problema.

Tomamos uno de los problemas de nuestra lista, por ejemplo la falla al tratar de conectarnos al **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 problema verificando el nombre de usuario y contraseña ingresados.

Un usuario que ingresa de manera errónea su dirección de e-mail o contraseña puede ser la causa del supuesto problema. De ser así,



AYUDA EN LÍNEA

Cuando un problema en nuestra red inalámbrica escapa del conocimiento que poseemos, será momento de buscar ayuda. Podemos consultar a compañeros o amigos con 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.

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 a las capas inferiores. Tal vez un problema de **interferencia** en la señal inalámbrica o un bajo nivel de señal en la notebook causan el inconveniente y de esta forma lo estaríamos identificando.

> LA CONECTIVIDAD IP SE COMPRUEBA FÁCILMENTE CON UN COMANDO LLAMADO PING

Este método requiere paciencia y dedicación, si consultamos en Internet por problemas específicos y formulándonos preguntas puntuales podremos obtener resultados muy satisfactorios.

Resolver problemas del centro-arriba o del centro-abajo

Resolver el problema utilizando este enfoque es el más popular. Se aplica, en general, de manera intuitiva por personas que ya poseen experiencia en redes y es la manera más fácil para empezar a lidiar con este tipo de problemas 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 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.

ETIQUETADOR DE RED

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

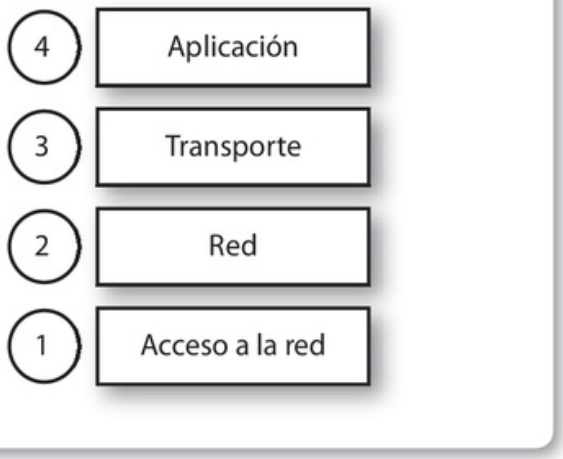


Figura 10. Tener una visión del problema desde un ángulo diferente nos proporciona posibles nuevas soluciones.

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). La conectividad IP se comprueba fácilmente con un comando llamado **ping**. Podemos decir que el comando **ping** es una de las herramientas más útiles empleada en diagnóstico de redes. Este comando existe en todos los sistemas operativos y se utiliza para enviar información binaria (ceros y unos) entre dispositivos 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.

Es realmente útil este comando y de muy fácil implementación.

SECUENCIA DE ENCENDIDO

Antes de encender un dispositivo de red, se recomienda estudiar el comportamiento normal de los **LEDs**. Esto se puede consultar en el manual o en Internet, al buscar en el sitio Web del fabricante. De esta forma podremos seguir la secuencia de arranque del equipo de forma visual y asegurarnos que el dispositivo trabaja correctamente al momento de conectarlo. También es útil cuando ya tenemos el dispositivo funcionando y queremos verificar la manera en que está operando en nuestra red.Esta práctica nos ayudará al buen funcionamiento de nuestro equipo.

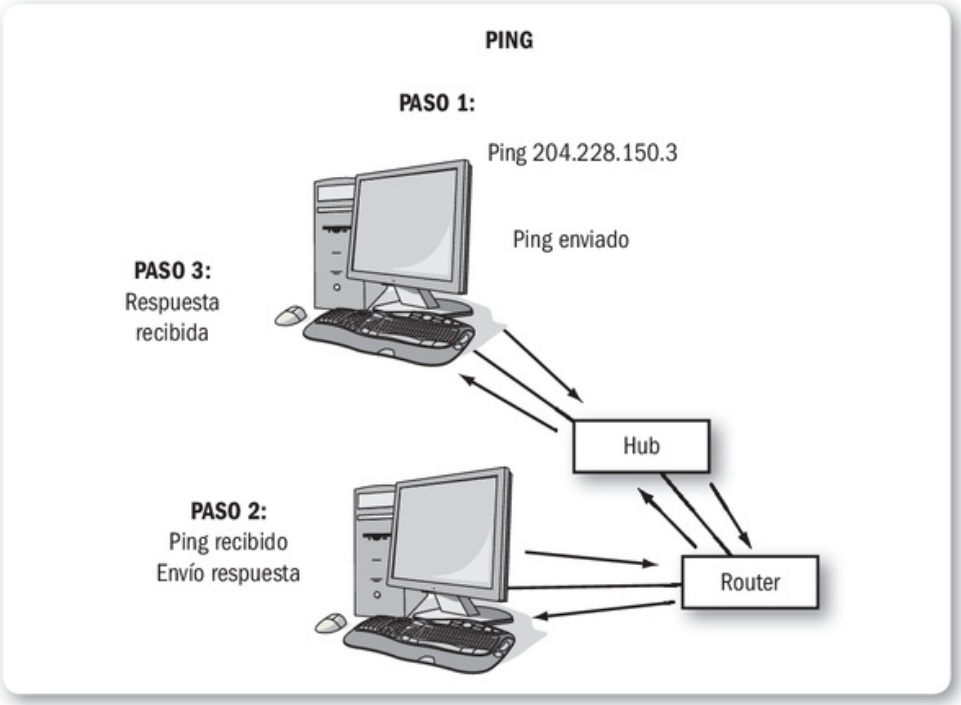


Figura 11. Este ejemplo nos muestra el camino de los datos enviados por el comando ping en una red.

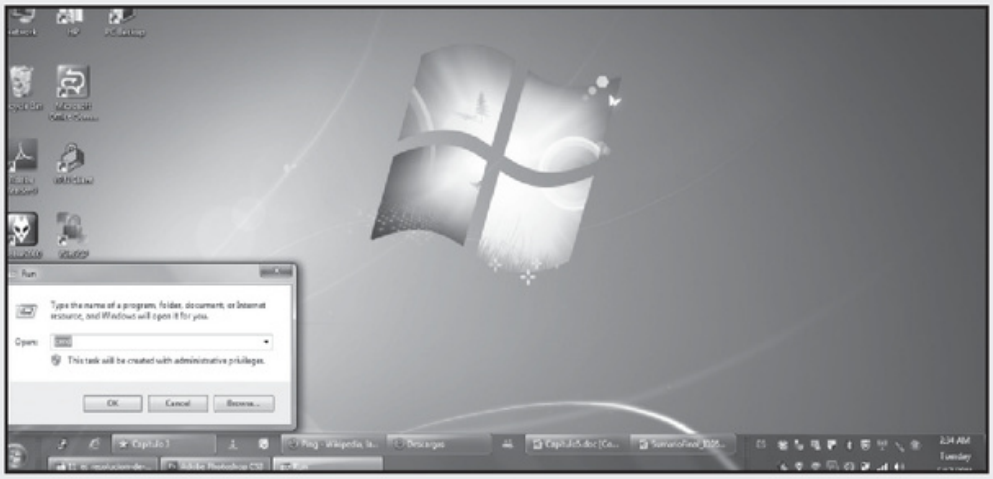
Vale aclarar que estos paquetes de información enviados por el comando ping no tienen información alguna, tan solo son señales, inertes para cualquier dispositivo de la red. Consideremos también que no importa el sistema operativo que utiliza el dispositivo destino, al cual enviamos los paquetes, el ping se realizará de todas formas. Veamos con un ejemplo cómo funciona este comando.

USAR UPS O ESTABILIZADOR

Los equipos de nuestra 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, *Unninterruptible Power Supply* en inglés). En el mercado existen UPS o estabilizadores de diferentes tipos y tamaños, siempre debemos buscar uno acorde a nuestras necesidades para mantener el buen funcionamiento de nuestros equipos.

EJEMPLO DE COMANDO PING

01 Ejecute el comando `ping` desde el símbolo del sistema (también llamado consola) que ejecutará de forma automática el archivo ping.exe alojado en la carpeta system32. Abra una consola como describimos en capítulos anteriores. Haga clic en `inicio`, luego en `Ejecutar` (o Run) y escriba `cmd`.



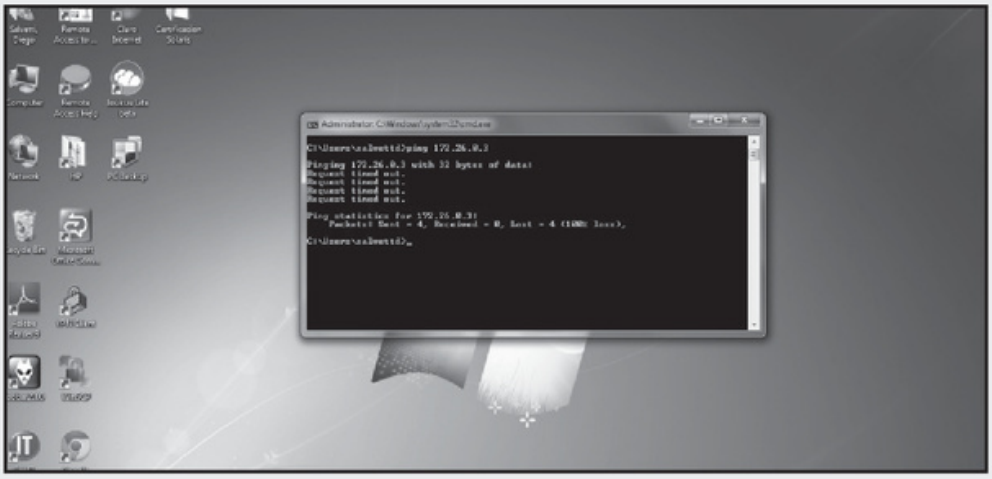
02 La sintaxis de este comando es la misma que para el resto de los comandos en Windows. Se forma: `ping <ip> -parámetro valor -parametro2 valor` . Ahora, reemplace `<ip>` por la dirección IP destino (esta variable es obligatoria, También puede usar una dirección de Internet como www.google.com). Luego de manera opcional puede utilizar parámetros con sus valores. Escriba `ping www.google.com.ar` y presione `Enter`.



03 Vea la salida que obtiene luego de presionar `Enter`. Se informa la dirección IP del sitio web y 4 confirmaciones de respuesta (Reply from) desde ese destino. Además se muestra la demora (en milisegundos) en realizar el camino entre el servidor de Google consultado y nuestra computadora. Envíe un mensaje a un destino inexistente. Escriba `ping www.google.com.xx` y luego `Enter`.



04 Como el destino no existe se muestra un mensaje de error diciendo que verifique la ruta destino. Ingrese una dirección IP que no pertenece a ningún usuario en su red. Escriba `ping 172.26.0.3` y presione `Enter`. Confirmará que no obtendrá respuesta. En cambio tendrá un mensaje de tiempo agotado (Time out) que indica que el destino no existe o presenta un problema de configuración.



Algunos de los parámetros más comunes que podemos utilizar con este comando los veremos a continuación:

• **-t** Realiza ping al destino hasta que se fuerza la salida (presionando la tecla **Ctrl-c**) y se termina el comando.

• **-n <numero>** Esta opción 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 se usa el parámetro **–t** como vimos.

Se puede consultar por más opciones la ayuda del comando. 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.

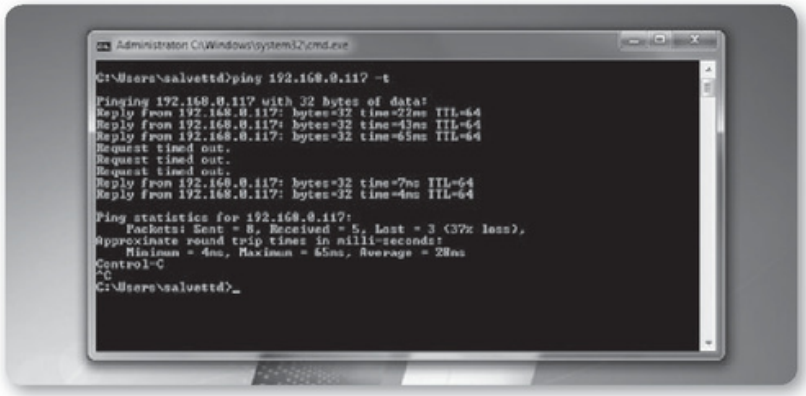


Figura 12. Si el número de paquetes enviados difiere del número recibido, entonces podemos tener un indicio de problemas.

MONITOR DE RED EN WINDOWS 7

Existe un **gadget** (programa con una función específica) para Windows 7 muy útil a la hora de monitorear una red. El **Network Meter** nos permitirá ver el SSID, calidad de la señal en porcentajes, direcciones IP asignadas, localización de la IP usando el servicio de GoogleMaps, velocidad de subida/bajada, entre otros. Podemos bajarlo en **http://addgadget.com.**

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

> SE RECOMIENDA CREAR UN PLAN Y SEGUIR LOS PROCEDIMIENTOS TAL COMO LO PENSAMOS

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) de nuestra red.

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

Recomendamos 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 problema, documentemos en un cuaderno los cambios realizados (el antes y después) para 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 que el problema ya no existe. Para esto vamos a solicitar a los usuarios

> NECESITAMOS DOCUMENTAR EL PROBLEMA ENCONTRADO Y LA SOLUCIÓN PLANTEADA

de la red inalámbrica que prueben la solución (básicamente esto es que usen de forma normal la red). Ellos serán los que confirmarán los resultados de nuestro trabajo.

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 dirección 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, provocando un nuevo problema en lugar de una solución.

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 aprender nuevos conocimientos en este tema.

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



DOCUMENTAR LA RED

Antes de emitir un diagnóstico de un problema, necesitamos averiguar el tipo de problema. Para esto recopilaremos la mayor información posible de la red. Si está documentada consultaremos eso si no deberemos elaborarlo nosotros. Incluiremos información como topología de red, resumen de dispositivos con sus nombres y direcciones (MAC e IP), entre otros.



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

Tengamos ciertas consideraciones presentes:

• 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** a cada una de esas partes de forma independiente analizando información para 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 el problema existe en un solo usuario de la red inalámbrica y no en todos.

• Si el problema se relaciona con el hardware recomendamos verificar: placas de red, cables y conectores de la red cableada y alimentación de los dispositivos, puntos de acceso y dispositivos similares, etc. Muchas veces el hardware es protagonista de los problemas en la red.

• Aislar una parte de la red en busca del problema puede resultar una solución para las otras partes. Si ocurre este caso, no considere resuelto el problema y concéntrese en la parte que no está operativa y posiblemente sea la originadora del problema.

• 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. 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 urgencia.

Caso práctico

Para tratar de resumir todo lo visto hasta el momento, veremos un ejemplo de la vida real así podremos mostrar cómo funciona el método planteado en este capítulo.

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

Veamos cómo resolveríamos este simple pero interesante problema sin morir en el intento.

• Basándonos en la resolución de problemas arriba-abajo, formularemos las siguientes preguntas para recopilar información sobre la causa del problema existente:

- ¿Cuál programa utiliza para chequear su correo? (verificamos posibles problemas en la capa aplicación).

- ¿Puede verificar la configuración de conexión de su programa?

- ¿Puede ingresar a otras **páginas web**? (verificamos problemas de DNS). ¿Puede entrar a Blogs, diarios, etcétera?

- 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? (verificamos problemas de autenticación). ¿Conoce esos datos?

- ¿Su computadora tiene una dirección IP asignada? (verificamos problemas a nivel IP). ¿Puede verificarla?

• 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 tener ambas respuesta 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 que usamos para encontrar y resolver los problemas es la misma para todos.

¿Cuáles herramientas usar para resolver problemas?

Necesitamos tener en claro cuáles **herramientas** tenemos disponible para ejecutar nuestro método y así resolver los posibles errores de la red inalámbrica. Básicamente decimos que usaremos dos tipos de herramientas, las que vienen con cada producto (según el fabricante esto puede variar) y las que trabajan con cualquier producto soportado por la norma IEEE 802.11. Enumeremos algunas herramientas y su aplicación básica. Podremos consultar más información en Internet.

TABLA 1

	▼ 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 en tiempo real una red.	Debe bajarse e instalarse 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.

	▼ NOMBRE	▼ USO	▼ EJEMPLO DE USO
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. En esta tabla vemos las 5 principales herramientas a utilizar al momento de resolver problemas en la red.

Se puede consultar en Internet para ver ejemplos de uso de las herramientas, buscando en Google. En la siguiente figura, podemos ver una de ellas en acción.

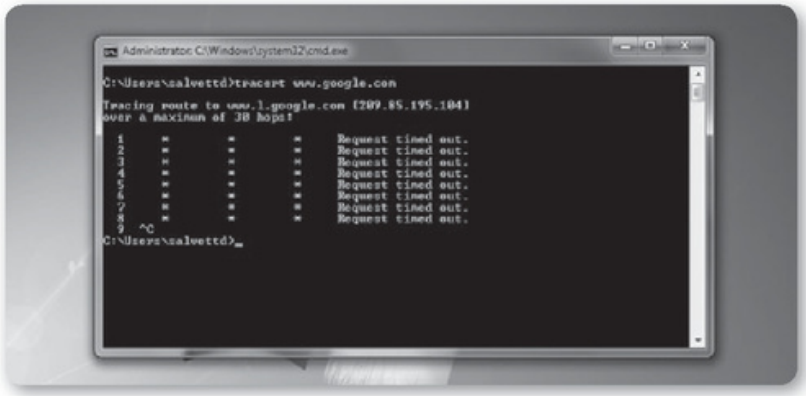


Figura 14. Ejemplo de aplicación de la herramienta **`tracert`** sobre la dirección **`www.google.com`**.

ETHEREAL LUEGO WIRESHARK

Para los que no saben, primero fue **Ethereal** 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.

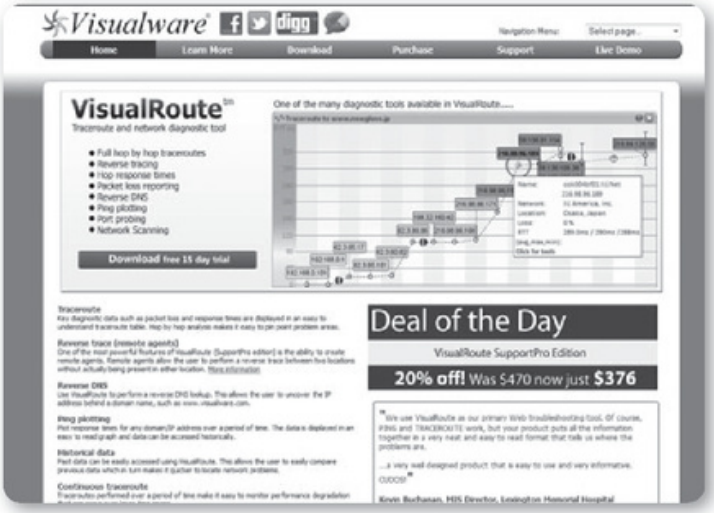


Figura 15. La empresa **VisualWare** nos presenta el producto **VisualRoute** para realizar diagnósticos en nuestra red.

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.

Además, existe otra gran variedad de herramientas para realizar esto, como la que vemos en la figura de la página siguiente.

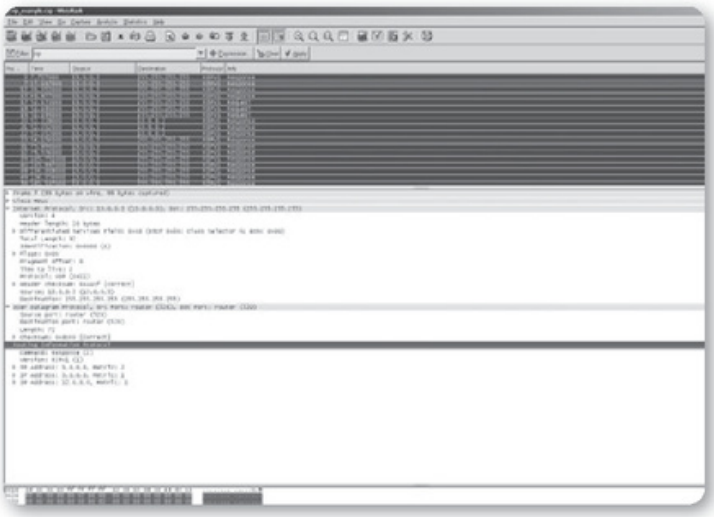


Figura 16. WireShark nos presenta los diferentes protocolos en tiempo real y discriminados con etiquetas y colores.

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. 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.

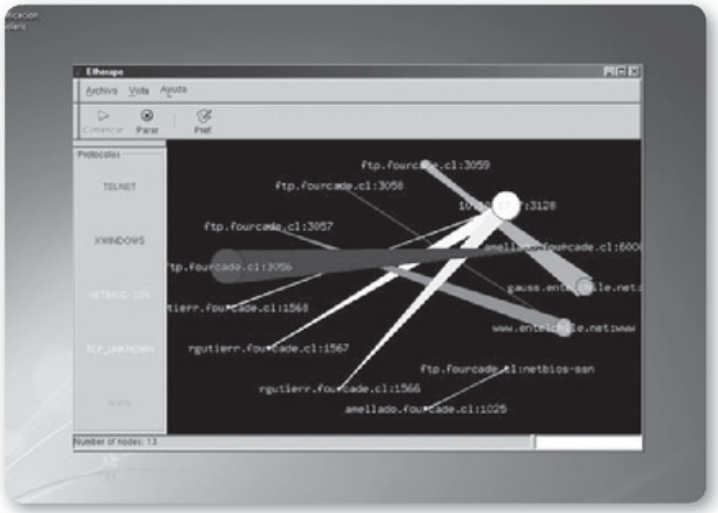


Figura 17. Otra herramienta útil es EtherApe que nos da una visión global del tráfico en la red y sus protocolos.

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

¿TE RESULTA ÚTIL?



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

NO ATENTES CONTRA LA LECTURA. NO ATENTES CONTRA TI. COMPRA SÓLO PRODUCTOS ORIGINALES.

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

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.

Es útil para:

• Monitorear pérdida de paquetes en conexiones TCP. Esto ocurre cuando la red está congestionada, **saturada de tráfico**, etc.

• Monitorear el tiempo de retorno. Este tiempo es un indicador del **retardo en la red**, muy útil cuando hay congestión.

• 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.

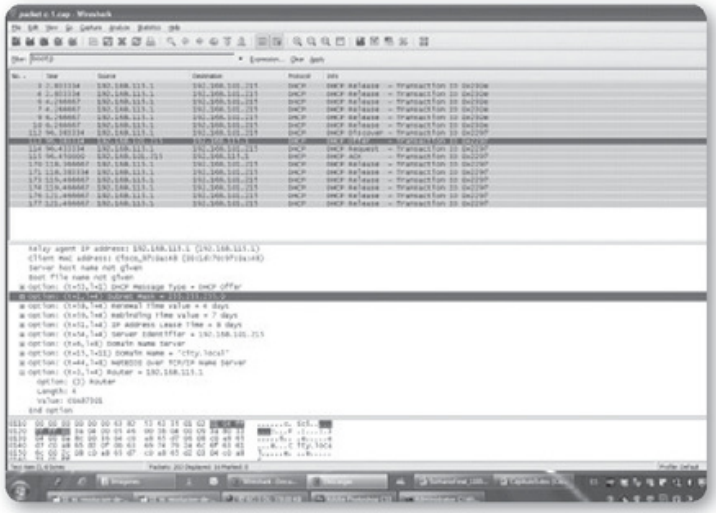


Figura 18. El programa **WireShark** realmente nos permite ir a ver lo profundo de las comunicaciones.

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 cuáles dos modelos se basa nuestro método para resolver problemas de red?
2	¿Cuál es un punto sensible a dañarse en nuestro punto de acceso si sufrimos anomalías en el servicio eléctrico?
3	¿Por qué motivo es importante tener el firmware del equipo actualizado?
4	Enumere los 5 pasos fundamentales de nuestro método
5	¿Para qué sirve realizar preguntas a los usuarios cuando reportan un problema?
6	¿Cuáles son los 2 enfoques que describimos para resolver los problemas?
7	¿Cuál de los 2 enfoques es el más popular y que se realiza de manera intuitiva?
8	¿Con cuál comando comprobamos que tenemos conectividad IP?
9	¿Por qué es importante documentar el procedimiento?
10	Enumere algunas herramientas que se recomiendan usar, en este capítulo, para la resolución de problemas de red

*06

Enlaces de larga distancia

Con los 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 que, en ciertos países, el uso de las redes inalámbricas es mucho más intenso, se aplica para situaciones en las que es necesario enlazar computadoras o equipos a larga distancia.

- **Introducción 208**
- **¿Qué es un radioenlace? 211**
  - Tipos de enlaces 215
- **¿Qué necesito para llegar más lejos? 223**
  - Consideraciones previas 226
- **Alineación de antenas 232**
  - Con extremos visibles 232
  - Con extremos no visibles 233
- **Cálculo de enlace 234**
  - Presupuesto de potencia 234
  - Cálculo con Radio Mobile 236
- **Resumen 243**
- **Actividades 244**

Introducción

En países europeos, es muy común que las empresas instalen cables de fibra óptica y así ofrecer 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. Las **fibras ópticas** instaladas, en nuestra región, no llegan hasta el usuario final y por lo tanto, no se provee un ancho de banda comparable a los países europeos o al propio Estados Unidos.

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, bandejas, entre otros) los costos son menores y la viabilidad de la red será 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 a unir, se denomina **radioenlace de larga distancia** o de forma más práctica **enlace de larga distancia** de manera indistinta.

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



RADIOPAQUETE DESDE LOS AÑOS 60

Packet radio (o radiopaquete) existe desde mediados de los años 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 por las islas hawaianas.

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

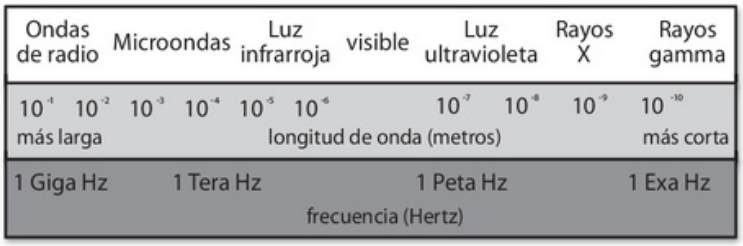


Figura 1. Recordamos la clasificación de las diferentes frecuencias y sus usos en el espectro electromagnético.

Los enlaces de larga distancia por microondas ofrecen mucha confiabilidad y estabilidad del servicio dado que son una tecnología madura. El problema que presentan es el elevado costo y la mano de obra calificada necesaria para instalar el equipamiento.

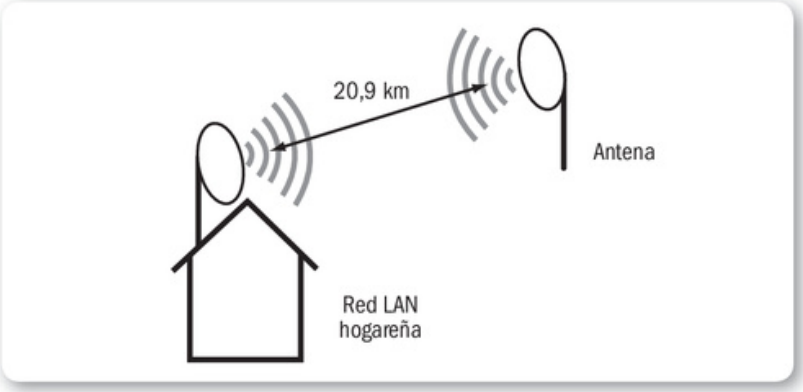


Figura 2. Los radioenlaces con microondas pueden unir puntos distantes y así compartir nuestra red hogareña.

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.

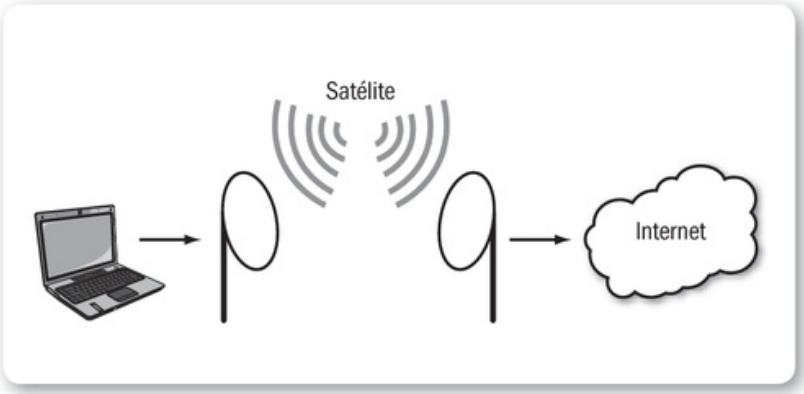


Figura 3. Un sistema satelital nos permite navegar, recibir y enviar e-mails y descargar archivos desde donde nos encontremos.

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

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 a tener en cuenta a la hora de evaluar unir puntos distantes.

Esto en comparación a las tecnologías vistas anteriormente.

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 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**.

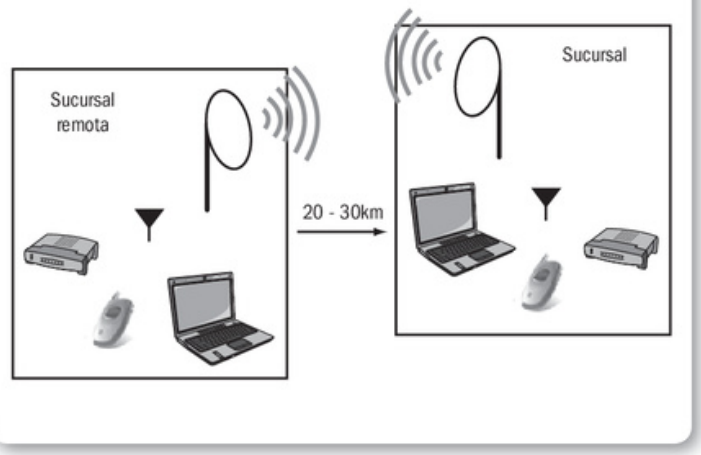


Figura 4. Extender nuestra red LAN que utiliza tecnología inalámbrica para vincular un destino aislado es el objetivo del radioenlace.

¿Qué es un radioenlace?

Un enlace de larga distancia,también llamado **enlace remoto**, es una conexión que usa tecnología inalámbrica para comunicar equipos que se encuentran distantes. La separación de estos puntos a unir puede ir desde los cientos de metros a kilómetros. Por ejemplo, un enlace nos permitirá conectar una red LAN de nuestra oficina con otro edificio, lugar de la ciudad o área geográfica.

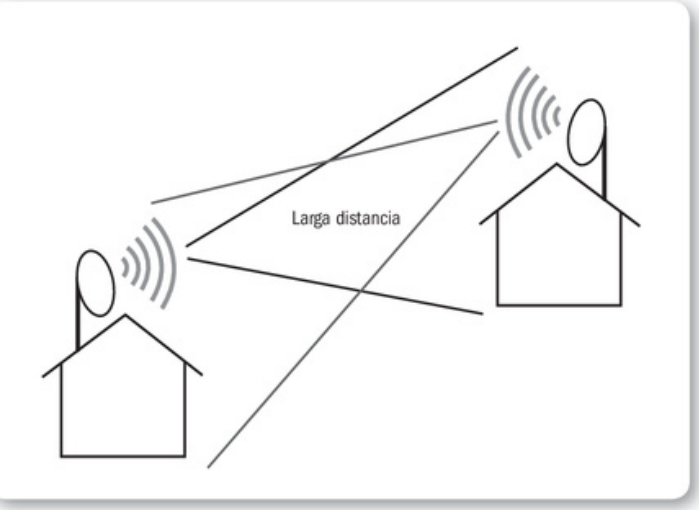


Figura 5. Ejemplo de un radioenlace fijo para unir dos hogares separados por un río. Las antenas permanecen fijas en un lugar.

Si los equipos 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 llama **enlace remoto móvil**.



Figura 6. Cuando empleamos un radioenlace móvil, los dispositivos poseen un área de cobertura por donde pueden moverse y conservar el vínculo.

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, estos conceptos no siempre están claros y son importantes.

RADIOPAQUETE

Radiopaquete (*Packet radio*) 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, a través de la radio, señales digitales mediante pequeños paquetes que luego forman un mensaje en el destino.

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

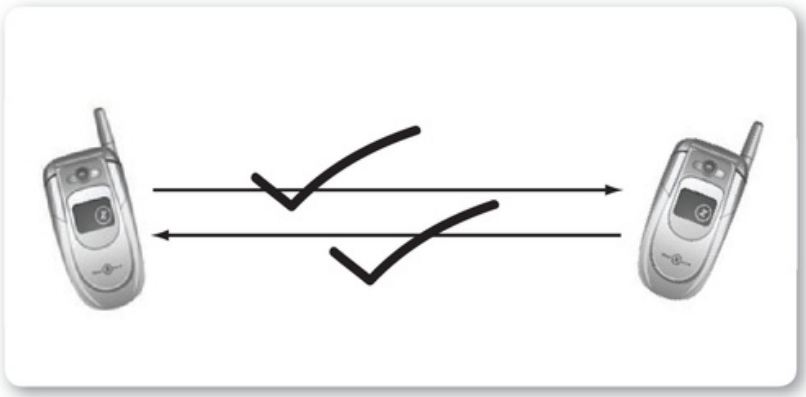


Figura 7. Ejemplo de comunicación dúplex donde ambos extremos pueden enviar y recibir mensajes simultáneos.

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 podría 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.

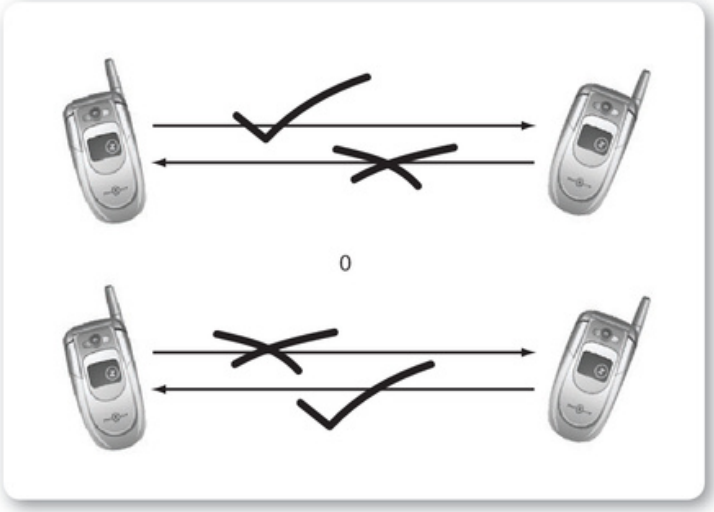


Figura 8. En el sistema **Half duplex** solo se permite comunicación en un sentido a la vez.

3) **Símplex**: en este caso, únicamente es posible realizar una transmisión en un solo sentido.

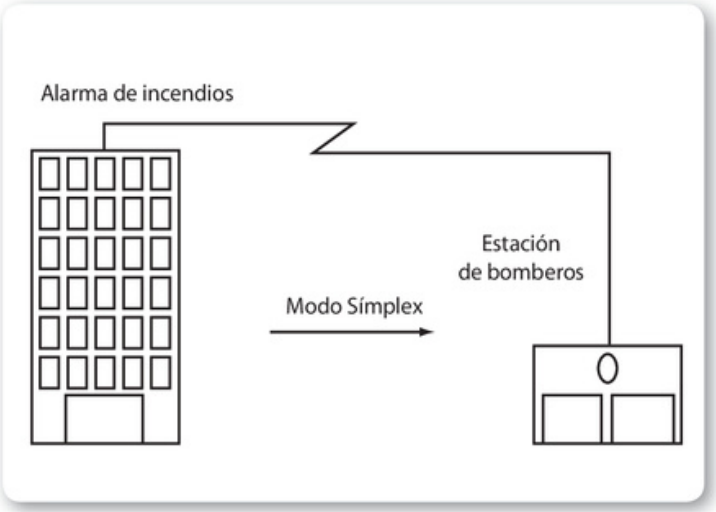


Figura 9. Un claro ejemplo de un modo símplex es cuando se acciona la alarma de incendios en un edificio para dar aviso a los bomberos.

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 para 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 (ciencia que estudia los procedimientos para representar

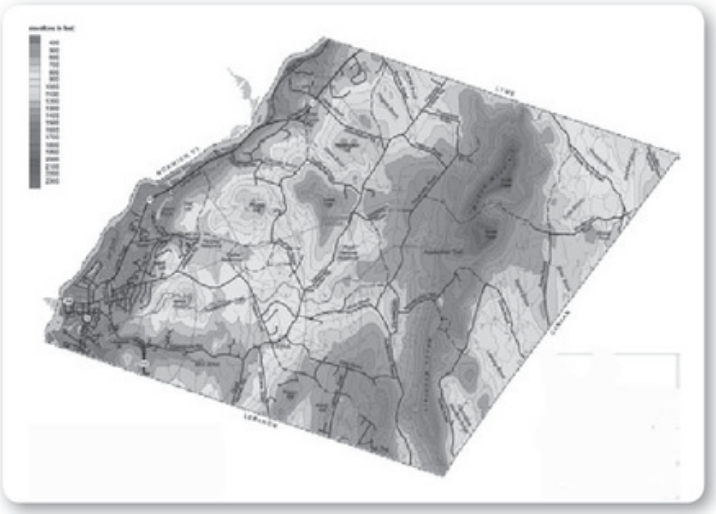


Figura 10. La topografía del lugar se representa en un mapa donde se distinguen los puntos más altos.

la superficie de la tierra). No importa cuán grande o pequeño sea nuestro enlace, para que funcione correctamente debemos asegurarnos 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 son árboles, edificios, entre otros.

> PARA CALCULAR LAS ALTURAS ADECUADAS, DEBEMOS CONOCER LA TOPOGRAFÍA DEL TERRENO

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 los 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 pueden lograr 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 (antena emisora y 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*)

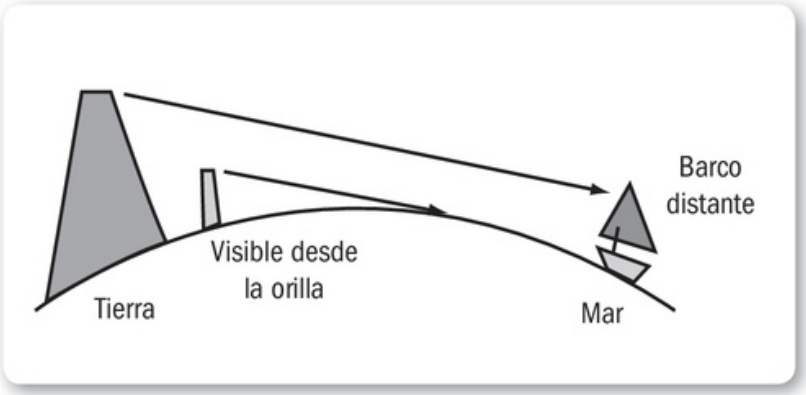


Figura 11. La curvatura de la tierra es determinante cuando trabajamos con puntos que necesitan unirse con línea visual directa.

También es común que para enlaces de muy largas distancias se utilicen repetidores. Así, un radioenlace está formado por equipos terminales y repetidores intermedios (en caso de ser necesarios por la distancia entre las terminales).

Se deberá evaluar cada enlace en particular para determinar si es o no necesario el uso de repetidores.

Los repetidores tienen una función simple, lograr que la señal recibida pueda ser enviada nuevamente a mayor distancia. De esta forma estarían salvando la falta de visibilidad que puede existir por obstáculos o por la curvatura de la tierra.

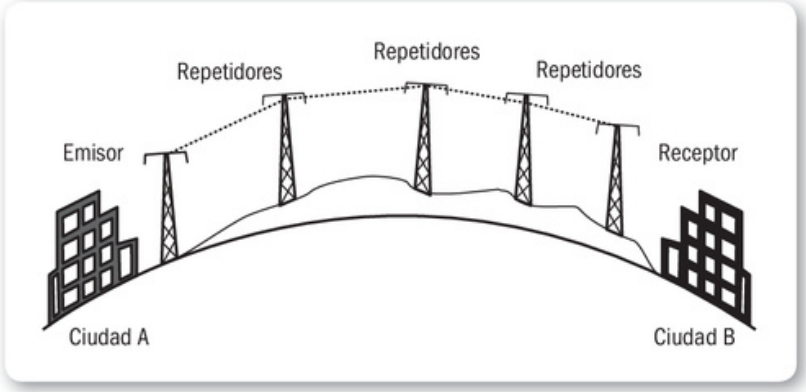


Figura 12. La imagen muestra cómo utilizar repetidores para lograr cubrir la distancia entre la ciudad A y B.

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 se retransmite esta nueva señal.

> LOS REPETIDORES ACTIVOS SON AQUELLOS QUE RECIBEN LA SEÑAL, LA AMPLIFICAN Y LA RETRANSMITEN EN ESTA NUEVA SEÑAL

En cambio, los repetidores pasivos repiten la señal sin cambiar nada. Simplemente se hace rebotar la señal recibida en una superficie espejo o acoplando dos antenas espalda con espalda (también llamado *Back to Back*).

Los repetidores pasivos se suelen utilizar cuando se necesita cambiar de dirección una señal y no es posible, o es muy costoso, instalar un repetidor activo en el lugar.

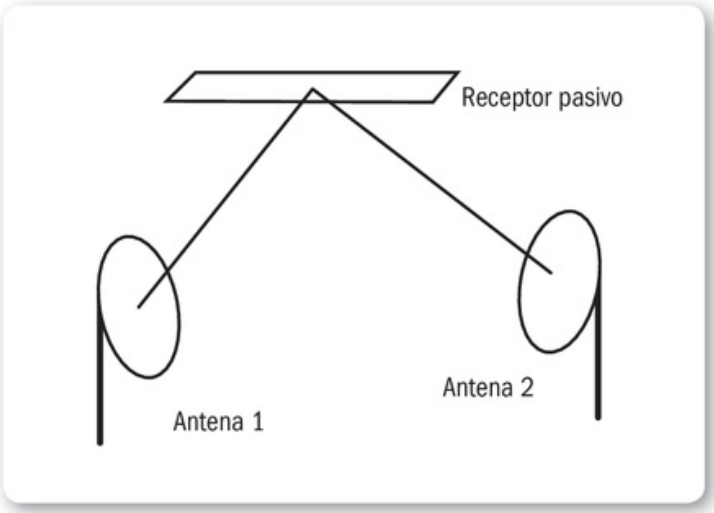


Figura 13. Vemos en la imagen una de las formas de implementar un radioenlace con un repetidor pasivo donde no se amplifica la señal.

ENLACE SATELITAL

Los satélites artificiales revolucionaron a las telecomunicaciones. Con ellos se difunde imágenes en directo y datos a larga distancia. En general, los satélites en orbitas a unos 35000 km (órbita geoestacionaria) están conformados por uno o más receptores y transmisores que cumplen la función de un enorme repetidor de microondas, como los usados en tierra.

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), según estemos uniendo un dos puntos o más.

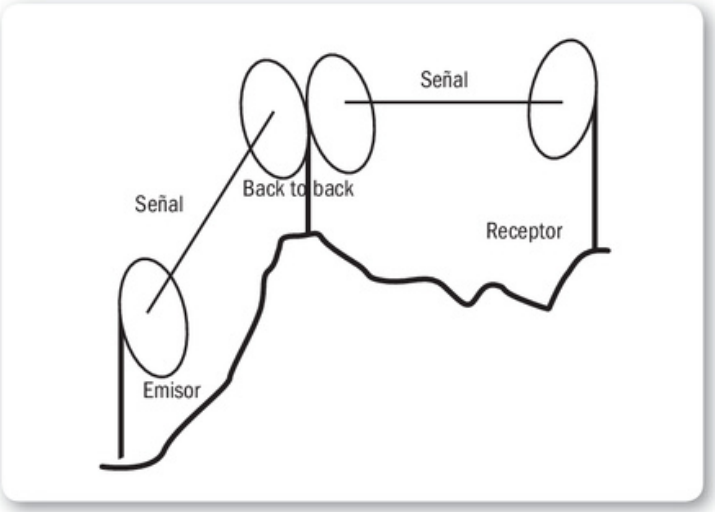


Figura 14. La señal puede ser amplificada (repetidor activo) o no (pasivo) para lograr llegar hasta el receptor.

Punto a punto

Solamente intervienen, en este tipo de enlaces, dos nodos. Estos nodos pueden ser de transmisión o de recepción, donde se interconectan simplemente dos computadoras o dos redes que existen en diferentes lugares distantes.

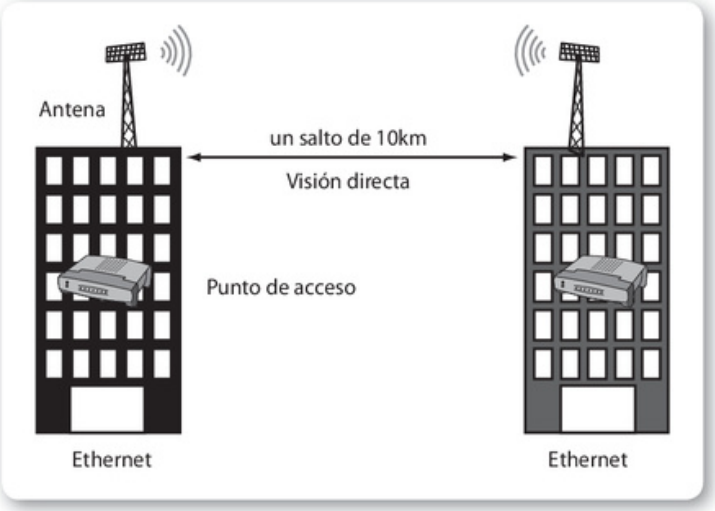


Figura 15. Se dice que un enlace punto a punto es simple cuando consta de un solo salto, es decir, la cantidad de sistemas que cuenta para lograr el destino.

Para este tipo de enlaces punto a punto, se utilizan **antenas direccionales**. Veremos con detalle todos los tipos de antenas en otro capítulo, pero acá vamos a describir las características de las antenas direccionales, de forma general.

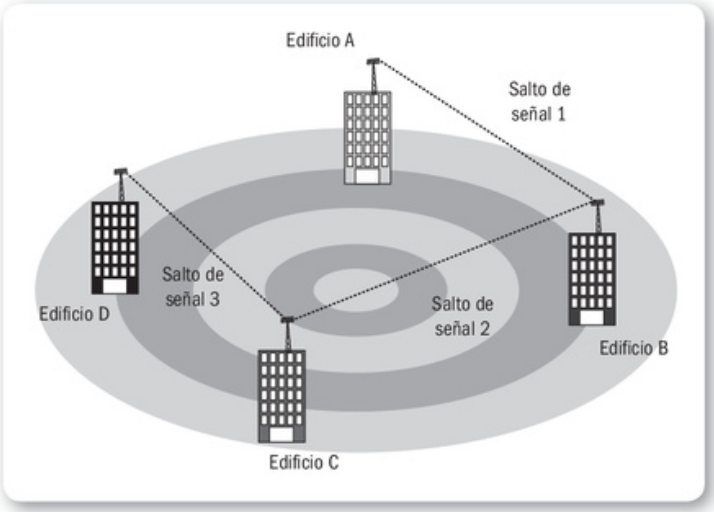


Figura 16. La imagen nos muestra un enlace punto a punto donde tenemos tres saltos de la señal para lograr el destino.

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 si están fuera de esta cobertura.

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 a unir. Sumado a esto, recordemos que la televisión satelital es otra área fuerte donde se usan satélites para difundir imágenes en movimiento, lo que hace que esta tecnología esté cada vez más cerca de las personas.



Figura 17. Antena parabólica usada para grandes distancias, con mejor rendimiento cuando necesitamos concentrar la información en una dirección.

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 de otro elemento, es un factor importante en los radioenlaces. Se define como la potencia, en decibeles o milivatios, que entrega el dispositivo emisor a la salida de la antena. Esta potencia es configurable en la mayoría de los equipos inalámbricos por medio del **software de gestión**. Hay variedad de antenas direccionales en el mercado, pero si se usan antenas parabólicas podremos alcanzar grandes distancias. Todo depende de los equipos utilizados y la información que vayamos a transmitir.

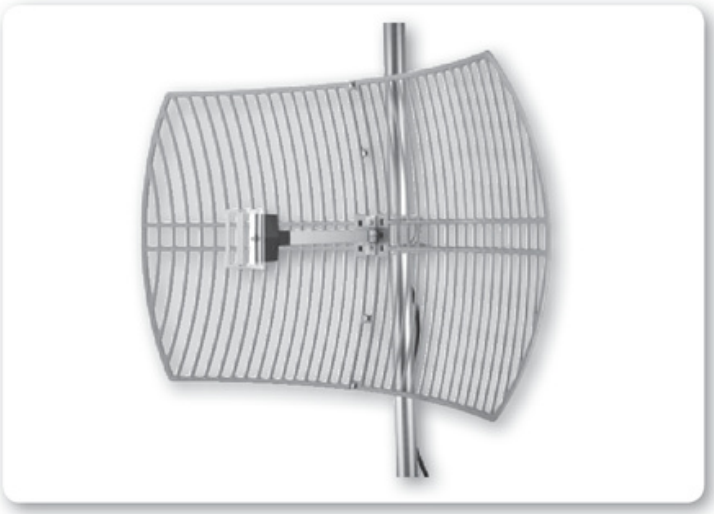


Figura 18. Esta antena direccional se llama **grid o parrila**. Es similar a la **parabólica convencional.**

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 que realiza 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.

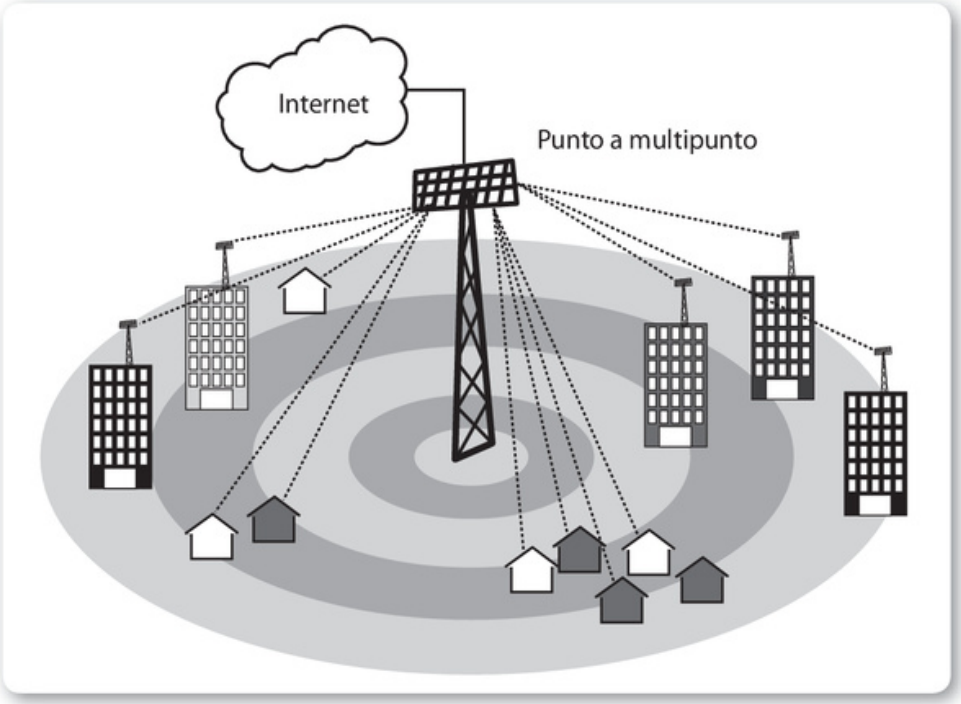


Figura 19. En un enlace punto a multipunto logramos zonas de cobertura para enlazar varios puntos.

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. Esta solución es muy precaria aunque resulta. De todas formas, existen otras soluciones en el mercado.

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

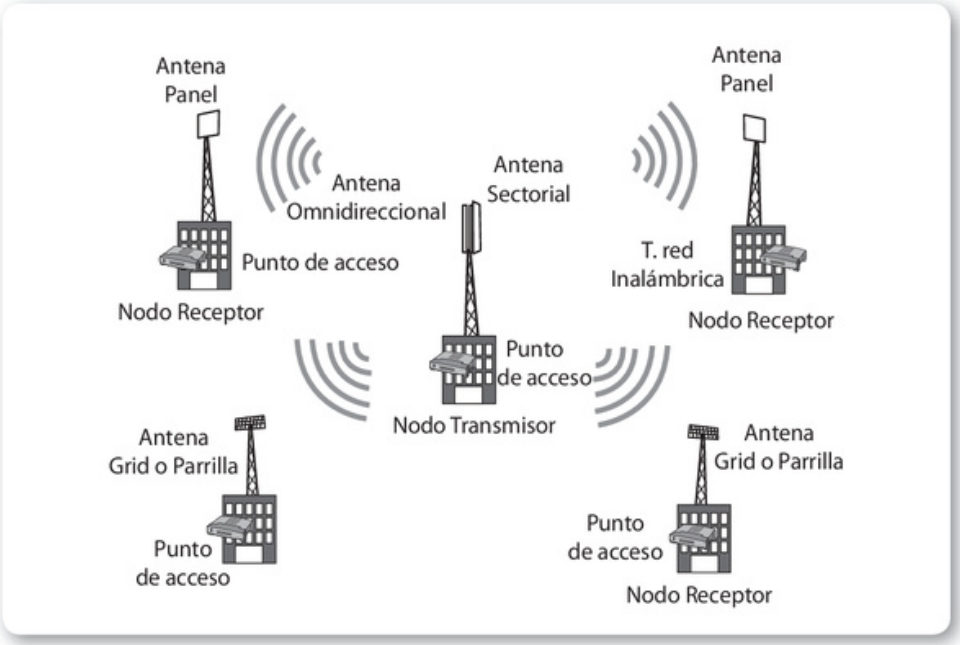


Figura 20. Como vemos en el diagrama, el enlace punto a multipunto es ideal para implementarlo en campus universitarios y edificios del gobierno esparcidos sobre un área local extensa.

Si vemos el lado del receptor, destacamos la utilización 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, mejor es 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 21. Las antenas sectoriales son de fácil fabricación y montado, lo que las transforma en antenas de bajo costo y gran rendimiento.

¿Qué necesito para llegar más lejos?

Ahora evaluaremos algunos puntos a tener en cuenta a la hora de pensar en realizar un enlace de larga distancia. Hablaremos de mejorar el presupuesto de potencia, considerar la distancia entre puntos a unir, verificar la existencia de línea visual entre los puntos, disminuir al máximo las perdidas posibles en conectores y cables de las antenas, evaluar el clima, mejorar la **sensibilidad del receptor** y considerar el tiempo de propagación de las señales inalámbricas por kilómetro como parámetros importantes.

Aclaremos algunos términos desconocidos como la sensibilidad del transmisor. Es un parámetro de los dispositivos inalámbricos que nos muestra el mínimo valor de potencia que necesita el receptor para poder **decodificar/extraer** la información enviada por el emisor y así alcanzar cierta velocidad de transmisión. Cuanto más baja sea la sensibilidad del dispositivo, mejor va a ser la recepción

de la señal. Tengamos en cuenta este parámetro importantísimo cuando compremos un dispositivo para nuestra red inalámbrica.

De la experiencia, concluimos que para llegar al receptor con una señal que nos dé un buen margen podemos realizar cualquiera de las siguientes acciones correctivas:

- Aumentar la potencia de transmisión en el equipo transmisor
- Incrementar la ganancia de las antenas utilizadas
- Reducir las pérdidas en los cables y conectores de antena
- Mejorar la sensibilidad del equipo receptor

Veamos un poco estos puntos.

Si aumentamos la potencia de transmisión tenemos que tener presente las **normas vigentes de nuestro país** en referencia a la potencia, ya que esto puede llevarnos a violar esas reglas.

Incrementar la ganancia de las antenas es la forma más práctica para optimizar el alcance. Lo único de debemos tener en cuenta es que el punto de acceso (o la placa inalámbrica en algunos casos) utilizado como transmisor tenga los conectores adecuados que permitan utilizar una antena externa. En el capítulo de antenas veremos en detalle los conectores y cables adecuados para antenas.

Lograr disminuir las pérdidas en los cables de antena es otro punto importante. Para conectar los dispositivos inalámbricos con la antena externa se usa un cable. A menos que el cable sea muy corto, lo habitual es que este cable que une el equipo con la antena sea un **cable coaxial** (similar a los usados en televisión, pero con algunas diferencias). Para conectar el cable a la antena y a los dispositivos inalámbricos, vamos a usar conectores específicos. Tanto el cable como cada conector utilizado añaden pérdidas a las señales de nuestro enlace.

Al preguntarnos cómo disminuir estas pérdidas, surge la respuesta obvia, usando cables y conectores de calidad. Además se aconseja



¿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.

usar un cable lo más corto posible y un número de conectores ajustado a la necesidad. Luego veremos en detalle los tipos de cables y conectores a usar en radioenlaces.



Figura 22. Un cable coaxial RG-58 utilizado en un enlace inalámbrico y su correspondiente conector.

Instalar el equipo cerca de la antena es una forma práctica de conseguir bajas pérdidas en los cables y conectores. Para esto se utilizan las llamadas **cajas estancas** (cajas para exteriores, donde los equipos que están adentro no se ven afectados por la lluvia o fenómenos similares). Veremos estas cajas en detalle en el capítulo de este libro, dedicado a las antenas.



Figura 23. Ejemplo de una caja estanca (para exteriores) modelo IP-67 que contiene un amplificador en su interior.

Por último, para mejorar la sensibilidad del equipo receptor seleccionaremos un equipo inalámbrico (punto de acceso, placa inalámbrica, entre otros) que se ajuste a nuestro proyecto. También podemos disminuir la velocidad de transmisión del enlace en nuestro transmisor y de esta forma mejoraremos nuestra sensibilidad en el receptor.

Consideraciones previas

Además de lo expuesto con referencia al equipo a utilizar y sus prestaciones, vamos a ver algunos factores a tener en cuenta que muchas veces son ajenos a nosotros y debemos conocer para poder optimizar al máximo nuestro enlace remoto e implementarlo de forma correcta y sin problemas.

Distancia

Para poder determinar cuál es la potencia y la sensibilidad necesarias en los equipos de transmisión y recepción, respectivamente, debemos considerar la distancia a la que se encuentran los puntos a vincular. Realizar esto es una tarea donde podemos usar algún dispositivo GPS (Sistema de posicionamiento global o *Global positioning system*) o el servicio de mapas que ofrece Google en Internet (**http://maps.google.com**). Más adelante veremos el uso del programa **Radio Mobile** que combina los mapas de Google para calcular distancias. Este software es un completo paquete de simulación de radioenlaces.



PÉRDIDAS POR LA LLUVIA

Factores atmosféricos y meteorológicos causan pérdidas en los radioenlaces. Durante la propagación de la señal en la tropósfera, se producen atenuaciones causadas por la absorción y dispersión en fenómenos como la lluvia, nieve o granizo. Esta atenuación se desestima para frecuencias por debajo de 5 GHz, pero se debe considerar para frecuencias superiores. El claro ejemplo de este fenómeno es la televisión satelital. Cuando el clima afecta la señal, tenemos degradación del servicio y hasta pérdida de la señal.

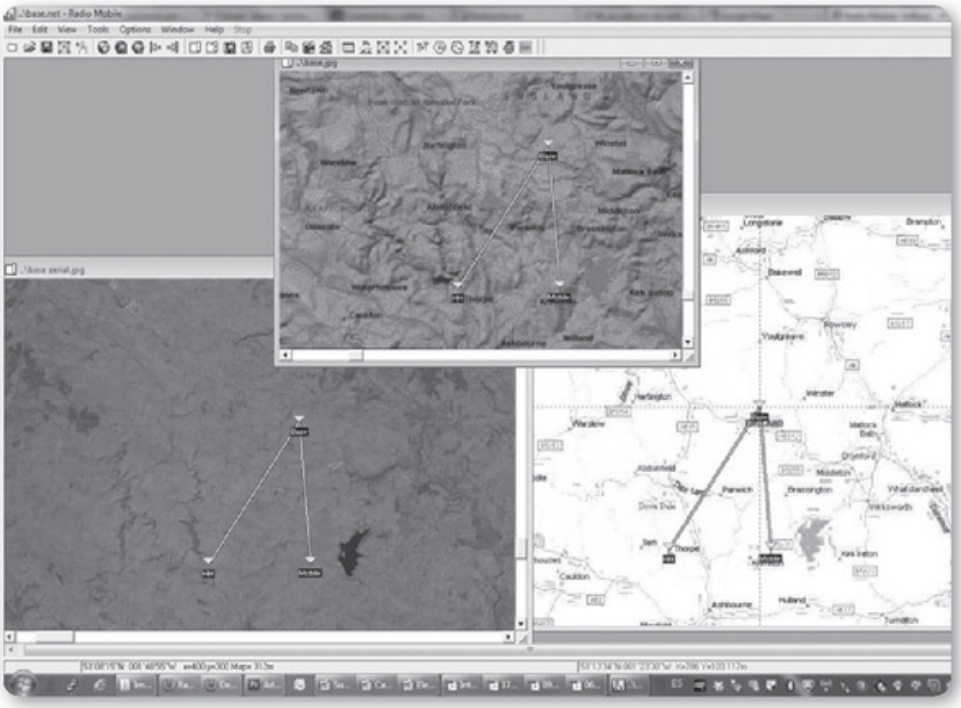


Figura 24. El programa **`Radio Mobile`** nos permite trabajar con mapas topográficos y calcular todo lo necesario para nuestro radioenlace.

Línea de vista

Es sabido que para concretar un enlace de larga distancia debe existir una línea de vista entre los puntos. Esto significa que entre los dispositivos no tiene que existir obstáculos, deben verse en línea recta.

Consideramos como obstáculos para nuestro enlace inalámbrico los árboles, las montañas, los edificios o las paredes, entre otros.

LA MÁS RENDIDORA

La antena panel es un tipo de antena direccional muy usada para compartir Internet. El diseño está basado en tecnología militar. Presenta la mejor relación ganancia/volumen ocupado y su rendimiento es del 85 a 90%. Estas antenas son similares a las antenas sectoriales usadas en comunicaciones móviles pero de un tamaño más reducido. Son de fácil construcción y cualquier usuario con mínimos conocimientos puede hacer una antena casera, en Internet tenemos mucha información y ejemplos de estas.



Figura 25. La línea de vista puede perderse por obstáculos en el medio que se sortearán eliminándolos o recalculando el trayecto.

Muchas veces podremos evitar los obstáculos elevando la altura de las antenas (también es posible agregar una torre a la antena para ganar altura). De todas formas, la línea de vista a distancias superiores a los 9 kilómetros se pierde debido a la curvatura de la tierra. De esta forma, para implementar enlaces con distancias mayores a 9 kilómetros se evaluarán la utilización de repetidores o el aumento considerable de la altura de las antenas. Esto último siempre que se pueda implementar, debemos tener cuidado de las condiciones climáticas y si la zona permite elevar la altura de la antena.

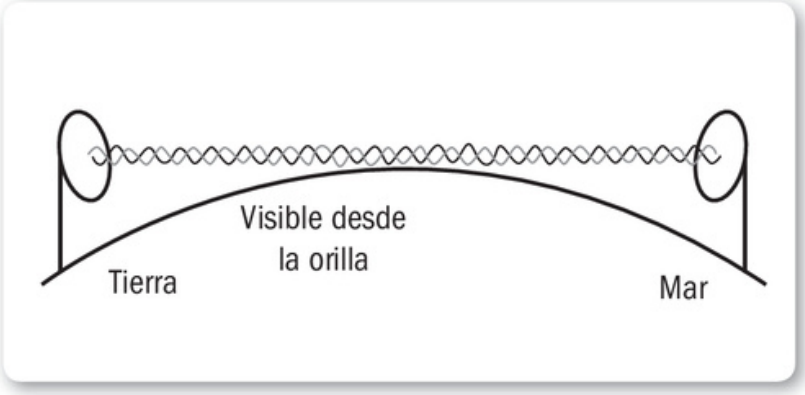


Figura 26. Para enlaces superiores a 9 km se debe tener en cuenta que la curvatura de la tierra va a influir en nuestro radioenlace.

Zona de Fresnel

Siempre tengamos presente que la **visión directa**, entre los puntos distantes de nuestro enlace, debe mantenerse permanentemente. Es habitual que se realicen enlaces inalámbricos que pasan cerca de árboles u otra vegetación similar, y más tarde son obstruidos porque la vegetación crece. Por este motivo, no es suficiente contar con la visión directa entre antenas para tener certeza de que nuestro enlace funcionará siempre y nuestra señal inalámbrica podrá estar libre de obstáculos. Dispondremos de un **margen de seguridad**, una zona con forma **elíptica** a lo largo de la visión directa entre los puntos. La zona de margen que obtendremos con este cálculo se llama **zona de Fresnel**.

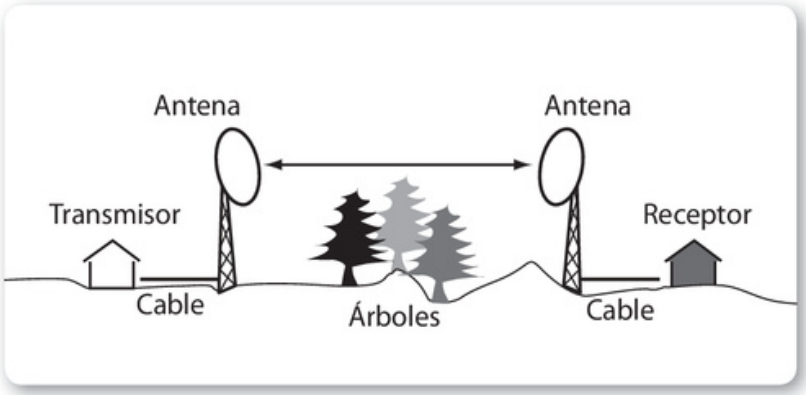


Figura 27. Vemos cómo evitar que la vegetación del lugar obstaculice nuestro enlace al utilizar torres para las antenas.

En general, la zona de Fresnel tiene una anchura que depende de la longitud de onda de la señal (para nuestro caso, donde utilizamos ondas en la frecuencia de 2,4 GHz, es de 12,5 cm), y la distancia a cubrir.

CALCULADORA DE FRESNEL

El volumen de espacio entre el emisor y el receptor en un radioenlace se llama **Zona de Fresnel** en nombre del físico Augustin-Jean Fresnel. El cálculo de ésta zona no es difícil pero lleva tiempo, para ahorrarnos esfuerzo podemos utilizar una calculadora online de la Zona de Fresnel si ingresamos en **http://wisp-router.com/wirelesscalculators.php#fresnel**.

Si necesitamos llegar al equipo receptor con el máximo de señal posible, vamos a disponer de una zona mayor, denominada **segunda zona de Fresnel** como parámetro principal.

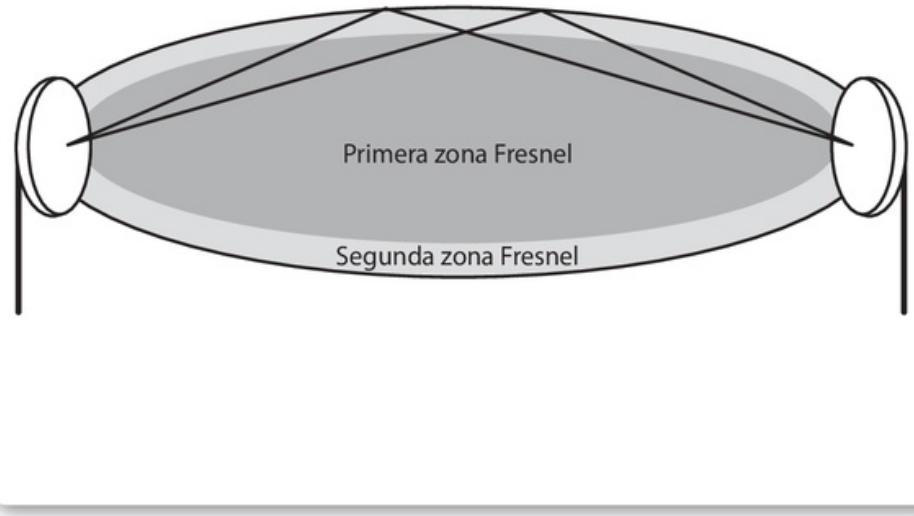


Figura 28. Vemos de forma práctica la representación de la primera y segunda zona de Fresnel.

Estas zonas deben considerarse en los cálculos de radioenlaces.

TABLA 1

▼ DISTANCIA	▼ 100 M	▼ 500 M	▼ 2 KM	▼ 10 KM
1ra zona de Fresnel	3,5 m	8 m	16 km	35 km
2da zona de Fresnel	5 m	12 m	22 km	50 km

Tabla 1. Valores de la primera y segunda zona de Fresnel para nuestro enlace inalámbrico de 2.4 GHz según diferentes distancias.



Figura 29. Al considerar la zona de Fresnel, vemos que existe una línea de vista de nuestra óptica y una línea de vista de radio.

Clima

Cuando el hielo, la nieve o fenómenos similares caen sobre nuestras antenas producen un **impacto** negativo. Directamente se ve perjudicado el rendimiento de la antena dado que cuando ocurre una lluvia persistente y pesada sobre paneles planos se crea una **película** de agua que actúa negativamente. También las **tormentas eléctricas** con relámpagos y rayos son peligrosas. En caso de que un rayo caiga en la antena puede producirse algún desperfecto. Para evitar estas situaciones, recomendamos utilizar dispositivos protectores contra rayos y así atenuar las posibles consecuencias a sufrir.

> LOS CLIMAS SECOS Y ÁRIDOS SON LOS ÓPTIMOS PARA REALIZAR UN RADIOENLACE DE LARGA DISTANCIA

En zonas donde se desarrollan fuertes vientos, nuestras antenas pueden **desalinearse** y perder la orientación óptima que precisa el radioenlace. El impacto de estos **ventarrones** en nuestras antenas pueden atenuarse si utilizamos antenas tipo parrilla para evitar que el aire se embolse en el plato de la antena.

Si la zona donde implementamos el enlace es propicia a sufrir tormentas de arena tendremos que tener en mente que este tipo de fenómenos puede atenuar la señal hasta un valor cercano al 90%. Es el fenómeno más perjudicial. Para resumir, los climas secos y áridos son los óptimos para realizar un radioenlace de larga distancia mientras que los climas húmedos no son tan buenos.

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 suponemos 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. Simplemente deberemos **alinear visualmente** ambas antenas y constatar los resultados con alguna herramienta.

Vimos herramientas como **NetStumbler** anteriormente y en este caso también la podremos utilizar. Con ella vamos a medir la **intensidad de la señal** en el receptor para así realizar un ajuste fino de la orientación de la antena. Siempre buscamos obtener el máximo punto de recepción.

Si trabajamos en equipo junto con otra persona, podremos comunicarnos por medio de un **celular** para hacer las correcciones necesarias estando ambos puntos distantes.

Algunas herramientas que podemos usar para orientar las antenas son:

- Teléfono celular o similar para comunicarnos con el otro extremo del enlace de forma práctica.



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 a utilizar. En zonas rurales no hay mucha congestión en la banda de 2.4 GHz como en las ciudades.

• 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 sea 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 (tener en cuenta que algunos programas pueden indicar el nivel de señal recibida como un porcentaje, en este caso mientras mayor sea el porcentaje, mayor será la señal). Es común confundirse con estos parámetros.

Realizamos lo siguiente:

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 encontremos el **máximo**, dejamos fija la antena del extremo 2 asegurándola con alguna **abrazadera** o similar que tengamos.

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, efectuamos lo mismo en el extremo 1. Muchas veces es necesario repetir el procedimiento para lograr el punto óptimo.

Ahora tenemos la posibilidad de realizar pruebas de transmisión haciendo uso del comando **ping**, y así ver las pérdidas de **paquetes** y el tiempo de transmisión existente.

Con extremos no visibles

En caso de no tener los extremos visibles (puede ser porque nuestro enlace es muy extenso), la alineación de las antenas lleva un poco más de tiempo. Además de lo listado anteriormente podemos llegar a necesitar los siguientes elementos:

- Un GPS, que nos sirve para medir la distancia de los puntos y la altura del terreno que tengamos.
- 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.

Existen otros métodos más elaborados que escapan al objetivo de este libro y no desarrollaremos y no los desarrollaremos.

Cálculo de enlace

Hasta ahora recomendamos realizar una correcta selección del equipo que vamos a utilizar y liberar una zona determinada del enlace (zona de Fresnel), que nos asegure la correcta propagación de la señal de un extremo al otro. Sin embargo, siempre es necesario realizar otros cálculos para no gastar dinero extra en equipamiento e implementar nuestro enlace sin causar problemas a otros usuarios del **espectro radioeléctrico** compartido.

Presupuesto de potencia

Un **presupuesto de potencia** de una enlace punto a punto es el cálculo de todas las ganancias y pérdidas desde el transmisor (origen de los datos a enviar), pasando por los cables, los conectores y el espacio libre hasta el receptor. Si logramos **estimar** con este simple cálculo el valor de la potencia en las diferentes partes del radioenlace, vamos a conseguir un mejor diseño y uso del equipamiento.

Es común escuchar que el presupuesto del enlace es como el **cimiento** en una construcción. Si el cimiento es débil, no importa que tan bien hechas estén las paredes y el techo, la edificación se caerá.

Vamos a dividir en tres partes el presupuesto del enlace:

1) Lado de transmisión
2) Lado de propagación
3) Lado de recepción

En el presupuesto del enlace simplemente se realiza la suma de todos los aportes (tenemos que usar la unidad **decibeles** para todos los valores) en el camino de las tres partes descriptas anteriormente.

Así vamos a tener una fórmula que expresa la cantidad total de señal que es generada por el transmisor y los componentes pasivos y activos en el camino entre los dos extremos, en relación a la cantidad de señal requerida para la recepción de la señal.

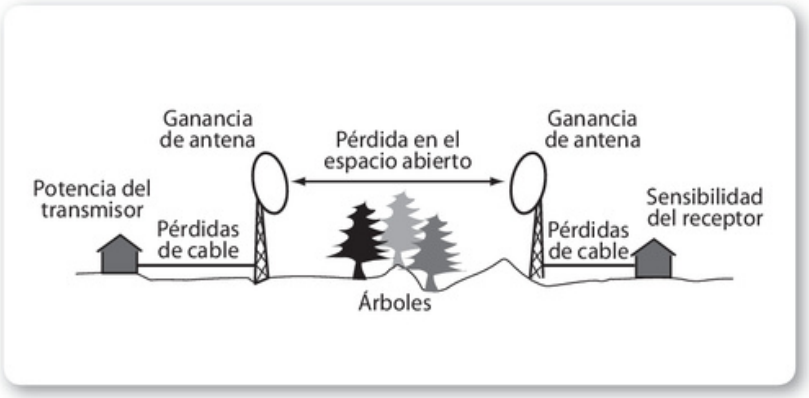


Figura 30. Vemos los puntos involucrados en la fórmula del presupuesto del enlace.

De esta forma, el presupuesto del enlace se formula recolectando los valores desde la izquierda de la imagen hasta llegar al receptor:

Potencia del transmisor [valor en dBm] – pérdida en el cable [dB] + ganancia de antena [dBi] – pérdidas en el espacio abierto [dB] + ganancia

RADIO MOBILE, LA SALVACIÓN

Este programa gratuito nos permitirá realizar los cálculos y obtener todos los datos necesarios para implementar nuestro radioenlace. Así, no tendremos que realizar la tediosa tarea de calcular a mano, conseguir mapas topográficos y verificar los posibles obstáculos del terreno. El programa se puede obtener en **http://radiomobile.pe1mew.nl**.

CON EL PROGRAMA GRATUITO RADIO MOBILE VAMOS A PODER SIMULAR NUESTRO RADIOENLACE

de antena [dBi] – pérdidas en el cable [dB] >= sensibilidad del receptor [dBm]

Recordemos que el símbolo >= significa **mayor o igual que**.

Ya vimos qué significaba la potencia del transmisor, la sensibilidad en el receptor y las ganancias. Las pérdidas en los cables pueden consultarse a los **fabricantes** en sus hojas de datos, así como para los conectores (en general, el valor ronda los 0.25 db por conector). Las pérdidas en el espacio libre se calculan con una fórmula que no veremos en este libro; de todas formas, resumimos algunos valores en la siguiente tabla que son de utilidad.

TABLA 2

▼ DISTANCIA \ FRECUENCIA	▼ 915 MHZ	▼ 2.4 GHZ	▼ 5.8 GHZ
1 km	92 dB	100 dB	108 dB
10 km	112 dB	120 dB	128 dB
100 km	**132 dB**	**140 dB**	**148 dB**

Tabla 2. El valor que nos interesa es el reflejado para la frecuencia de 2.4 GHz.

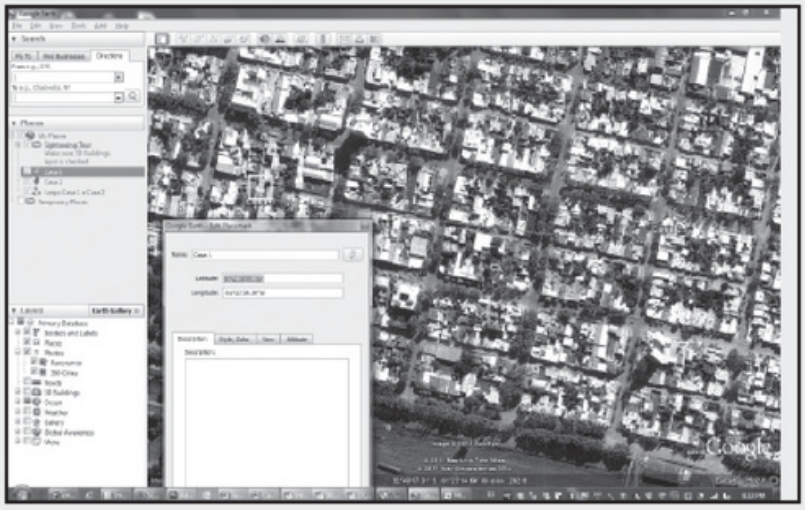
Cálculo con Radio Mobile

Con el programa gratuito Radio Mobile vamos a poder **simular** nuestro radioenlace. Sirve para enlaces que operan dentro del rango de 20 MHz a 20 GHz. Siguiendo las instrucciones que detallamos a continuación, podremos efectuar los **cálculos** y ver si nuestro enlace es **factible** de realizar. Tomaremos un enlace entre dos casas donde el equipo transmisor compartirá Internet con el receptor. La distancia entre los puntos es de 400 m, aproximadamente.

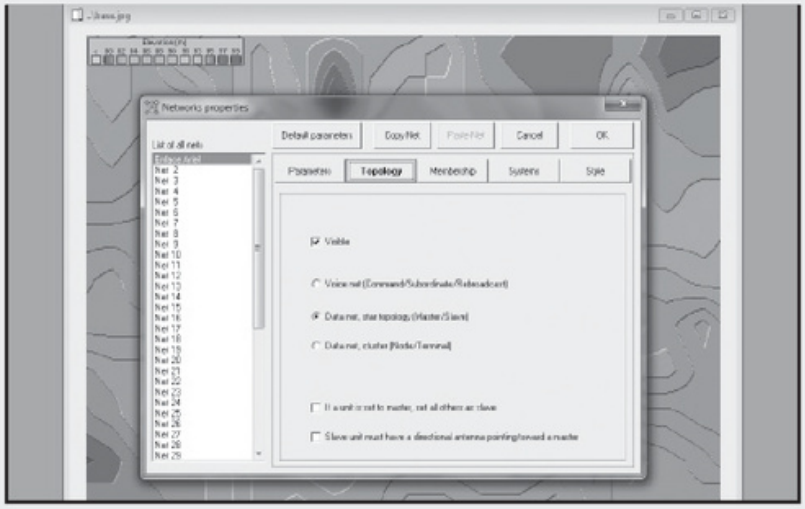
Antes de comenzar debemos descargar e instalar el programa, podemos bajarlo desde **http://radiomobile.pe1mew.nl** o buscarlo directamente en Internet.

CALCULAR ENLACE CON RADIO MOBILE

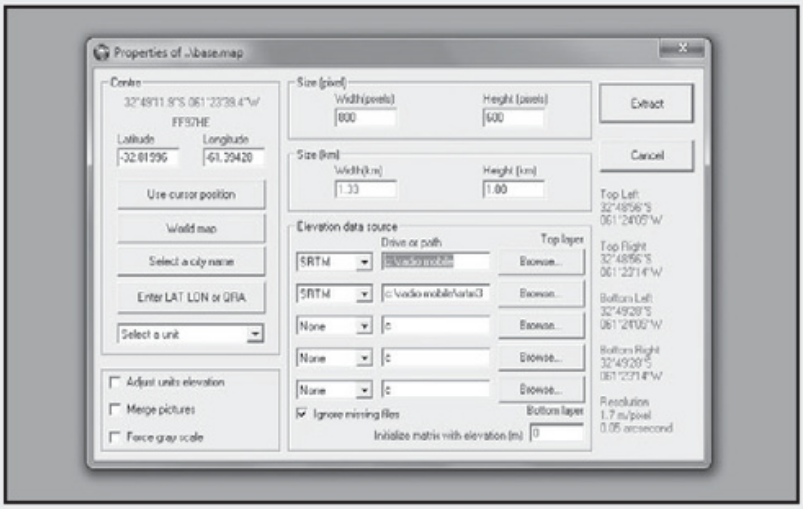
01 Necesita tener las coordenadas del punto transmisor y del punto receptor. Utilice un GPS o Google Earth para obtenerlas. La figura siguiente muestra los puntos a utilizar marcados en Google Earth y sus correspondientes coordenadas.



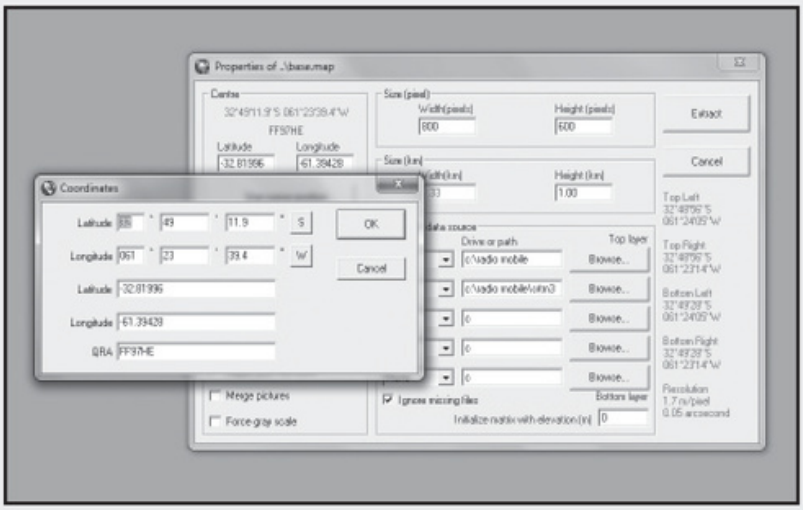
02 En el programa Radio Mobile, vaya a el menú `File` y luego a `Map Properties`. Ahora deberá ingresar uno de los valores de coordenadas obtenidas anteriormente. Con las coordenadas para uno de nuestros extremos crearemos un mapa.



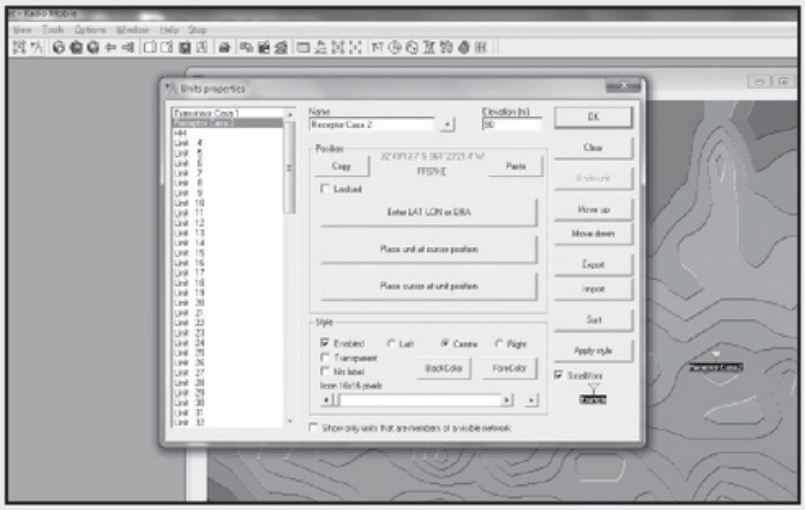
03 En la nueva ventana, vaya a `Elevation data source`, indique el formato de los datos y la carpeta donde instaló el programa Radio Mobile (ahí se encuentran los mapas). Haga clic en `Browse` y busque la carpeta. Seleccione el tamaño del mapa en `Size`. Para este caso se usa `1` km, que permite tener una buena visión del enlace. Es necesario ingresar el centro del mapa, donde dice `Centre` introduzca un valor cercano a sus coordenadas.



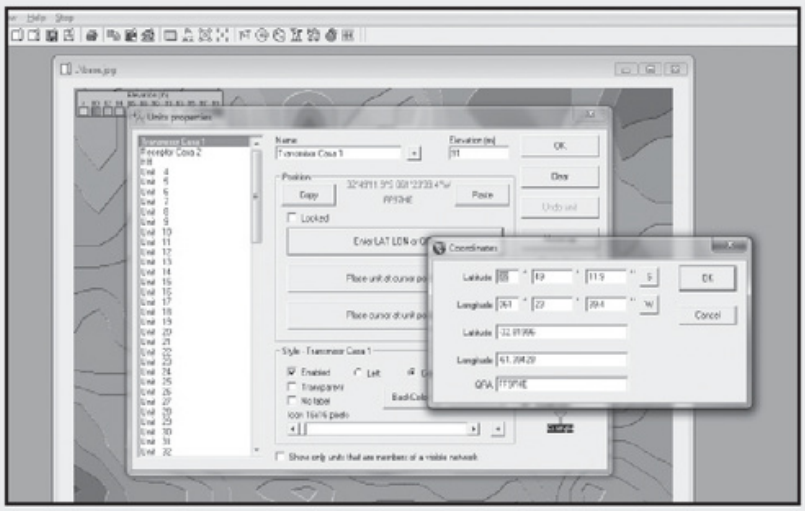
04 Luego tiene que ingresar las coordenadas de los puntos a enlazar en el mapa. Haga clic en `Enter LAT LON o QRA`. Ingrese sus coordenadas y tenga cuidado de no equivocarse. Cuando finalice, presione OK y en la ventana anterior haga clic sobre `Extract` para obtener el mapa según coordenadas.



05 Ahora tiene el mapa de su región donde realizará el enlace con sus elevaciones. El próximo paso es crear los puntos del enlace en el mapa. Haga clic en `Unit Properties` de la barra de herramientas como muestra la figura.



06 En esta nueva ventana, seleccione una de las 50 unidades disponibles para definir un punto del enlace. En `Name` ingrese el nombre del extremo transmisor. En el ejemplo se usa `Transmisor Casa 1`. Haga clic en `Enter LAT LON o QRA` e ingrese las coordenadas correspondientes a ese punto transmisor y luego presione OK. A continuación, seleccione otra unidad para el receptor y repita este procedimiento.



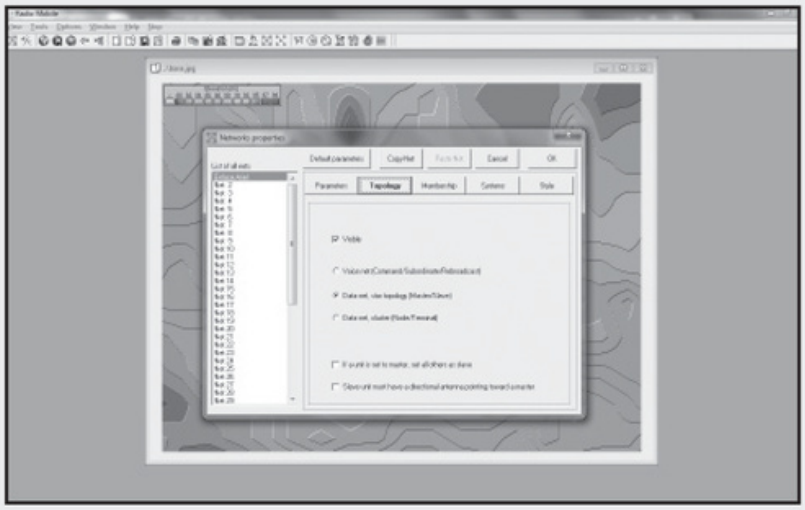
07 Haga clic en OK en la ventana `Unit properties` y los puntos aparecerán en su mapa según las coordenadas que ingresó, tal como muestra la imagen.



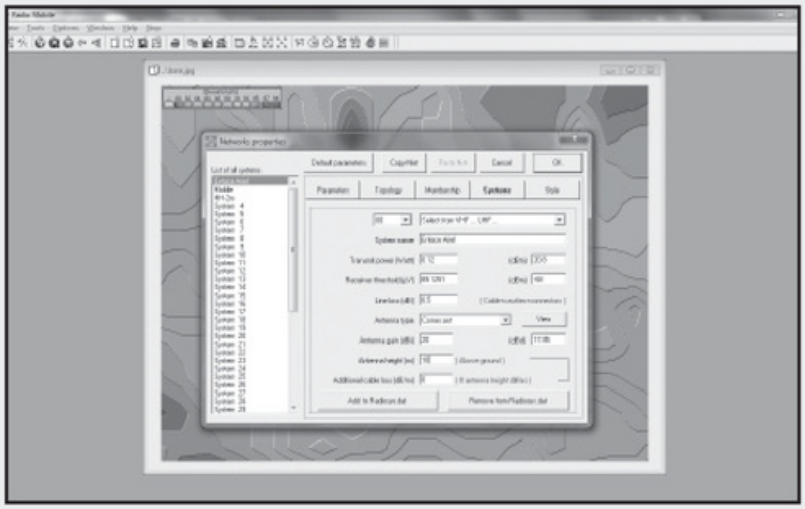
08 En la barra de herramientas haga clic en el icono de `Networks properties` para crear la red. Seleccione la pestaña `Parameters` e ingrese el nombre de la red en `Net name` y el rango de frecuencia en el que operará el enlace. En su caso ingrese 2400 a 2484.5 Mhz, según el ejemplo.



09 Seleccione la pestaña Topology, en la que seleccionará la topología del enlace punto a punto. En este caso es un enlace de Datos, Maestro (transmisor) y Esclavo (receptor).



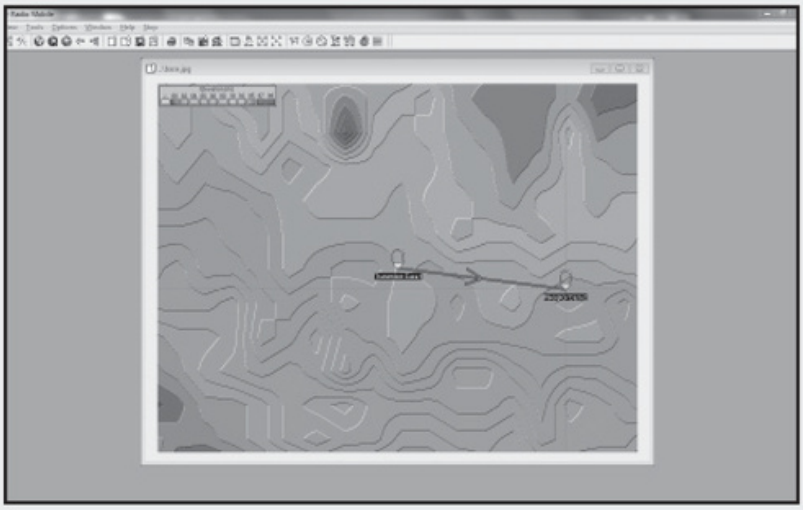
10 Diríjase a la pestaña Systems, donde configurará el sistema, o sea introducirá las características y especificaciones de los equipos (algo que tiene que conocer con anterioridad). Ingrese el nombre del sistema en System name y las características de los equipos. La imagen muestra los datos usados para el enlace de este ejemplo.



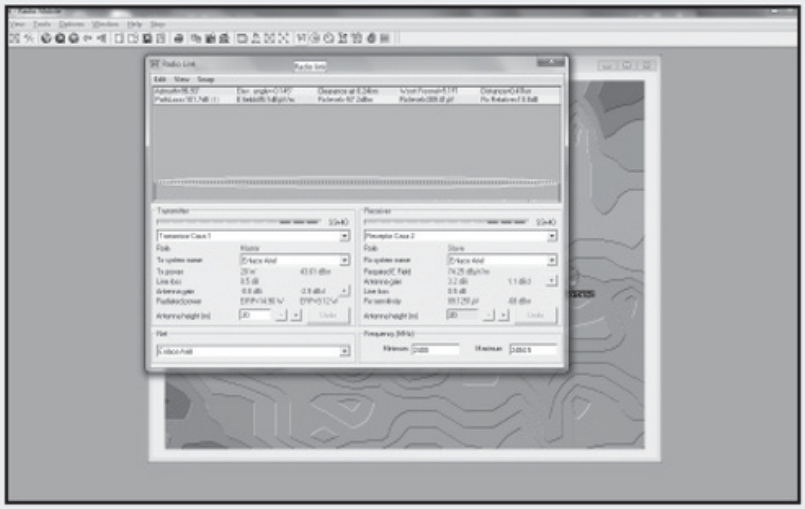
11 Ahora vaya a `Membership`, donde definirá los roles de cada elemento. Primero seleccione el transmisor de la lista y defina el rol de Maestro en el sistema que usted creó. Configure el rol del receptor de igual manera, pero defina el rol de Esclavo para el mismo sistema. Luego presione OK.



12 Aparecerán en el mapa los puntos y una línea que indica el enlace. Si es factible con los datos ingresados, la línea será verde, sino será roja. Si nuestros enlaces no son posibles, se debe revisar los sistemas y mejorar la potencia de salida del transmisor, la sensibilidad o demás parámetros vistos.



13 Por último podrá ver un perfil del enlace para determinar la correcta altura de las antenas y las zonas de Fresnel. Haga clic en el ícono de `Radio Link` en la barra de herramientas para esto.



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 y 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 Duplex?
5. ¿Cómo se representa la topografía de un lugar?
6. ¿Qué es la sensibilidad del transmisor?
7. ¿Cuáles 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?

PRÁCTICAS

1. 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 posible el enlace anterior.

*07

Enlaces de corta distancia

Las redes inalámbircas son enlaces de corta distancia. Anteriormente definimos a una red inalámbrica como un vínculo entre dos o más terminales que se comunican sin la necesidad de utilizar cables. 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 en varias categorías a las redes inalámbricas. En este capítulo, estudiaremos las redes inalámbricas de área personal.

- **Red inalámbrica de área personal 246**
  - Los grupos de trabajo de la IEEE .. 247
  - ¿Dónde se aplica la tecnología WPAN? 248
  - Tipos de WPAN 249
  - Principio básico de funcionamiento 250
  - Tecnologías usadas en WPAN 250
- **Bluetooth: ¿qué es y cómo funciona? 253**
  - Topología de red 256
  - Seguridad 257
  - Vulnerabilidades 259
- **Resumen 261**
- **Actividades 262**

Red inalámbrica 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 utilizar cables. Estas redes WPAN conectan dispositivos como impresoras, teléfonos celulares, electrodomésticos, notebooks, agendas, entre otros, sin la necesidad utilizar cables.

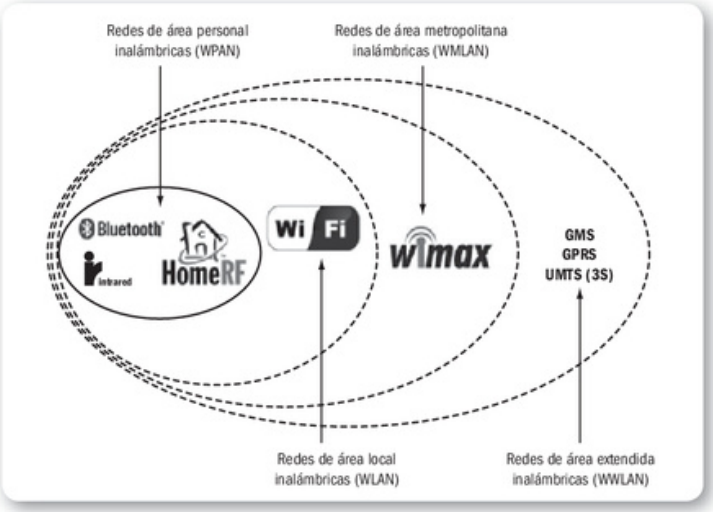


Figura 1. Una red inalámbrica de área personal se desarrolla en el ámbito hogareño donde el área de cobertura no supera los pocos metros.

Las comunicaciones punto a punto de corta distancia pueden ocurrir ya que, comúnmente, no se requiere de altos índices de transmisión de datos. Un ejemplo es la tecnología **Bluetooth** (que veremos más adelante en este capítulo), en la que el área de cobertura es de unos 10 metros y los datos se transfieren con una velocidad de 1 Mbps. 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 implementada), podemos usar nuestros teléfonos y demás dispositivos sin preocuparnos por el gasto de nuestra batería.



Figura 2. Las WPAN son redes que tiene como centro al usuario y que permiten la comunicación entre sus dispositivos personales y el mundo exterior.

Estas redes nacieron de la necesidad que tenían los usuarios de poder crear una forma rápida, confiable y eficiente para transferir información sin los molestos cables que vinculan nuestros dispositivos hogareños hoy en día. Esta solución tomó el nombre de WPAN y posee 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.

El estándar **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 veremos de forma general nombrando algunas características específicas.

* **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 día 14 de junio del año 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 soluciones de bajo costo. Se quieren lograr velocidades de 20 Mbps o 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): este grupo se ocupa de todos los puntos necesarios para formar una red con topología en malla usando la tecnología WPAN. Este estándar es del año 2009.

¿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,



BLUETOOTH

La tecnología que hoy en día más se usa en redes WPAN es **Bluetooth**, que fue lanzado por la empresa Ericsson en el año 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. Más adelante, veremos más sobre este tema.

sistemas de calefacción, ventilación, aire acondicionado y portones que utilizan 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.

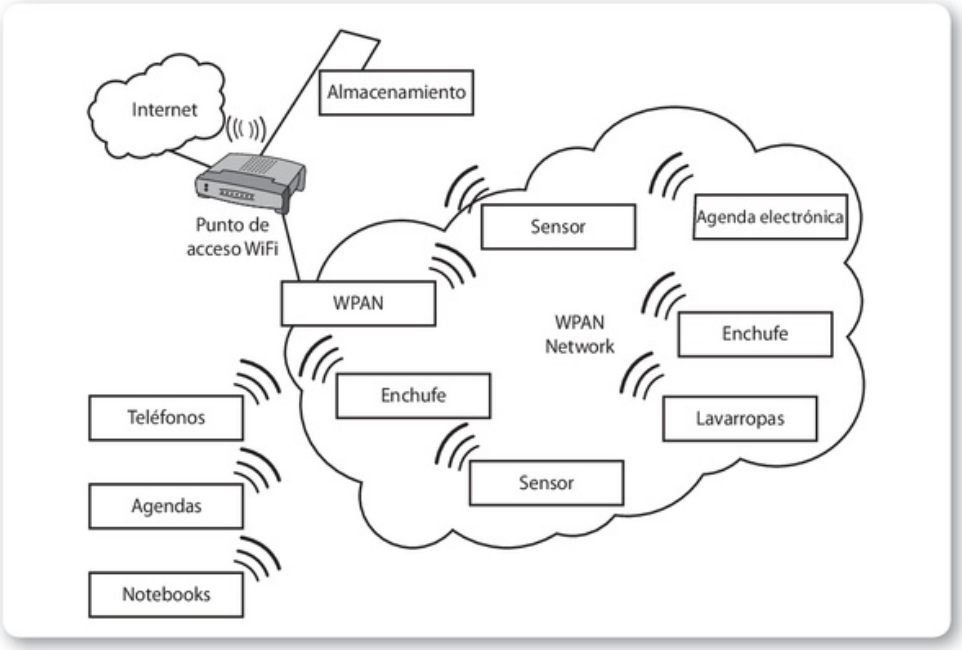


Figura 3. En un hogar del futuro podremos tener control total utilizando la tecnología que nos provee una WPAN. La imagen muestra el vínculo con Internet que puede existir.

Tipos de WPAN

Según vimos antes, la IEEE 802.15 definió tres clases de redes inalámbricas de área personal. La diferencia sustancial que existe entre estas es su consumo de energía y la velocidad. Así tenemos:

- **IEEE 802.15.3**: WPAN que necesitan mucha velocidad.
- **IEEE 802.15.1**: WPAN que trabajan con un rango medio de velocidad (celulares y agendas electrónicas).
- **IEEE 802.15.4**: WPAN que trabajan con baja velocidad de transmisión. También son llamadas **LR-WPAN** (*Low rate-wireless personal area network*, en inglés).

Es importante identificar cada una de éstas tecnologías.

Principio básico de funcionamiento

Para establecer una comunicación entre dos elementos en una red WPAN, en general, debe existir un dispositivo principal (llamado **maestro**) y uno secundario (llamado **esclavo**). En estas redes, la conexión es iniciada por un dispositivo y dura tanto como sea necesario. Así, si queremos transferir un archivo entre dos teléfonos celulares, la conexión durará hasta que el archivo sea transferido de un teléfono al otro. Al finalizar la transferencia, la conexión creada se puede terminar si se desea.

En una red WPAN, no existe un registro de los dispositivos a los que nuestro celular, siguiendo con el ejemplo, se conectó o a los que vaya a conectarse. Si, por ejemplo, luego de terminar la transferencia del archivo, deseamos enviar por e-mail esa información, nos conectaremos a nuestra computadora. Así crearemos rápidamente una nueva conexión con este dispositivo.



Figura 4. Tener una conexión rápida y eficiente sin mucho despliegue es una característica importante de las WPAN.

Tecnologías usadas en WPAN

Para implementar las WPAN se desarrollaron diferentes tecnologías, las cuales con el paso del tiempo fueron tomando mayor influencia en el uso cotidiano. Veamos algunas de estas tecnologías y sus principales características.

* **Bluetooth**: esta tecnología está presente en muchos de los dispositivos que actualmente encontramos en el mercado. Permite la transmisión de **voz y datos** entre diferentes dispositivos. Con

esta tecnología, se busca eliminar cables y conectores entre equipos móviles y fijos, además de facilitar la creación de WPAN para sincronizar datos entre dispositivos. También se la conoce como IEEE 802.15.1. Tiene **bajo consumo** de energía, lo que extiende la duración de la batería en el caso de los celulares. Veremos con mayor detalle esta tecnología más adelante.

* **HomeRF**: fue un estándar lanzado en 1998 por el HomeRF Working Group, integrado por fabricantes como HP, Compaq, Intel, Motorola y otras 100 empresas más. HomeRF (*Home Radio Frecuency*) ofrecía una velocidad de 10 Mbps para un área de cobertura de 50 a 100 metros. Este proyecto se abandonó en el año 2003, luego de que el estándar IEEE 802.11b se implementara para usuarios hogareños, y la empresa Microsoft comenzara a incluir el soporte para Bluetooth (competencia del HomeRF) en su sistema operativo Windows. Consecuencia de esto, HomeRF quedó **obsoleto**.

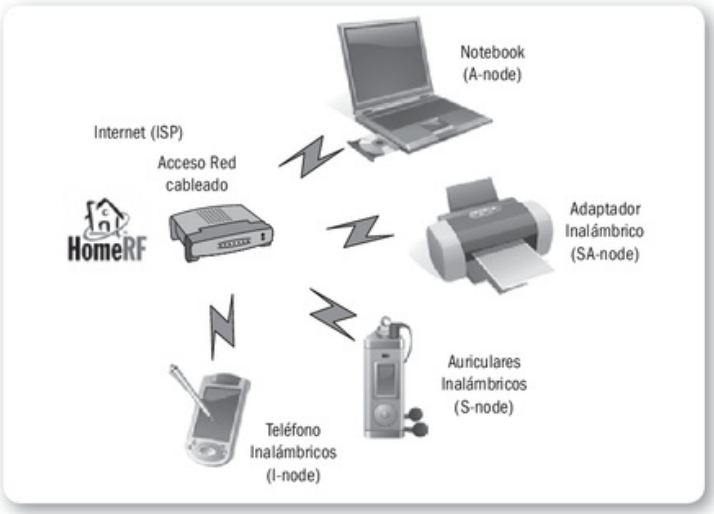


Figura 5. Dispositivos utilizados en una red implementada con la tecnología **HomeRF**.

* **ZigBee**: es una especificación que aglomera un conjunto de protocolos destinados a la comunicación inalámbrica de bajo consumo. Se basa en el estándar IEEE 802.15.4 para redes WPAN. Con esta tecnología se pretende **extender** la vida de las baterías, ya que tiene bajo consumo de energía (algunos fabricantes garantizan que se puede lograr una autonomía de hasta 5 años antes de cambiar la batería). Se utiliza en electrodomésticos, sistemas de audio, juguetes o similares. Funciona en la banda de frecuencias de 2.4 Ghz y puede

alcanzar velocidades de transferencia de datos de hasta 250 Kbps, logrando un alcance de 100 metros. No veremos esta tecnología en detalle porque escapa a los objetivos del libro. En Internet existe buena cantidad de material sobre esto.

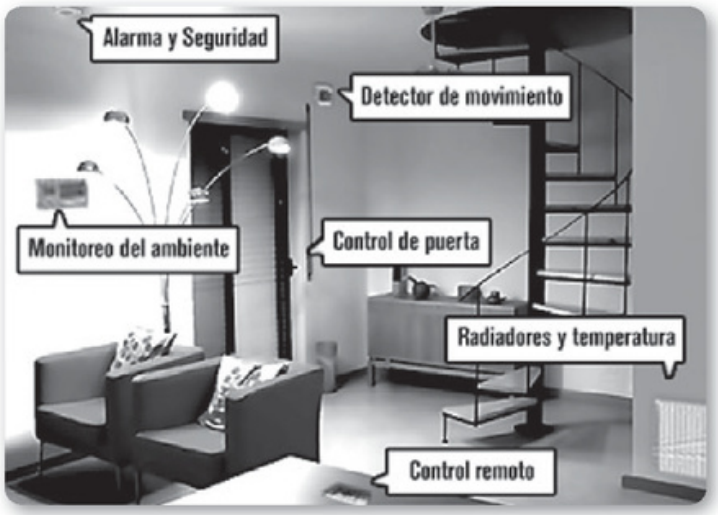


Figura 6. La domótica (término que hace referencia a la automatización del hogar) es uno de los principales usos de la tecnología ZigBee.

* **Infrarrojo**: se utiliza para crear conexiones inalámbricas de unos escasos metros. Las velocidades alcanzadas pueden llegar a pocos megabits por segundo. Encontramos esta tecnología en dispositivos hogareños (el más común es el control remoto de nuestra **TV** o reproductor de **DVD**). Es muy común sufrir **interferencias** con esta tecnología. También es habitual el uso como un sensor infrarrojo para los microondas (lo que permite medir la distribución de la temperatura en el interior) o para el control climático de una casa otros diferentes usos que se le puede dar.

INFRARROJO EN EL AUTO

Los **sensores infrarrojos** son muy usados en la industria automovilística para la seguridad y el confort. Tareas como monitoreo del tráfico, de neumáticos y frenos o detección de los ocupantes para activar los airbags inteligentes (sistemas de seguridad ante un choque) son algunas de las tantas aplicaciones donde los sensores infrarrojos tienen un importante rol. Actualmente, siguen desarrollando adelantos para esta industria utilizando sensores infrarrojos.

Bluetooth: ¿qué es y cómo funciona?

Para empezar a comprender todo sobre Bluetooth, conozcamos la historia de esta tecnología. En el año 1994, la empresa 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 los 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 fácil transmisiones de voz y datos entre dispositivos. Bluetooth se puede incorporar en la gran mayoría de los aparatos electrónicos y ofrecer una nueva forma de comunicación sin necesidad de cables, es compatible con cualquier fabricante (conseguimos la **interoperabilidad** entre diferentes dispositivos).

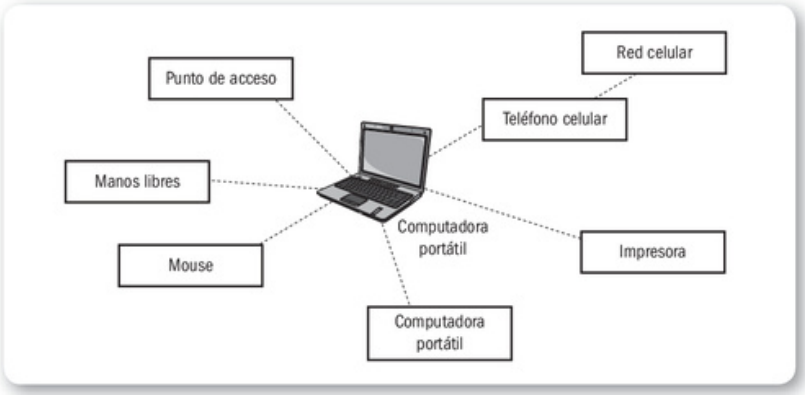


Figura 7. Ejemplo de la conectividad Bluetooth, se intenta alcanzar la conectividad total para dispositivos de la casa y oficina.

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).

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

TABLA 1

▼ 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. La tabla nos muestra el área de cobertura según la potencia utilizada por cada clase para Bluetooth.

Existe también una clasificación según el **ancho de banda** de cada una de las versiones estandarizadas de la tecnología Bluetooth. No veremos esta clasificación porque escapa a los objetivos de este libro. Para saber más podemos entrar en **www.bluetooth.com**.

Veamos algunas cuestiones técnicas de Bluetooth. Se utiliza un canal de comunicación de máximo 1 Mbps de capacidad bruta, obteniendo así un área de cobertura óptima de 10 m (se puede lograr mayor cobertura usando repetidores). Tal como era de esperar, la frecuencia de trabajo de Bluetooth está dentro del rango de 2.4 Ghz (para ser más específicos entre 2.4 Ghz y 2.48 Ghz). Se puede transmitir en Full Duplex y utilizando la tecnología de **saltos de frecuencia**, podemos lograr un sistema robusto y seguro.

SE UTILIZA UN CANAL DE COMUNICACIÓN DE MÁXIMO 1 MBPS DE CAPACIDAD BRUTA

El sistema de saltos de frecuencia logra evitar posibles interferencias y mejorar el nivel de seguridad. El sistema divide la banda de frecuencia de operación de Bluetooth en varios canales de salto, donde los **transeptores** (transmisores y receptores) durante la conexión van cambiando entre los canales de salto siguiendo una secuencia

casi aleatoria. Con esto conseguimos que el ancho de banda en un determinado momento sea diminuto pero una gran inmunidad a las interferencias.

Para lograr el bajo consumo y el bajo costo de esta tecnología se buscó una solución que se pueda implementar en un solo chip utilizando circuitos **CMOS** (familia lógica usada para fabricar circuitos integrados). Así, se consiguió un chip de 9 x 9 mm y que consuma un 97% menos energía que un teléfono celular común.

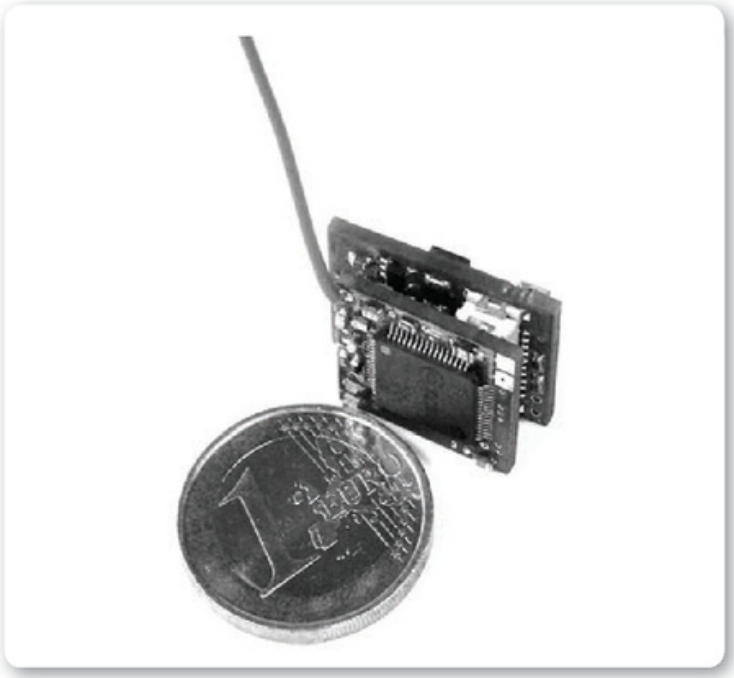


Figura 8. El tamaño de los integrados con tecnología CMOS utilizados en Bluetooth es menor que una moneda.

EL REY BLUETOOTH

El nombre de esta tecnología está inspirado en el rey danés y noruego, **Harald Blantand** (Harold Bluetooth, en inglés), conocido por ser un buen comunicador y por unificar las tribus noruegas, suecas y danesas en el siglo X. La traducción textual del nombre al español es diente azul, pero el término era utilizado para denotar su tez oscura y no sus dientes azules.

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. Este dispositivo será el encargado de regular el tráfico.

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.

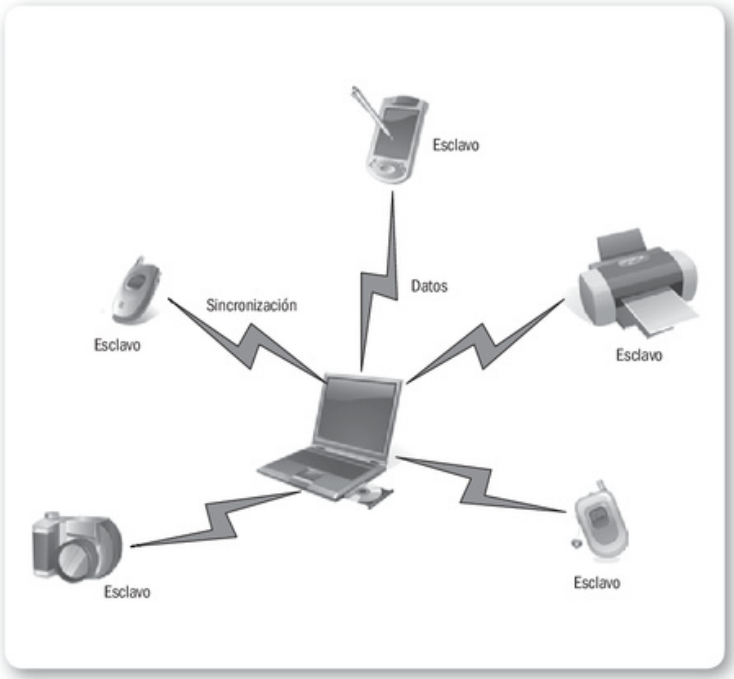


Figura 9. Esquema de conexión de varios dispositivos Bluetooth que forman una piconet.

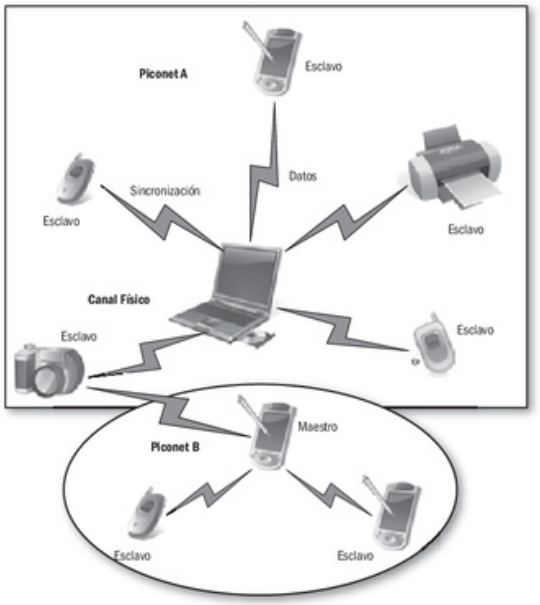


Figura 10. Al tener diferentes piconets en el mismo rango se forman las scatternets. Notemos que cada piconet tiene su dispositivo maestro.

Seguridad

Los dispositivos Bluetooth se conectan fácilmente entre ellos, esta fue una de las principales premisas a tener en cuenta cuando se desarrolló el estándar. Por consiguiente, existen muchos fabricantes que implementan la tecnología Bluetooth consiguiendo fácil conectividad, mientras la información del usuario es expuesta para cualquiera que esté cerca. En el estándar Bluetooth se especifican tres **niveles de seguridad**, que veremos a continuación.

UNIFICADOR DEL SIGLO XXI

La tecnología Bluetooth comprende el desarrollo de tecnología de hardware y de software; así como también, requerimientos de compatibilidad. Para concretar esto los principales fabricantes de los sectores de telecomunicaciones e informática participaron juntos. Empresas como **Ericsson**, **Nokia**, **IBM** e **Intel** unificaron fuerzas para mejorar la tecnología.

TABLA 2

▼ MODO DE SEGURIDAD	▼ DESCRIPCIÓN
1	Sin seguridad. El dispositivo opera en modo escucha permitiendo que cualquier otro dispositivo con Bluetooth se conecte a él.
2	Seguridad a nivel servicio. Las medidas de seguridad se establecen luego de que el canal de radiofrecuencia se establece. Soporta autenticación, encriptación de datos y autorización.
3	Seguridad a nivel de canal. Las medidas de seguridad se inician antes de que el canal de radiofrecuencia se establezca. Soporta autenticación y encriptación de datos.

Tabla 2. En esta tabla podemos ver los niveles de seguridad implementados en Bluetooth para proteger nuestros datos.

Los dispositivos configurados con el modo 1 no tienen mecanismos efectivos de seguridad. No se recomienda utilizar este modo cuando necesitamos compartir información importante. El modo de seguridad 2 es el más **flexible** de las tres opciones. Una vez que los dos dispositivos establecen un canal físico (canal de radio) de comunicación, se pueden aplicar políticas de seguridad a las aplicaciones o servicios para así dictar el nivel de seguridad requerido. No es necesario que todas las aplicaciones o servicios que utilicemos tengan el mismo nivel de seguridad. Por ejemplo, una clínica privada de salud puede desarrollar una aplicación que comparte información de los pacientes entre dispositivos con

BLUEJACKING

El término **Bluejacking** hace referencia, en seguridad informática, a una técnica de **hacking** para dispositivos que utilizan Bluetooth. Consiste en enviar mensajes no solicitados entre dispositivos (celulares, agendas, entre otros) con el objetivo de hacer algún daño, instalando, por ejemplo, un virus para celulares o algún tipo de programa malicioso.

Bluetooth usados por los médicos. En este caso, la autenticación, encriptación y autorización son medidas de seguridad que deben ser implementadas por el tipo de información sensible que se comparte. La autenticación permite que el dispositivo rechace una conexión, mientras que la encriptación de los datos protege la información que viaja en el canal establecido para que no sea fácilmente legible.

Si hablamos de autorización pensamos en habilitar, por ejemplo, un proveedor de servicio para permitirle se conecte a nuestro dispositivo y acceder a ciertas aplicaciones (pero no a todas, se aplican reglas de acceso según el usuario desee).

El modo de seguridad 3 es el más seguro de todos pero no posee la flexibilidad del modo 2. Cuando se establece un canal de comunicación con el modo 3, la autenticación y encriptación surgen antes de que el canal de comunicación se establezca. Toda información intercambiada entre los dispositivos es encriptada. La particularidad de este modo es que no se requiere implementar autorización, ya que se asume que estos dos dispositivos conectados con el modo de seguridad 3 están autorizados para acceder a toda la información y servicios disponibles en cada aparato.

Los modos de seguridad 2 y 3 descriptos son comúnmente llamados **pairing** (emparejamiento) de dispositivos Bluetooth.

Vulnerabilidades

Aunque los dispositivos Bluetooth cuenten con medidas de seguridad, muchos **SmartPhones** (teléfonos celulares de última generación), celulares de gama media y otros dispositivos tienen configurado por defecto el modo 1 de seguridad. Esta configuración viene así desde fábrica. Además, es común encontrar dispositivos configurados en el modo



ZIGBEE VS BLUETOOTH

Aunque son muy similares tienen varias diferencias marcadas. Por ejemplo, Bluetooth posee un mayor consumo de batería frente a la tecnología ZigBee. Esto se debe a que el sistema ZigBee permanece en estado **dormido** la mayor parte del tiempo, mientras que Bluetooth siempre está transmitiendo o recibiendo información una vez activado.

discovery/visible-to-all (es el modo que busca dispositivos con Bluetooth y muestra nuestro aparato para aceptar conexiones). Estas configuraciones permiten a los usuarios experimentar rápidamente los beneficios de usar las piconets sin tener las molestias de preocuparse por la configuración de seguridad.

Hace algunos años se llevó a cabo un experimento donde se intentaba identificar las vulnerabilidades de la tecnología Bluetooth en un espacio público. Según la experiencia, se detectaron más de 1000 aparatos con Bluetooth en el modo discovery/visible-to-all, o sea estos 1000 dispositivos estaban listos y esperando por otro dispositivo para establecer una conexión. Sin ningún tipo de seguridad que prevenga accesos no deseados, estaban expuestos a **fugas de datos** o contagio de algún **virus troyano**. Entre los aparatos detectados se incluían:

* Teléfonos celulares
* SmartPhones
* Notebooks
* Agendas personales
* Computadoras de escritorio

Si no se implementa un nivel de seguridad de modo 2 o se deshabilita el modo discovery/visible-to-all, se podría estar exponiendo información de la siguiente forma:

- Datos privados disponibles para ser examinados.
- Un atacante puede hacer uso de su teléfono para realizar llamadas.
- La agenda de contactos puede ser bajada.
- Un virus o un programa malicioso pueden ser instalados para ejecutar un ataque que infecte otros dispositivos, incluyendo un posible ataque a la red utilizada.

* Un atacante puede instalar un programa malicioso con la intención de tener el control de su dispositivo mientras lo usa.



MANEJARLO CON CUIDADO

La tecnología Bluetooth es una gran herramienta para implementar en una empresa y mejorar tareas. Sin embargo, debe ser manejada por personas capacitadas y su implementación debe ser seguida de cerca. Si no se cumplen las medidas de seguridad los datos de nuestro negocio pueden estar expuestos para cualquier individuo tenga o no autorización.

No debemos tener miedo ante estos posibles ataque, simplemente debemos implementar siempre un nivel de seguridad para prevenir. A continuación vemos algunas recomendaciones extras de seguridad:

- Configurar el dispositivo para que el otro extremo tenga que aceptar toda solicitud de conexión.
- Apagar el servicio Bluetooth cuando no se utiliza.
- No utilizar el modo de seguridad 1. Asegurarse de tener el modo **discovery** (para buscar otros dispositivos) habilitado solo cuando se desea conectar a dispositivos conocidos.
- Minimizar el área de conexión de los dispositivos a la mínima distancia posible siempre que podamos.
- Cuando sea posible, instalar antivirus y protección contra aplicaciones maliciosas (en el caso de una notebook o computadora de escritorio) y mantenerla actualizada.



RESUMEN

Analizando las comunicaciones de corta distancia, describimos las redes inalámbricas de área personal o WPAN, que permiten al usuario interactuar con periféricos y diferentes dispositivos en un área de cobertura determinada. Luego de detallar las WPAN, nos centramos en la tecnología Bluetooth, ya que es muy común hoy en día en cualquier celular. Conocimos su funcionamiento y algunos detalles para luego ver de qué forma nuestra información viaja segura y cuáles son los puntos vulnerables de Bluetooth.

Actividades

TEST DE AUTOEVALUACIÓN

1	¿Qué es una WPAN?
2	¿Cuál es la principal característica de estas redes inalámbricas de área personal?
3	¿Qué define el estándar IEEE 802.15.2?
4	¿Con qué nombre se conoce a la tecnología IEEE 802.15.1?
5	¿Cuáles son las 4 tecnologías WPAN descriptas en el texto?
6	¿Según qué parámetro se pueden clasificar en Clase 1, 2 y 3 los dispositivos inalámbricos Bluetooth?
7	¿Bluetooth permite la comunicación Full Duplex? ¿Para qué implementa la tecnología de saltos de frecuencia?
8	¿Qué se define como picored?
9	¿Cuál es la tarea del dispositivo maestro en una picored?
10	Identifique los tres modos de seguridad de Bluetooth.

*08 –

Antenas y conectores

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, tanto generales como específicas. Además, analizaremos las diferentes clasificaciones: según su construcción y patrón de radiación. Aprenderemos sobre sus cables y conectores utilizados. Para finalizar, veremos la relación entre radiación y salud.

- **¿Qué es una antena? 264**
  - ¿Cómo funciona una antena? 267
  - Características generales de una antena 271
  - Características específicas de una antena 272
- **Clasificación de las antenas 278**
  - Según el patrón de radiación 279
  - Según su construcción 281
- **Cables y conectores usados ... 286**
  - Cables coaxiales 287
  - Conectores 289
  - El pigtail 296
- **Radiación y salud 297**
  - ¿Es peligrosa la radiación electromagnética? 302
- **Resumen 303**
- **Actividades 304**

¿Qué es una antena?

Estudiemos un poco de historia y veamos cómo nacieron los sistemas para transferir información. El primer sistema de comunicación eléctrico fue la **telegrafía**, introducida en 1844. Luego, haría su aparición la telefonía allá por el año 1878. En ambos sistemas, las señales del emisor se enviaban a través de líneas de transmisión de dos hilos conductores (cables), que conectaban directamente con el receptor.

La teoría de las antenas nace a partir de los desarrollos matemáticos de James C. Maxwell en el año 1854. Los experimentos de Heinrich R. Hertz en 1887 corroboraron la teoría de Maxwell y, luego, los primeros sistemas de radiocomunicaciones de Guglielmo Marconi en 1897 harían lo propio.

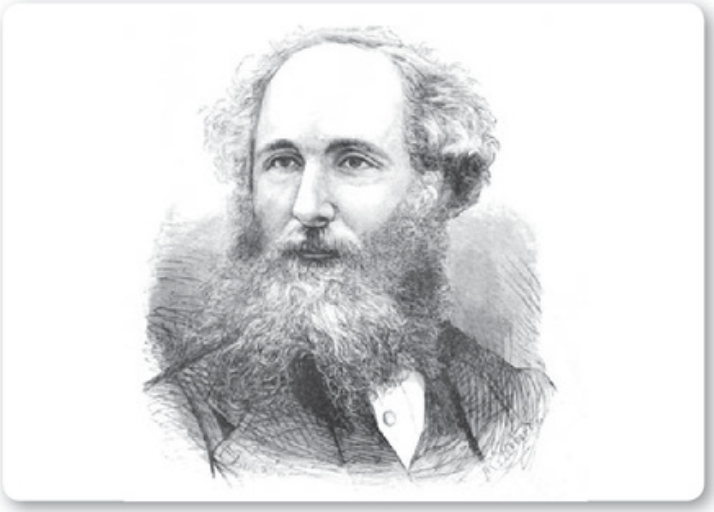


Figura 1. James Clerk Maxwell fue un físico escocés conocido por haber desarrollado la teoría electromagnética clásica.

Partiendo de Marconi y llegando hasta los años 40, vemos que toda la tecnología de las antenas se centraba en elementos radiantes de hilo, a frecuencias hasta UHF (recordemos la representación del espectro radioeléctrico vista en capítulos anteriores). Estas **antenas de hilo** tenían conductores de hilo que irradiaban las ondas y transmitían en el rango de frecuencias de 50 y 100 KHz. Luego, algunas personas empezarían a investigar una forma más eficiente de realizar antenas para operar en frecuencias entre 100 KHz y varios MHz del espectro radioeléctrico.

El tiempo pasó y con la llegada de la Segunda Guerra Mundial, aparecieron nuevos elementos utilizados para radiar energía

de antena (tales como guías de onda, bocinas, reflectores, entre otros). En este contexto, se descubrió y desarrolló el generador de microondas a frecuencias mayores a 1 GHz.

Así, en la época actual, con los avances tecnológicos que existen, el desarrollo de la teoría de antenas se vio afectado positivamente dando como resultado una variedad de dispositivos con diminutas antenas que nos permiten tener conectividad. Vemos de esta forma, que las antenas cumplen un papel fundamental y crítico cuando se diseña un sistema, sea cual sea su tecnología.

Además de detallar las características de las antenas, trataremos otros componentes pasivos que hemos nombrado anteriormente como los **cables** y **conectores** necesarios para diseñar e implementar cualquier red de datos que utilice la tecnología inalámbrica, como en nuestro caso.

Es un término bastante común hoy en día y lo podemos escuchar a diario, pero ¿realmente sabemos qué es una antena?

Una antena es un elemento usado para transmitir y recibir información. Este dispositivo físico es capaz de convertir una onda guiada por la línea de transmisión (un cable) en ondas electromagnéticas, que se pueden transmitir por el espacio libre. Para ser prácticos con la definición, una antena es un pedazo de material conductor al cual se le aplica una señal (por ejemplo, proveniente de un punto de acceso inalámbrico de nuestra red), que es radiada al espacio libre o al aire con el objetivo de propagarse y llegar a destino.

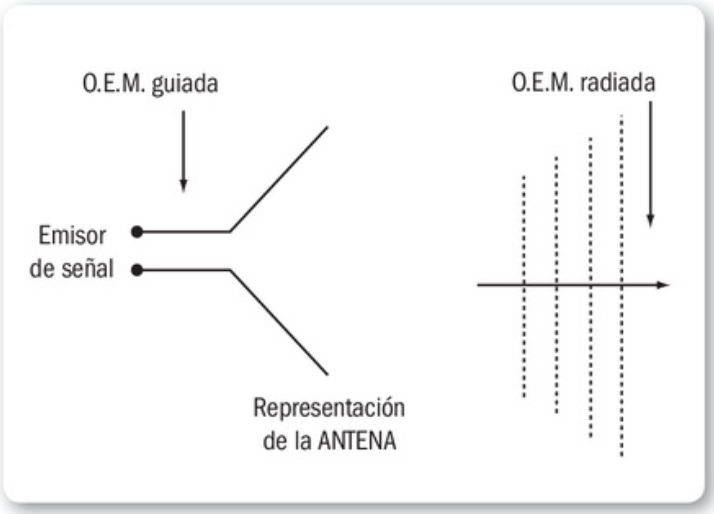


Figura 2. Representación del principio de la antena, donde una onda electromagnética (O.E.M) es radiada al espacio libre.

Así, estamos transformando la energía proveniente, por ejemplo, del punto de acceso en un campo electromagnético o viceversa. Esto es necesario para comunicar una estación origen con un destino sin recurrir a cables que interconecten ambos equipos.

Cuanto más eficaz sea la transformación de energía, mayor alcance tendremos, independientemente del equipo que tengamos.

> LA ANTENA , POR SÍ SOLA, CONSTITUYE MÁS DEL 50% DE LA CALIDAD DEL DISPOSITIVO INALÁMBRICO

En la actualidad, la antena por sí sola constituye más del 50% de la calidad del dispositivo inalámbrico. De esta forma, tendremos dos posibilidades: que la antena sea buena o que sea excelente.

Existen en el mercado diferentes tipos de antenas. Algunas son sencillas y fáciles de instalar y manipular y otras que son todo lo contrario. El hecho de que una antena sea sencilla no quiere decir que no tenga un rendimiento alto. Cualquiera sea la antena, por más sencilla o compleja que sea, si realiza su función de transformar energía de manera óptima (o sea, sin producir pérdidas de energía), será una antena con buenas prestaciones.

Existen muchas maneras de concretar la transferencia de energía desde el emisor al espacio libre y por esto las antenas pueden ser físicamente muy diversas. Por ejemplo, existen antenas que están integradas por lentes que enfocan el haz de radiación en una región particular del espacio, antenas formadas por ranuras, etc., de todas maneras las más populares están compuestas por elementos metálicos con una geometría especial en función de la frecuencia de operación del sistema implementado.



UNA MENTE BRILLANTE

James Maxwell es considerado como el científico del siglo XIX que más influencia tuvo sobre la física del siglo XX. Realizó contribuciones fundamentales a la ciencia y se lo compara con el trabajo realizado por Isaac Newton y Albert Einstein. En 1931, Einstein describió el trabajo de Maxwell como **el más profundo y provechoso que la física ha experimentado desde Newton**. Y si lo dice una persona como Einstein, algo de razón tendrá.



Figura 3. Diferentes antenas instaladas en un mismo mástil ubicado en el techo de una vivienda.

Un objetivo que muy a menudo puede desearse al hacer (o instalar) una antena es concentrar el **campo electromagnético radiado** en una dirección determinada. Hay antenas que realizan la difusión de la energía en todas las direcciones, mientras que otras antenas lo hacen en una sola dirección. Veremos esto y otras características de las antenas más adelante en este capítulo.

¿Cómo funciona una antena?

Expliquemos de forma general cómo funciona una antena. No entraremos en definiciones que estén relacionadas a la física o la electrónica porque escapa a los objetivos del libro. Simplemente queremos entender, a grandes rasgos, el funcionamiento básico de las antenas que diariamente utilizamos.

Las antenas basan su funcionamiento en el principio de la **radiación electromagnética** producida al circular una corriente eléctrica por un conductor. Esta corriente genera un **campo magnético** alrededor del

elemento, el cual forma un **campo eléctrico oscilante** y así se continúa generando. De esta manera tendremos conformada una onda que será irradiada al **espacio libre**. Debemos hacer notar que este campo magnético es variable y sigue las mismas ondulaciones de la corriente eléctrica que se aplica a la antena.

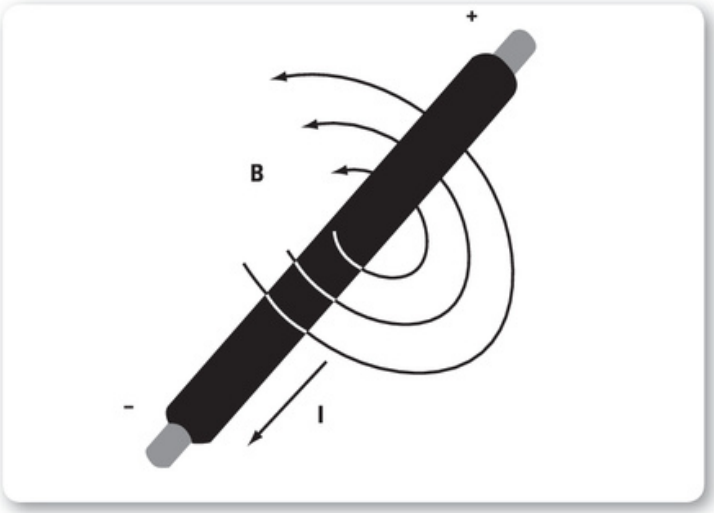


Figura 4. Cuando por un conductor circula una corriente eléctrica se genera un campo magnético (siguiendo la llamada Ley de Ampère)

Para entender el principio de una onda radiada en el espacio, podemos decir que es similar al fenómeno de las ondas circulares que se crean cuando cae una gota de agua sobre un estanque, fenómeno que vemos, por ejemplo, cuando llueve.

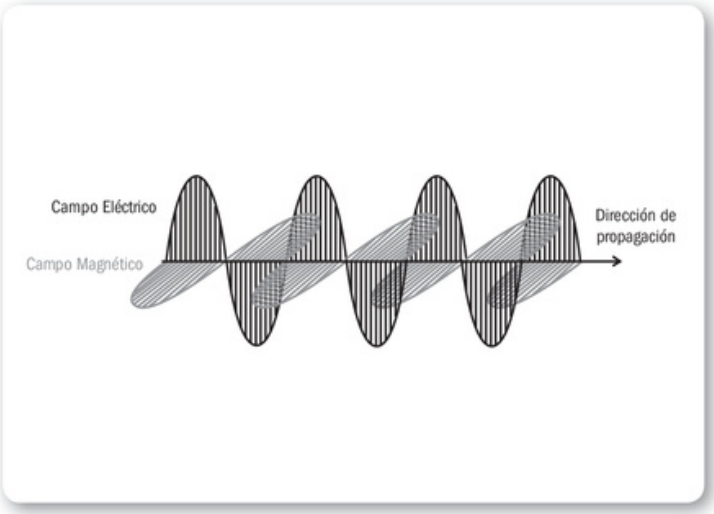


Figura 5. La onda generada por el campo magnético y eléctrico oscilante.



Figura 6. Vemos cómo se propagan las ondas en el agua, fenómeno que se compara con la propagación en el espacio libre.

Aprovecharemos la ocasión para explicar qué son las **cámaras anecoicas de radiofrecuencia**. Una cámara anecoica es una sala diseñada para absorber el sonido que incide sobre las paredes, el suelo o el techo de esta. De esta forma, se anulan los efectos de **eco y reverberación** del sonido y se simulan condiciones óptimas para realizar pruebas evitando ruidos e interferencias. Cuando hablamos de antenas y radiofrecuencias, debemos explicar la cámara anecoica de radiofrecuencia que difiere de la cámara anecoica acústica. Las cámaras de radiofrecuencias son recintos con un blindaje metálico, básicamente, constan de dos partes fundamentales: el blindaje metálico (o **jaula de Faraday**) y los materiales absorbentes electromagnéticos.

> LA CÁMARA ANECOICA DE RADIOFRECUENCIA DIFIERE DE LA CÁMARA ANECOICA ACÚSTICA

ESTACIONES EMISORAS DE INTERFERENCIAS

A comienzos del siglo XX aparecían las primeras emisiones destinadas a **interferir** señales de telégrafo y de radio. El objetivo de estas estaciones era interferir las comunicaciones del enemigo por medio de una señal generada localmente que actuaba como ruido. La Unión Soviética logró el bloqueo masivo de las emisiones de radio en 1948.

Una jaula de Faraday es una estructura completamente metálica con la que logramos una atenuación de las interferencias externas. El objetivo es dual, primero busca que las interferencias externas sean atenuadas y así evitar que el interior sea influido, y además busca atenuar los campos generados en el interior que podrían afectar al entorno exterior. De esta forma se simulan las condiciones del espacio libre para un sistema.

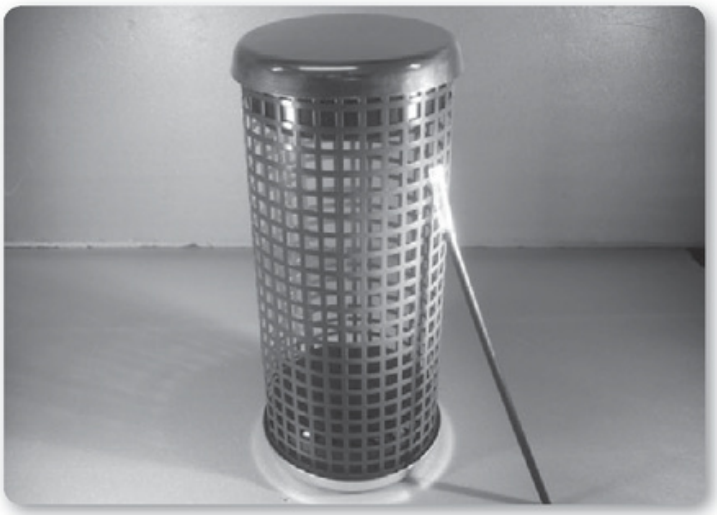


Figura 7. Ejemplo de una jaula de Faraday utilizada para inhabilitar la señal de un dispositivo celular dentro de ella.

La jaula de Faraday se recubre en su interior con material absorbente electromagnético para darle propiedades de absorción y que finalmente se convierta en una cámara anecoica. Es importante recalcar que el objetivo de los materiales absorbentes es evitar posibles reflexiones en paredes o el piso de la cámara por parte de los campos electromagnéticos. Esencialmente, no existe otro objetivo para esos materiales.

COMUNICACIONES SOVIÉTICAS

Con la necesidad de comunicar tierras lejanas y baldías con zonas habitadas, hace varias décadas, el gobierno soviético creó una **red de antenas**, que enviaban ondas a la ionósfera y luego transmitían por medio de una cadena de repetidores. Esto fue consecuencia de la imposibilidad de utilizar cables (dado que las distancias eran de miles de kilómetros).

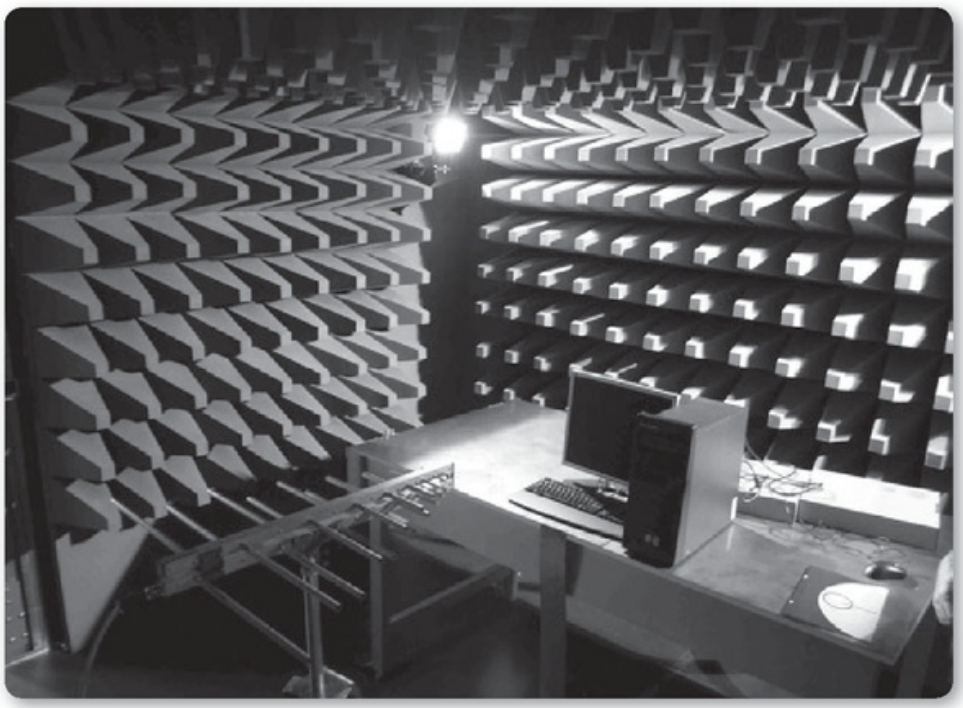


Figura 8. Medición de una antena directiva en una cámara anecoica.

Características generales de una antena

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 o componentes).

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

Características específicas de una antena

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 y no suele tenerse en cuenta.



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) del espectro radioeléctrico.

Ganancia de antena

Antes de hablar específicamente de la ganancia de una antena, necesitamos comentar un concepto básico que se utiliza para entender este parámetro importantísimo.

Definiremos a una **antena isotrópica** como aquella antena 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, ya 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.

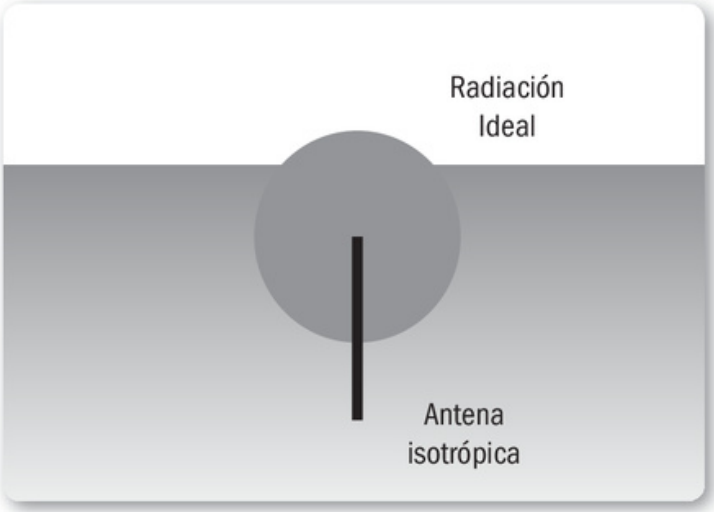


Figura 9. El modelo propuesto de antena isotrópica sirve para comparar la ganancia de nuestras antenas con el modelo teórico ideal..

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

JAULA SALVADORA

La **jaula de Faraday** se puede encontrar en muchos dispositivos que utilizamos a diario como microondas y escáneres. También en dispositivos que sin estar provistos de una jaula de Faraday, actúan como tal. Algunos ejemplos son los ascensores, aviones, autos. Por este motivo, ante una tormenta eléctrica se recomienda permanecer en el interior del auto ya que la carrocería actúa como una jaula de Faraday.

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 hablamos anteriormente, al momento de diseñar una antena vamos a necesitar 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.

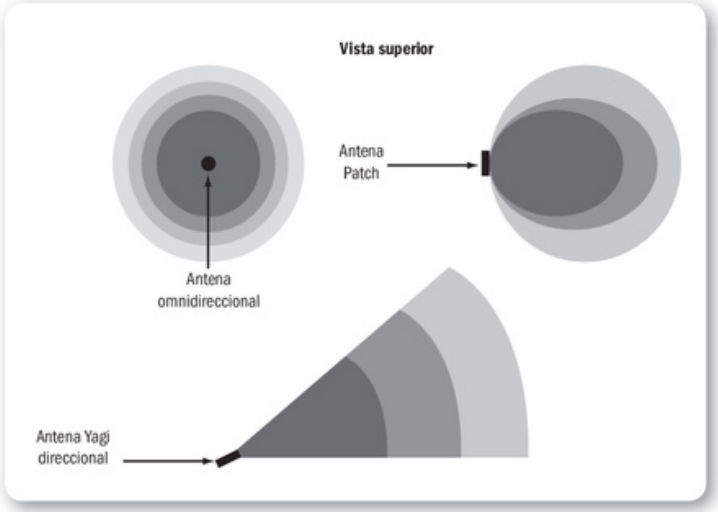


Figura 10. La vista superior de estas tres antenas muestra el diagrama de radiación (o lóbulo de radiación) de cada una.

Hay que tener presente que nuestras antenas no amplifican las señales (son elementos pasivos) y que solamente concentran la señal en un haz para cierta dirección específica.

ANTENAS DUGA

En la Unión Soviética se realizaron sistemas de detección de misiles llamados **Duga 1**, **2** y **3**. El más conocido fue el **Duga 3** construido en los años 70 en la zona de Chernobyl. Se usaba para la detección de misiles a largas distancias y poseía el sistema **OTH** (over the horizon radar system). Era una construcción metálica de 800 m de largo por 100 m de alto.

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 nos muestra la forma y la ubicación de los lóbulos de radiación lateral y posterior, así como otros puntos donde la potencia irradiada es menor.

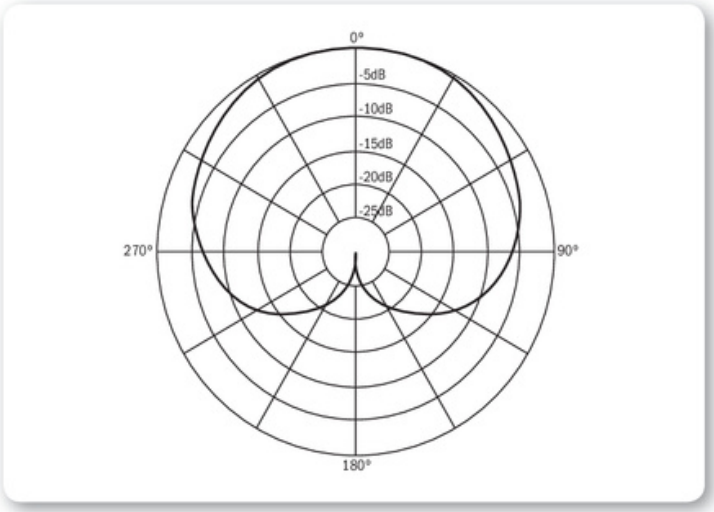


Figura 11. Diagrama de radiación direccional. Para este caso, el diagrama suele llamarse cardioide, ya que su forma es similar a un corazón.

Lo que se trata de hacer al diseñar una antena es reducir al mínimo los lóbulos extras (laterales y posteriores), ya que 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**.

La ventaja de los diagramas tridimensionales, como el que vemos en la figura, es que nos permite ver con mayor detalles la forma en que nuestra antena va a radiar su energía cuando esté funcionando en nuestro sistema.

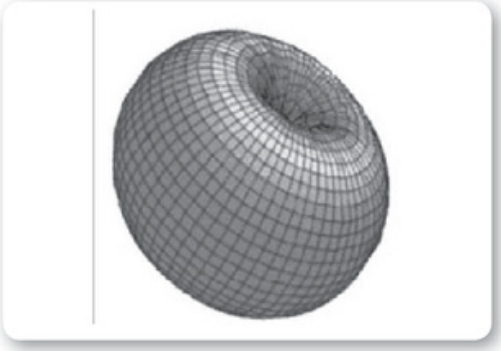


Figura 12. Dado que los diagramas de radiación son volúmenes, podemos representarlos en tres dimensiones.

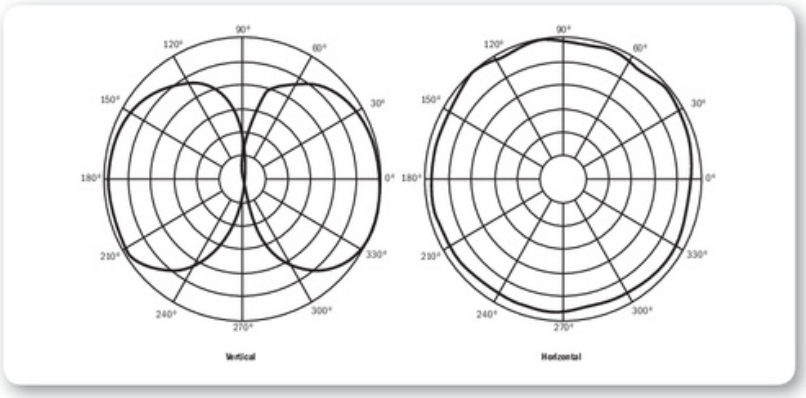


Figura 13. Es habitual que los diagramas de radiación se realicen en dos planos: radiación vertical y radiación horizontal.

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).

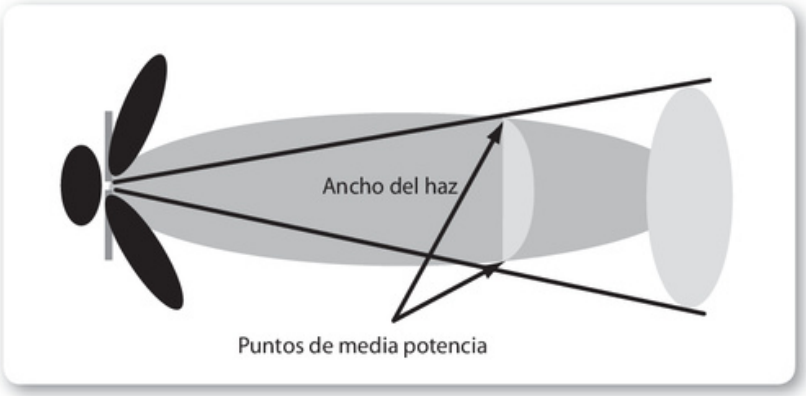


Figura 14. El parámetro ancho del haz está ligado directamente al diagrama de radiación y sus diferentes formas de graficarlo.

Frecuencia de operación de la antena

Este parámetro nos define el rango de frecuencias soportadas por nuesta antena. Así, si usamos una frecuencia en nuestro transmisor dentro del rango de nuestra antena, la radiación de ondas electromagnéticas se realiza de forma adecuada.

Las antenas no pueden irradiar en cualquier frecuencia. Las antenas son diferentes según la frecuencia de trabajo. Por este motivo, es importante tener en mente el mencionado parámetro a la hora de diseñar o comprar una antena.

Polarización de la antena

La polarización de una antena se refiere solo a la **orientación del campo eléctrico radiado** desde esa antena. En general la polarización puede ser horizontal o vertical, si suponemos que los elementos de la antena se encuentran dentro de un plano horizontal o vertical con el cual trabajamos.

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

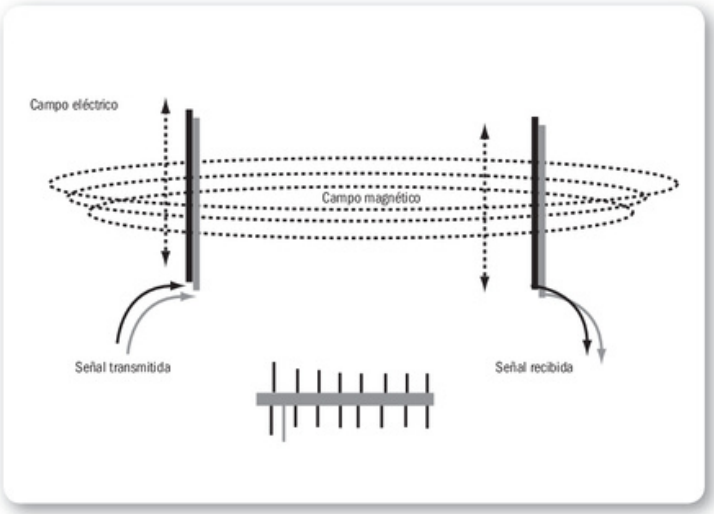


Figura 15. La polarización es vertical si nuestra onda mantiene el campo eléctrico en dirección vertical durante todo el recorrido.

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. Este diagrama es más común dado que es fácil de medir e interpretar sin utilizar elementos complementarios.

En cambio, si la onda propagada está polarizada horizontalmente, nuestra antena tendrá polarización horizontal. Hay mucha bibliografía para consultar sobre este tema, inclusive en Internet, existe mucha información.

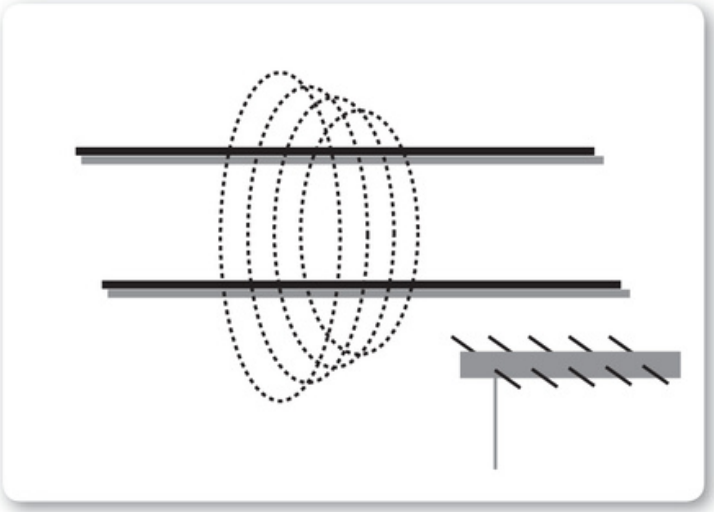


Figura 16. Al modificar la orientación de los elementos de antenas obtenemos la polarización horizontal.

Lo importante es saber que podemos emplear cualquier tipo de polarización siempre y cuando tengamos la misma configuración en ambos extremos. Existen además otras polarizaciones que no veremos en este libro dado que escapan a sus objetivos.

Clasificación de las antenas

Tal como dijimos antes, existen variedades de antenas. La forma, el tamaño y el uso dependen de los parámetros vistos en la sección anterior. Así, para poder conocer algunos tipos de antenas que son habituales, podemos realizar una clasificación de las antenas si nos basamos en algunas especificaciones. Por ejemplo, tendremos algunas clasificaciones según los siguientes parámetros: si es o no directiva, el tamaño, la frecuencia de uso, el patrón de radiación, cómo está construida físicamente, para qué aplicación se puede usar la antena, entre otros. 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 de la antena), 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 esta forma 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.

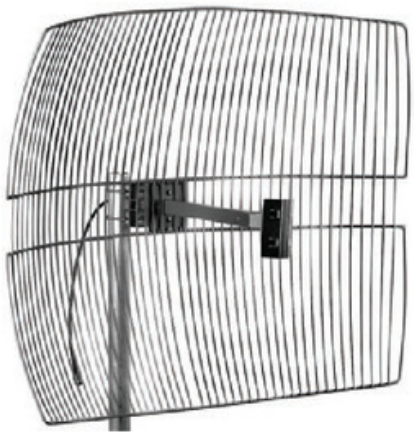


Figura 17. Esta antena direccional posee forma de parrilla para evitar embolsar vientos fuertes.

• **Sectoriales**: si el diagrama de radiación corresponde a un área o zona especifica, la antena se llama sectorial. Como detalle podemos decir que estas antenas poseen mayor ángulo de irradiación que las antenas direccionales, de esta forma tienen corto alcance ya que no se proyectan hacia adelante. 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 el plano horizontal, 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, sin embargo, puede variar.



Figura 18. Varían su rango de ganancia entre 10 y 19 dBi. Además, el ancho de haz horizontal suele estar en los 90° y el vertical en los 20°.

Este tipo de antenas puede construirse de forma casera.

Existen muchos ejemplos que podemos buscar en Internet donde se plantean diferentes modelos de antenas con la utilización de materiales que se encuentran en comercios de electronica.

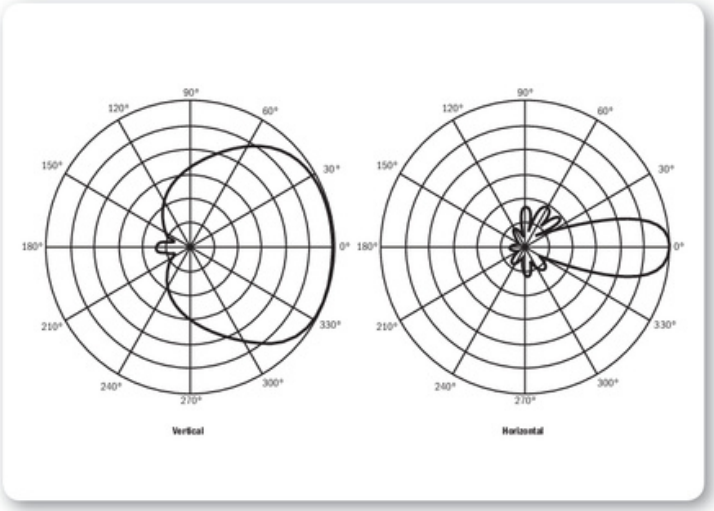


Figura 19. Diagrama de radiación horizontal posee la mayor energía irradiada en la parte frontal de la antena.

• **Omnidireccionales**: tal como describimos antes, estas antenas son las que irradian energía en todas las direcciones. Por esto se dice que su ángulo de radiación es de 360° en el plano horizontal, o sea con forma de círculo. 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 en el lado del cliente se obtienen buenos resultados.



Figura 20. La **antena omnidireccional** para exteriores posee un soporte que permite instalarla según cuál sea su polarización.

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.

ANTENA TIPO CUERNO

La antena tipo **cuerno** (*horn*) nació como una antena construida para apoyar el proyecto Echo de la NASA en 1959. Esta antena está en Nueva Jersey, EE.UU. Consta de una estructura diseñada con un metal pulido que emula la forma de un cuerno para así dirigir las ondas de radio. Se utiliza como antena para frecuencias UHF y microondas por encima de los 300 MHz.



Figura 21. Al ser una antena fácil de construir, es muy común utilizar el dipolo para redes inalámbricas, tanto en exteriores como en interiores.

* **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 provee 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. Esta antena 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

INVENCIÓN DE LA YAGI

El diseño de la famosa antena **Yagi-Uda** fue creado en los años 30 en Japón por el Dr. Hidetsugu Yagi y su ayudante el Dr. Shintaro Uda. Su innovación fue en el nuevo diseño de antena que combinaba una estructura relativamente simple con un elevado rendimiento. Esta antena fue patentada en 1926 y desde entonces se puede encontrar en los techos de millones de hogares.

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

* **Panel**: también son llamadas patch y consisten en 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.

EL REGRESO DE LA YAGI

Las antenas yagi fueron muy famosas cuando la televisión nació, sin embargo, luego perdieron algo de protagonismo con la llegada de la televisión por cable ya que no se utilizaban. Hoy vuelven a pisar fuerte en el mercado de WiFi y encontramos gran variedad de modelos con diferentes ganancias para usar en redes inalámbricas.



Figura 23. Antena panel con soporte para exteriores. Es muy fácil de identificar este tipo de antenas en la ciudad ya que son llamativas.

* **Parrila**: también se puede encontrar esta antena con el nombre de malla o grid. La característica de este tipo de antenas es que su reflector posterior es similar a una parrilla (por esto el nombre). Se utilizan para zonas donde las inclemencias del tiempo son un factor a tener en cuenta a la hora de montar una antena. Si, por ejemplo, necesitamos colocar una antena en una zona de mucho viento, utilizando este modelo evitaremos posibles corrimientos de la antena, lo que provocaría una pérdida del enlace. Poseen alta direccionalidad de la señal y son de muy fácil construcción además de económicas.



Figura 24. El reflector tipo parrilla identifica a las antenas con ese nombre. Existen muchos modelos de antenas de este tipo.

* **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

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 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 vientos, ya que se podría desapuntar nuestro enlace.



Figura 25. La propiedad de las parabólicas de concentrar la energía en un punto es similar a la forma en que una linterna concentra la luz.

Un punto extra que debemos tener en cuenta a la hora de montar las antenas en una torre es el aislamiento. Esto se aplica en caso de tener varias antenas en una misma torre. Solo a modo informativo diremos que el aislamiento entre antenas permite evitar que las señales electromagnéticas se interfieran. Se realiza aislamiento horizontal y vertical, según corresponda.

Cables y conectores usados

Como todos sabemos, para conectar nuestros equipos inalámbricos con las antenas usamos cables y conectores. En esta sección describiremos los cables y conectores utilizados habitualmente para este tipo de conexiones, ya que son conectores especiales para este tipo de redesque estamos estudiando.

> PARA CONECTAR NUESTROS EQUIPOS INALÁMBRICOS CON LAS ANTENAS USAMOS CABLES Y CONECTORES

El cable que normalmente se usa para conectar nuestro equipo a la antena es el cable coaxial de **50 ohmios de impedancia**. Estos cables son de baja pérdida y se utilizan para conducir señales de radiofrecuencia (por ejemplo, generadas en nuestro equipo) hasta la antena. Se dará la máxima transferencia de la energía cuando todos los elementos involucrados tengan la misma impedancia (en la gran mayoría de los casos es de 50 ohmios). Tengamos en mente que, si utilizamos un cable con otra impedancia, parte de la señal de radio se reflejará nuevamente hacia el origen, lo que introducirá pérdidas de energía considerables en nuestro enlace.

LOS MÁS USADOS

El cable más utilizado en redes inalámbricas es el tipo **LMR**, que es fabricado por la empresa Times Microwave Systems (**www.timesmicrowave.com**). Como alternativa se usa el cable **Heliax**, fabricado por la empresa Commscope (**www.commscope.com**). Son cables que introducen poca perdida pero cuestan más. La empresa Belden (**www.belden.com**) también tiene productos interesantes.

Cables coaxiales

Los cables coaxiales poseen un conector central (llamado **activo**) que está rodeado de una malla metálica. La función de esta malla es proteger al conductor activo de las **interferencias externas** que pueden existir. Un ejemplo de cable coaxial es el utilizado para la televisión.



Figura 26. Los cables coaxiales también introducen una pérdida de la señal entre la antena y nuestro transmisor/receptor.

Para conectar el cable a la antena y a los elementos de nuestra red (tales como puntos de acceso o placas de red inalámbricas), usamos **conectores**. No todos los dispositivos inalámbricos disponen de un conector donde enchufar, por ejemplo, la antena. Algunos nuevos puntos de acceso no tienen antenas externas (como vimos en los primeros capítulos) y por esto no se les puede conectar un cable. Sin embargo, podemos encontrar muchos fabricantes que sí tienen antenas desmontables o lugar para conectar el cable coaxial.

Hay variedad de conectores en el mercado, básicamente tenemos conectores tipo **macho** y tipo **hembra**. Los conectores también introducen una pérdida de señal. Para evitar esto no solo debemos utilizar conectores y cables de **calidad** sino que también debemos usar el **número de conectores imprescindibles** y un **cable lo más corto posible**, siempre que se pueda.

El número de conectores depende de la cantidad de dispositivos de nuestra red inalámbrica que tengamos que conectar, la calidad variará según lo que queramos gastar y el largo del cable estará determinado por el tipo de cable a usar. Por ejemplo, tenemos una antena tipo

parabólica, direccional, para nuestro enlace de larga distancia, donde compartimos Internet con el otro extremo, pero nuestro punto de acceso transmisor está un poco lejos. Por esto usamos un cable coaxial largo para conectar la antena. Como no contamos con mucho presupuesto, el cable comprado no es de muy buena calidad y los conectores utilizados son los más económicos. Con este escenario, posiblemente tengamos muchas pérdidas y la ganancia obtenida con la antena parabólica se estaría desaprovechando.

Es recomendable evitar usar cables largos y conectores extras para extender el largo de los cables (es preferible invertir en un nuevo cable del largo adecuado). No se recomienda hacer empalmes entre cables.

Al momento de comprar un cable, debemos pensar que lo utilizaremos para la frecuencia de **2.4 GHz**. Hay cables que se usan para televisión y otros que son adecuados para el mundo inalámbrico, por esto debemos considerar que seleccionar el cable correcto es tan importante como elegir una buena antena.

Veamos una tabla con los tipos de cables y sus pérdidas según la longitud del cable. Esto es para la norma IEEE 802.11b/g a 2.4 GHz.

TABLA 1

▼ TIPO DE CABLE	▼ PÉRDIDA 802.11B/G (2.4 GHZ) DB/1M
LMR-100	1.3 dB por metro
LMR-195	0.62 dB por metro
LMR-200	0.542 dB por metro
LMR-240	0.415 dB por metro
LMR-300	0.34 dB por metro
LMR-400	0.217 dB por metro
LMR-500	0.18 dB por metro
LMR-600	0.142 dB por metro
LMR-900	0.096 dB por metro
LMR-1200	0.073 dB por metro

▼ TIPO DE CABLE	▼ PÉRDIDA 802.11B/G (2.4 GHZ) DB/1M
LMR-1700	0.055 dB por metro
RG-58	1.056 dB por metro
RG-8X	0.758 dB por metro
RG-213/214	0.499dB por metro
9913	0.253 dB por metro
3/8" LDF	0.194 dB por metro
1/2" LDF	0.128 dB por metro
7/8" LDF	0.075 dB por metro
1 1/4" LDF	0.056 dB por metro

Tabla 1. Pérdidas de los diferentes cables coaxiales en relación a la longitud. Se toma un metro de largo para la tabla.

El cable más utilizado para conexiones caseras es el famoso cable coaxial **RG58**. Es un cable barato y fácil de encontrar en los comercios. La desventaja es que tiene bastantes pérdidas (un poco más de 1 dB por metro), por este motivo debemos usar cables cortos. Por ejemplo, si tenemos una antena de 12 db y un cable RG58 de unos 2 metros de largo y sumamos la pérdida de conectores, tal vez se estén perdiendo unos 3 dB en todo el circuito. En conclusión, sería como si tuviéramos una antena de 9 dB en lugar de 12 dB.

Conectores

La función de un conector es vincular el equipo inalámbrico al cable coaxial y el cable a la antena. Para esto debemos seleccionar qué tipo de conector usaremos y tener especial cuidado, ya que existen diferentes conectores. Al no haber una **regulación** que especifique cómo deben ser los conectores, cada fabricante puede tener un conector propio y, por consiguiente, existe una gran variedad de modelos distintos en el mercado. En general podemos diferenciar

los conectores por sus atributos, como por ejemplo por sus atributos, tomemos por ejemplo la lista que a continuación detallamos:

- Tipo: es la forma que tiene el conector.
- Género: puede ser macho (*male*) o hembra (*female*).
- Polaridad: **normal** o **invertida** (**RP**).
- Rosca: normal o invertida (**RT**).

Si estamos por usar un cable grueso, lo normal es que tengamos que comprar un conector tipo **N macho**. Se puede decir que, en general, los dispositivos como puntos de acceso tienen conectores hembra. Además de los conectores N es común encontrar los tipos **SMA** y **TNC**. Si hablamos de antenas, se encuentran en casi todos los casos con un conector N hembra. Veremos algunos tipos de conectores que podemos encontrar en redes inalámbricas (aunque no todos son válidos para este tipo de redes caseras).

Conectores N

El nombre de este conector proviene de su creador Paul Neill y es el conector que se usa en la gran mayoría de las antenas de 2.4 GHz. El conector es tipo rosca y tienen un tamaño considerable. Muchas veces es fácil confundirlo con los conectores utilizados para trabajar en **UHF**, sin embargo, la diferencias es que estos últimos no sirven para la banda de 2.4 GHz. Es extraño encontrar placas inalámbricas o puntos de acceso con este conector (debido a su tamaño). Es realmente fácil trabajar con este conector y es muy práctico para montarlo en antenas de fabricación casera.

Encontramos dos tipos de conectores N:

* **Conector N macho**: es el más utilizado para conectarse a las antenas externas que hay en el mercado.



RADOMO

Para proteger a las antenas y evitar que sus propiedades electromagnéticas se vean afectadas por diferentes factores se utiliza un **Radomo** (que nace de juntar la palabra radar y domo). Es un recubrimiento estructural resistente a la intemperie que resguarda a la antena. El material con el cual está construido permite atenuar de forma mínima la señal emitida o recibida por la antena.



Figura 27. El **conector N macho** es el que usamos en el cable para enviar las señales desde nuestro equipo hasta la antena.

* **Conector N hembra**: todos los fabricantes usan este conector para sus antenas comerciales. Tenemos que identificar las tres diferentes formas en que se presenta este conector (todos son considerados conectores N hembra pero cambian respecto a la forma física), según el fabricante).

a) Conector N hembra **estándar** (sin agarre físico): se encuentra en el cable de la antena y se conecta al dispositivo inalámbrico de nuestra red.



Figura 28. Este conector no posee ninguna forma de sujeción física.

b) Conector N hembra **de chasis** de agarre con 4 tornillos: se fija directamente a la antena, por eso, se llama de chasis.



Figura 29. Con cuatro tornillos podremos fijar el conector a nuestra antena o chasis para evitar movimientos indeseados.

c) Conector N hembra **de chasis** de agarre solo con una tuerca: ideal para implementarlo en antenas caseras dada su facilidad de montaje.

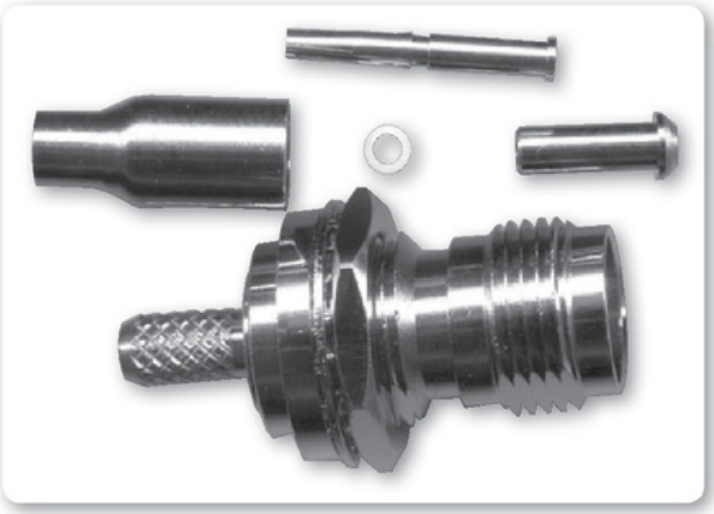


Figura 30. Con cuatro tornillos podremos fijar el conector a nuestra antena o chasis para evitar movimientos indeseados.

Conectores SMA

El conector **SMA** (*Sub-Miniature version A*) se implementa para el cable coaxial utilizado en microondas. Es un conector tipo roscado y de pequeño tamaño, que sirve para frecuencias de trabajo de hasta 33 GHz. En general, trabaja de forma adecuada con frecuencias de hasta 18 GHz, pero existen algunos fabricantes que diseñan equipos para 26.5 GHz o frecuencias similares.

Tal como dijimos, hay diversidad de conectores y el SMA también tiene su variante. El conector estándar es el SMA macho que lleva una tuerca como veremos a continuación, pero también existen los **SMA inversos** (RP-SMA o *Reverse Polarity*), que llevan la tuerca en el conector hembra. Existe mucha confusión con respecto a la descripción de los conectores SMA y RP-SMA. La terminología correcta es la que se refiere al conector central como macho o hembra. Así, por ejemplo, el conector SMA macho tendrá una rosca por dentro y el conector central macho (también conocido como **plug**). El SMA hembra tendrá rosca por afuera y conector central hembra (**socket**). La confusión aparece con los modelos RP donde se invierte la polaridad y se tiene rosca interna y conector central hembra para el RP-SMA macho y la inversa (rosca externa y conector central macho) para el RP-SMA hembra. Veamos unas imágenes para clarificar el concepto que venimos explicando.

• **Conector SMA macho**: es uno de los conectores más utilizados por los fabricantes para equipamiento de redes inalámbrica.



Figura 31. Vemos dos antenas con diferentes conectores, el de la izquierda de la imagen es un RP-SMA Macho y el de la derecha, un SMA Macho.

• **Conector RP-SMA hembra**: este conector es usado para conectarse a un punto de acceso o placa inalámbrica PCI. La gran mayoría de las placas inalámbricas PCI o puntos de acceso tienen este conector que permite conectar la antena directamente, sin necesidad de un adaptador.



Figura 32. Podemos encontrar diferentes formatos de los conectores RP-SMA, por ejemplo para fijarlo a un circuito impreso.

Trabajar con este tipo de conectores requiere de paciencia y prolijidad, ya que son muy pequeños.



Figura 33. El conector SMA hembra viene en una versión bañada en oro para mejorar la conductividad de la señal.

Conectores BNC

Este tipo de conectores era el utilizado en las redes Ethernet de los años 80. BNC significa *Bayonet Neill-Concelman* y fue diseñado para cables coaxiales como el RG58 o RG59. Es apto para trabajar en radiofrecuencia pero no muy usado en redes inalámbricas dada su incapacidad para operar en 2.4 GHz. Con la aparición del cable UTP, los problemas de mantenimiento y las limitaciones del cable coaxial,

entre otras razones, se dejaron de usar estos cables en las redes. En la actualidad, se usan mucho en sistemas de video profesionales. El conector se caracteriza por tener un anillo que rota en la parte exterior y de esta manera asegura el cable (por medio de un mecanismo de **bayoneta**). Tenemos versiones BNC macho y hembra, que se distinguen por el conector central.



Figura 34. Podemos encontrar conectores BNC en instrumentos electrónicos de medición como osciloscopios..

Conectores TNC

Por último, tenemos el conector TNC (*Threaded Neill-Concelman*), que es una versión con rosca del conector BNC. Ideal para trabajar en las frecuencias de hasta 12 GHz, se encuentra en la gran mayoría de equipos Wireless Cisco y Linksys. Al igual que el conector SMA (y usando la misma forma de identificarlos explicada anteriormente) tenemos varios tipos de conectores:

LOS USOS DEL TNC

Varios fabricantes hacen uso del conector TNC en sus dispositivos. Por ejemplo, Linksys, fabricante de equipos de red, utiliza el RP-TNC para muchos de sus equipos WiFi, incluyendo al popular router WRT54G. Además, el conector se utiliza en sistemas de video y sistemas profesionales de audio. Empresas como Camplex y Electro-Voice se dedican a estos dispositivos, donde no existe una relación directa con la tecnología WiFi.

- **TNC macho**
- **TNC hembra**
- **RP-TNC macho**
- **RP-TNC hembra**



Figura 35. Conector RP-TNC macho que permite asegurar el conector al equipo haciendo uso de una rosca.

El pigtail

En redes inalámbricas caseras no se utiliza el mismo tipo de cable coaxial que en redes en las que los vínculos son más extensos. Por ejemplo, conectar un equipo inalámbrico a un cable **LRM400** puede ser inviable, dado que generalmente estos cables utilizan un conector tipo N y los equipos que nosotros manipulamos usan conectores pequeños como los SMA o RPTNC. De esta forma nace el **pigtail** (que significa trenza), un cable coaxial de corta longitud que tiene un conector en cada punta. Se utiliza para vincular dispositivos inalámbricos y antenas o cables de largo alcance (utilizados en

PERDIDAS EN PIGTAIL

Según el fabricante, la pérdida de señal que introduce el uso de un cable Pigtail es del orden de los 0.4dB por pie (1 pie equivale a 30.48cm aproximadamente). Esto es para cables pequeños. Además, se puede decir que la pérdida permanece lineal en todo el cable y se desprecia cualquier variación para fines de cálculo.

radioenlaces de larga distancia). Podemos utilizar el conector que necesitemos en las puntas del cable, según sea nuestra necesidad.



Figura 36. `Pigtail` de conector SMA a N. Observamos que el cable no tiene una longitud mayor a 2 metros.

Radiación y salud

Recientemente llegó a nuestras manos la noticia que calificaba a los teléfonos celulares como posibles fuentes generadoras de cáncer. La Organización Mundial de la Salud (OMS), a través de la Agencia Internacional de Investigación del Cáncer, informó sobre un estudio (que no es el primero en realizarse) donde se concluía tal contundente noticia. Desde hace más de 10 años se viene estudiando sobre este tema en diferentes partes del mundo, ya que el auge de los celulares (y toda comunicación que utilice ondas electromagnéticas) está en crecimiento constante. Las redes que ofrecen servicios de telecomunicaciones –si hablamos de teléfonos, pueden ser fijos o móviles– utilizan tecnologías inalámbricas, es decir, hacen uso del espectro radioeléctrico. Estas frecuencias del espectro son las encargadas de transportar la información y de esta manera se presta un servicio al usuario final.

> EL CRECIENTE MERCADO DE CELULARES PREOCUPA A LOS MÉDICOS

Desde las primeras épocas de los celulares y demás sistemas inalámbricos, se plantea la inquietud para conocer si el uso de estas frecuencias provoca o no algún problema en la salud de las personas. Como consecuencia de los extensos estudios realizados a lo largo de los años, se fijaron valores de seguridad para estos sistemas. Hablaremos un poco de estos valores tolerables de seguridad que las normas establecen, para así poder tener conocimiento y no dar lugar a dudas o conjeturas posibles frente a noticias que no tienen mucho fundamento.

EN ARGENTINA, EN EL AÑO 1995, SE FIJARON LOS VALORES LÍMITES DE RADIACIÓN ELECTROMAGNÉTICAS

En Argentina, el Ministerio de Salud y Acción Social de la Nación presentó pautas a seguir a través de la Resolución N° 202/1995; se fijaron los valores límites de radiación electromagnética permitidos para la población. Los valores límites fueron considerados por los especialistas como los niveles precautorios, debajo de los cuales hay bajas posibilidades de afectar la salud humana. Desde (SECOM), se recopilaron este y otros estudios para emitir la Resolución N° 530/2000. Luego, en los años 2002 y 2003, se formularon otras resoluciones. Así se llega a la Resolución N° 3690/2004, que se basa en las resoluciones de salud de varios organismos internacionales como:

- Comisión Internacional de Protección Contra Radiaciones No Ionizantes (ICNIRP son sus siglas en ingles)
- Unión Internacional de Telecomunicaciones (recomendación UIT-T K-61 proteccion contra interferencias)
- Comité Electrotécnico Internacional (norma internacional 61566/1997)
- Instituto de Ingenieros Electrónicos y Electricistas (Norma IEEE 95.3/2002 sobre radiaciones)
- Reglamento dictado por la Agencia Nacional de Telecomunicaciones de Brasil (ANATEL son sus siglas en portugués)

En esta resolución se establece que las entidades titulares de licencias de servicios radioeléctricos y de radiodifusión deben demostrar que las radiaciones generadas por las antenas de sus estaciones no afectan a la población en el espacio circundante a ellas, indicando además los protocolos usados para las evaluaciones. Tratemos de aclarar algunos temas que tal vez desconozcamos cuando hacemos referencia a las ondas que se utilizan en estos

sistemas de telecomunicaciones y son fundamentales para comprender la esencia del tema.

Recordemos lo que significa la palabra **onda**, que es todo fenómeno físico capaz de permitir la propagación de energía sin producir desplazamiento de materia. Como vimos, una onda puede ser el sonido, la luz y las ondas radioeléctricas (estas junto a la luz son ondas electromagnéticas).

Si nos referimos al concepto **frecuencia**, planteamos que es la cantidad de ciclos completos que realiza una onda en un segundo. Lo que se traduce como la cantidad de veces que un fenómeno físico se repite en un intervalo de tiempo.

Si hablamos de ondas electromagnéticas decimos que son aquellas ondas que transportan energía radioeléctrica a distancia y se componen de un campo eléctrico y uno magnético. Estas ondas están presentes en la naturaleza también (no solo se generan de forma artificial). Por ejemplo el Sol genera ondas electromagnéticas, así como las estrellas u otros cuerpos celestes.

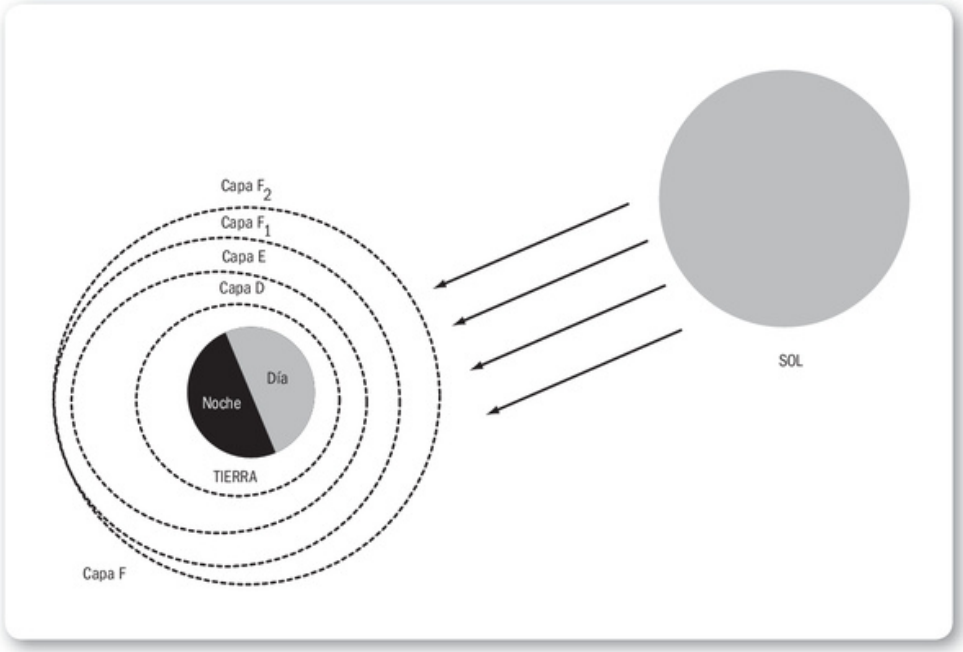


Figura 37. Vemos cómo se ioniza, por acción de los rayos solares, la capa de iones que rodea la Tierra. Esta capa se llama ionósfera. Los rayos actúan sobre las moléculas de la atmósfera.

Muchos habremos escuchado una clasificación de las ondas electromagnéticas en **no ionizantes** e **ionizantes**. Así, decimos que las ondas que son capaces de romper moléculas (por ejemplo, los rayos X o rayos gamma) se llaman ondas ionizantes. Mientras que las que no logran hacerlo son las no ionizantes (por ejemplo, ondas de radio, microondas, luz visible, entre otros). Es común que radiaciones no ionizantes puedan aumentar los movimientos de las moléculas, lo que se traduce en calor (los hornos microondas utilizan esta propiedad).

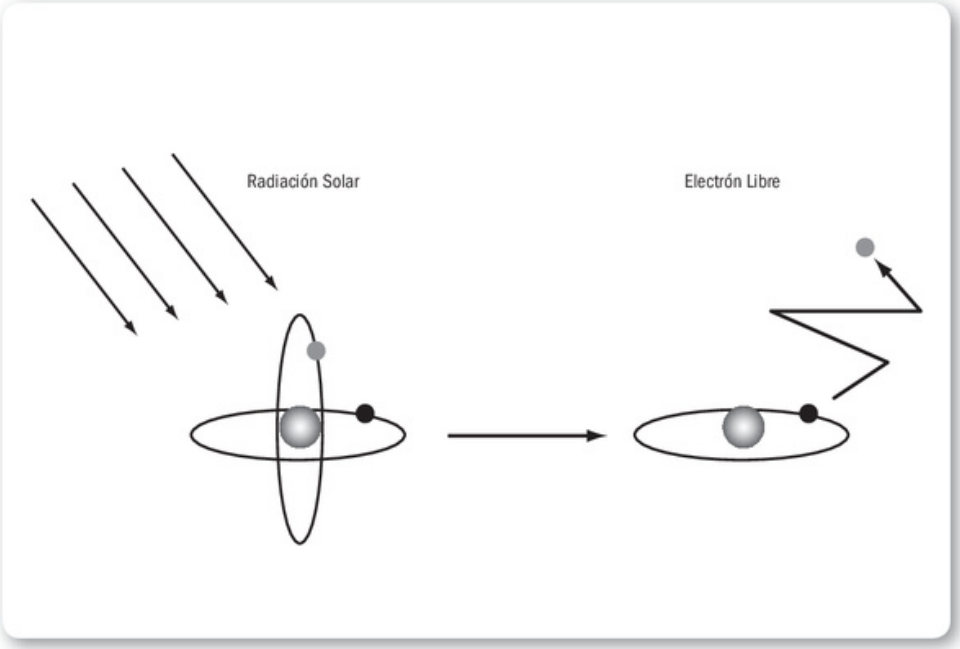


Figura 38. Este esquema muestra cómo se ioniza un átomo por la incidencia de la luz solar. El átomo se convierte en un ión positivo luego del efecto de la radiación electromagnética solar recibida.

MUCHOS CELULARES

En el mundo, hoy en día, hay alrededor de cinco mil millones de teléfonos móviles activos, o sea casi un celular por persona en una población global de 6,8 mil millones de almas. Según algunos informes sobre nuestro país, se dice que cerca de 35 millones de líneas activas están en la Argentina. Es un gran número que sigue creciendo.

Las radiaciones ionizantes son ondas electromagnéticas de frecuencia extremadamente elevada. Tienen energía suficiente para producir la ionización mediante la ruptura de los enlaces atómicos, y afectar así el estado natural de los tejidos vivos.

Como la energía es proporcional a la frecuencia, si aumentamos la frecuencia (el caso de las radiaciones ionizantes) la energía irradiada se incrementa notablemente.

A las radiaciones que no poseen energía suficiente para ionizar la materia se las denomina no ionizantes. Las radiaciones no ionizantes no tienen energía suficiente para producir el proceso de ionización, que puede traer problemas en la salud. De todas formas las RNI también pueden producir un riesgo en la salud, si no se respetan las normas nacionales e internacionales que establecen los valores máximos de exposición del ser humano a este tipo de radiaciones. Además, según el grado y tiempo de exposición, se podrían generar daños de diferente magnitud al estar expuestos a las RNI.

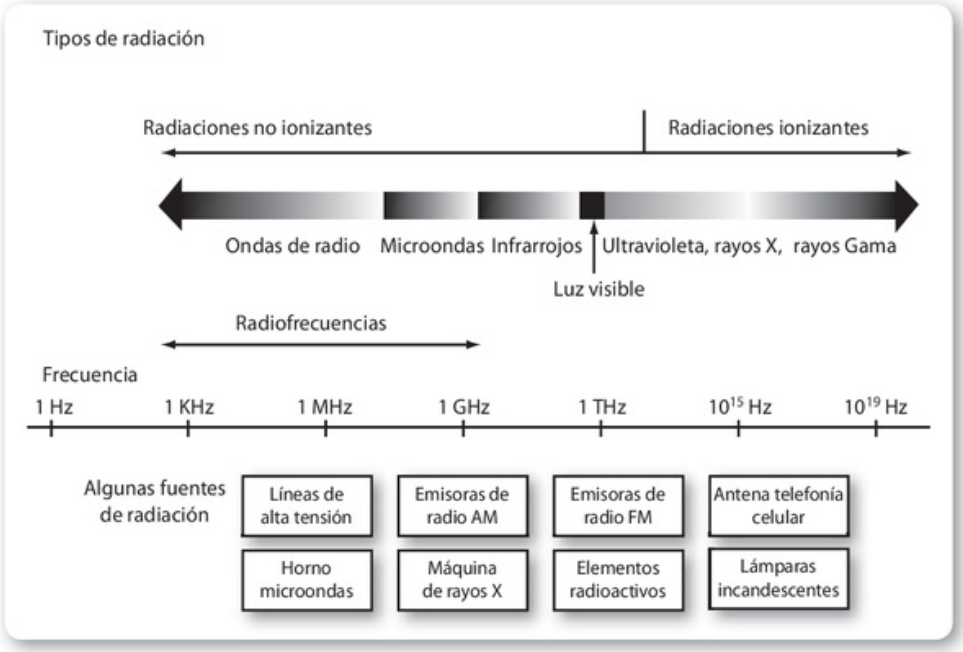


Figura 39. Gráfico que representa las frecuencias del espectro radioeléctrico. Desde las bajas frecuencias (50 Hz de la red eléctrica) pasando por la luz visible (RNI) hasta llegar a las radiaciones ionizantes.

¿Es peligrosa la radiación electromagnética?

Como dijimos antes, el peligro depende del tipo de radiación y la dosis que el ser humano reciba. Si una radiación puede romper las moléculas de nuestro cuerpo, entonces se considera nociva. En caso de que eso suceda con nuestro ADN, se podría ocasionar un cáncer. Un solo fotón de rayos X puede romper una molécula de ADN, de todas formas millones de fotones de luz visible no podrían conseguirlo. Tomemos un ejemplo práctico para entender el concepto. Pensemos en la cantidad de energía que se necesita para lanzar una piedra al otro lado del océano Atlántico. Aunque muchas personas (coordinadas) lancen sus piedras, ninguna llegaría a la otra orilla del océano. Otro factor que debemos tener en cuenta es la dosis, que depende de la intensidad de la radiación y el tiempo en que uno está expuesto. Si nos exponemos a fuentes naturales de radiación, como el sol, en dosis que no son peligrosas no veremos nuestra salud afectada.



Figura 40. Debido a que no podemos superar cierto valor de umbral cuando estamos expuestos a radiación, se nos permiten realizar cierta cantidad de radiografías al año.

Según la clasificación que realizó la **OMS** (**Organización Mundial de la Salud**) en su polémico informe, se colocó a los teléfonos celulares en un grupo llamado **2B**. En este grupo se encuentran los agentes posiblemente carcinógenos pero cuya capacidad para provocar cáncer no está demostrada. Dentro de ese mismo grupo existen otros 240 agentes ambientales, como algunas sustancias químicas industriales, el DDT (compuesto en los insecticidas) y hasta el café (ya que es considerado potencial causante de tumores intestinales) y los vegetales en escabeche.

Existe otro grupo llamado **2A** en el que se encuentran los agentes probablemente cancerígenos, en estos casos sí se comprobó que provocan cáncer en las personas.

Las respuestas al informe no se hacen esperar y diferentes paneles de expertos expresan lo que nosotros analizamos previamente. Por ejemplo, en la Argentina, una semana luego del polémico informe, científicos y autoridades sanitarias llevaron tranquilidad a los usuarios recomendando un uso racional del celular.

Imaginamos que si hubiera un vínculo claro entre el cáncer y el uso del celular, la tasa de casos sería muy alta como para pasar desapercibida y esto sería una clara señal de alerta.

De esta forma podemos decir, a modo de prevención ya que ningún estudio nos da seguridad para indicar si son malas para la salud las ondas electromagnéticas originadas por celulares, que no recomendamos dejar de usarlos ni tampoco estar todo el día con el celular pegado en la oreja (esto aumenta el impacto de la radiación).

Las personas que menos se verían afectadas son las que usan el celular mirando la pantalla (SMS, chat, e-mails, redes sociales, entre otros) y no deberían alarmarse en lo más mínimo, de la misma forma que los usuarios de manos libres o auriculares para hablar.

RESUMEN

En el inicio del capítulo aprendimos el concepto básico de antena para luego especificar las características más importantes. De esta forma clasificamos las antenas según su patrón de radiación o su construcción física. Para vincular las antenas y los equipos de nuestra red inalámbrica utilizamos cables y conectores, detallamos características y los tipos más usados. En la parte final del capítulo hablamos sobre el informe de la OMS y si las ondas electromagnéticas afectan o no a la salud de las personas.

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	¿Qué es una antena isotrópica?
6	¿Cuáles son las antenas sectoriales?
7	¿Cuál cable coaxial es recomendando 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	¿Cuál es la principal diferencia entre radiaciones no ionizantes y las ionizantes?

Servicios al lector

En esta sección nos encargaremos de presentar un útil índice temático para poder encontrar en forma sencilla los términos que necesitamos. Además, podremos ver una interesante selección de sitios y programas que se encuentran relacionados con el contenido de esta obra.

▾ Índice temático.....306

Servicio de atención al lector: **usershop@redusers.com**

Índice temático

A

Abrazadera 233
Acceso a la red 17
Actualizar controlador 107
Adaptador inalámbrico Ethernet 94
Administrar redes inalámbricas 146
Agregar o quitar cuentas de usuario 134
Ahorro de costos 29
Albert Einstein 62
Amenazas de seguridad 176
Amplificador de antena 221
Amplificadores de señal 37
Ancho de banda 254
Ancho del haz 276
Ángulo de elevación óptimo 233
Ángulo determinado 219
Antena isotrópica 273
Antena panel 227
Antenas de hilo 264
Antenas direccionales 219/220
Antenas parabólicas 220
Antivirus 261
Ataques de repetición 164/173
Autenticación abierta 169
Autenticación de llave compartida 169
Autentificador 165

B

Backbone 22
Bajo consumo 251
Baliza 94
Bayoneta 295
Beacon 94, 95
Bidireccional 23
Bluetooth 246/250/253/256
Brújula 234
BSS 139/140

B

BSSID 140
Bugs 186

C

Cable coaxial 224/287
Cable UTP 141
Cajas estancas 37/225
Cámara anecoica 269
Cámaras de vigilancia inalámbricas 37
Cambiar configuración de uso compartido avanzado 146
Cambiar configuración del adaptador 141/143
Cambiar la configuración de una cuenta actual 134
Campo eléctrico oscilante 268
Campo electromagnético radiado 267
Campo magnético 267
Caos en el espacio 210
Capa de aplicación 16/17
Capa de enlace de datos 17
Capa de presentación 16/17
Capa de red 17/18/97
Capa de sesión 16, 17
Capa de transporte 16/17/18
Capa física 17
Centro de redes y recursos compartidos 141/143/146
Chat 187
Cifrado 157/161
Cimiento 234
Climas húmedos 231
Climas secos y áridos 231
Compatibilidad 50
Concentrador 22
Concesión expirada 118

C

Concesión obtenida ... 118
Conector N hembra ... 291
Conector N macho ... 290
Conector RP-SMA hembra ... 293
Conector SMA macho ... 293
Conexión ad hoc ... 145
Contraseña ... 99/113
Controlador ... 107
CRC ... 164, 173
Crear nueva cuenta de usuario ... 134

D

Denegación de servicio ... 160
Desconectar ... 145
Diagrama de radiación ... 275
Dipolos ... 281
Dirección IP ... 126
Dirección IP dinámica ... 115
Dirección IP fija ... 115
Direcciones IP duplicadas ... 198
Distancia ... 226
División de frecuencia ortogonal ... 50
División en capas ... 15
Divisores de señal ... 37
DNS ... 126
Documentar el problema ... 198

E

EAP ... 166
EAPOL ... 166
Enfoque metodológico ... 180
Enlace de larga distancia ... 208
Enlace remoto ... 211
Enlace remoto fijo ... 212
Enlace remoto móvil ... 212
Ericsson ... 253

F

FHSS ... 53
Fibras ópticas ... 208
Filtrado por MAC ... 170

F

Firewall ... 177
Firma digital ... 158
Firmware ... 67/70/71/186
Fm ... 63
Frecuencia ... 53
Frecuencia ortogonal ... 50
Full duplex ... 213

G

Ganancia de antena ... 274
Garantía de la información ... 155
Gmail ... 200
Google ... 126
Google Earth ... 234
Google Maps ... 196
GPS ... 234
Grupo de aplicación ... 17
Grupo de flujo de datos ... 17
Guglielmo Marconi ... 264

H

Half duplex ... 213
Heinrich R. Hertz ... 264
Hembra ... 287
Herramientas ... 201
HomeRF ... 251
Hub ... 46

I

Icono de Equipo ... 106
Identificador ... 27
Impedancia característica de antena ... 271
Impresora ... 28
Infrarrojo ... 252
InSSIDer ... 86
InstallShield ... 105
interoperabilidad ... 253
Intervalo de Beacon ... 95
Ionizantes ... 300
IP ... 118

I

IP estática 120
IP privada 115
IP pública 115

J

James C. Maxwell 264
Jaula de Faraday 269/270
Joysticks de consolas 248

L

LAN 19, 26
LEDs 68
Lenguaje HTML 47
Línea visual libre 215

M

MAN 19
MAU 22
MIC 164
Modelo de referencia OSI 14
MSN 190

N

NAT 91
Navegador web 81
NetStumbler 86/232/233
Número de canal 39/84

O

OFDM 53
OMS 303
Ondas electromagnéticas 14/23/209
Organización Internacional para la Normalización 14
Organización Mundial de la Salud 303

P

PAN 25
Parabólicas 285
Parrilla 284
Patch 283
Patrón de radiación 275

R

Radio Mobile 226
Radioenlace de larga distancia 208
Radioenlace de microondas 215
Radioenlace de onda corta 215
Radioenlace infrarrojo 215
Radioenlace satelital 215
Radioenlace UHF 215
Red cerrada 169
Red congestionada 203
Red fuera de servicio 204
Repetidores activos 217
Repetidores pasivos 217

S

Segunda zona de Fresnel 230
Semidúplex 213
Sensibilidad del receptor 223
Servidor de autentificación 165
Símplex 214
SmartPhones 259/260
Socket 293
Spam 174

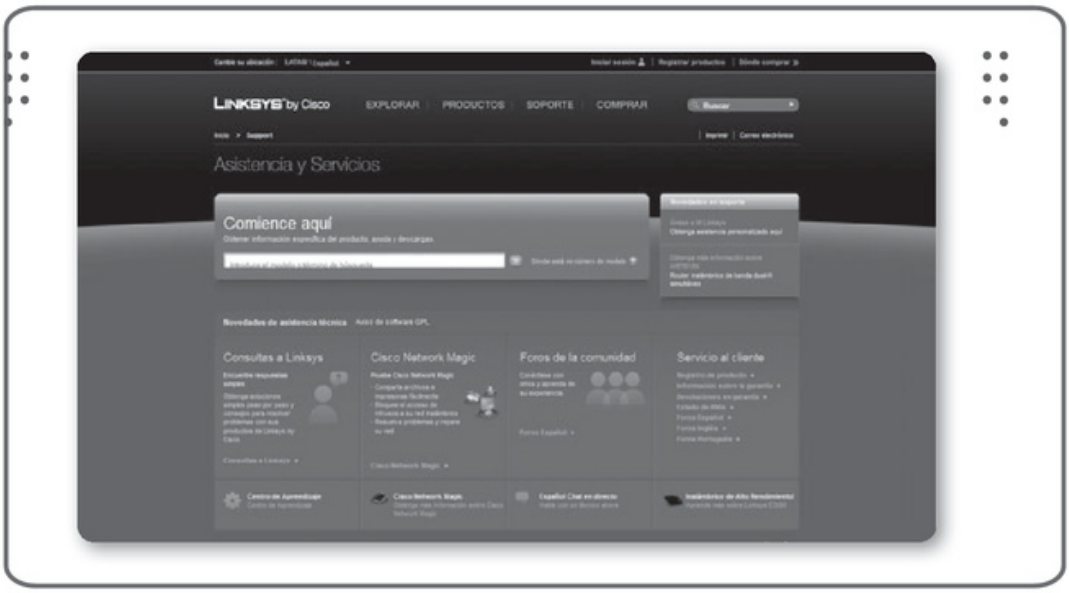
T

TCP/IP 17
Telecomunicaciones 208
Telegrafía 264
Tkip 164
Tnc hembra 296
Tnc macho 296
Topografía 215

Sitios web

LINKSYS BY CISCO ● www.linksysbycisco.com

En este sitio encontraremos todas las novedades y las actualizaciones de nuestros productos Linksys. Para obtener información sobre un producto específico, ingresaremos a la opción Soporte en el menú y podremos consultar el modelo de nuestro dispositivo.



PARAMOWIFIX ● www.paramowifix.net

Encontraremos información vinculada a la creación de diferentes tipos de antenas caseras. Provee enlaces a distintos sitios en castellano o inglés, en los que podremos encontrar detallados paso a paso para construir nuestras antenas de red inalámbrica.



RADIO MOBILE BY ROGER COUDÉ ● www.cplus.org/rmw

Sitio oficial del programa Radio Mobile creado por Roger Coudé para la simulación de enlaces de larga distancia. El autor nos invita a descargar y utilizar el programa de manera totalmente gratuita. Además proporciona un detallado manual para aprender a usar todas sus funciones y realizar una instalación completa.



STEVE´S TECH LOG ● http://stevehorbachuk.com/?cat=11

Steve, el autor de este útil blog, nos proporciona un emulador de router inalámbrico, el WRT54G (y otras variantes como el WRT54GS, el WRT54GL y el WRTSL54GS). Con este emulador podemos probar las configuraciones antes de hacerlas en nuestro equipo. Encontramos el emulador dentro de la categoría Linksys.



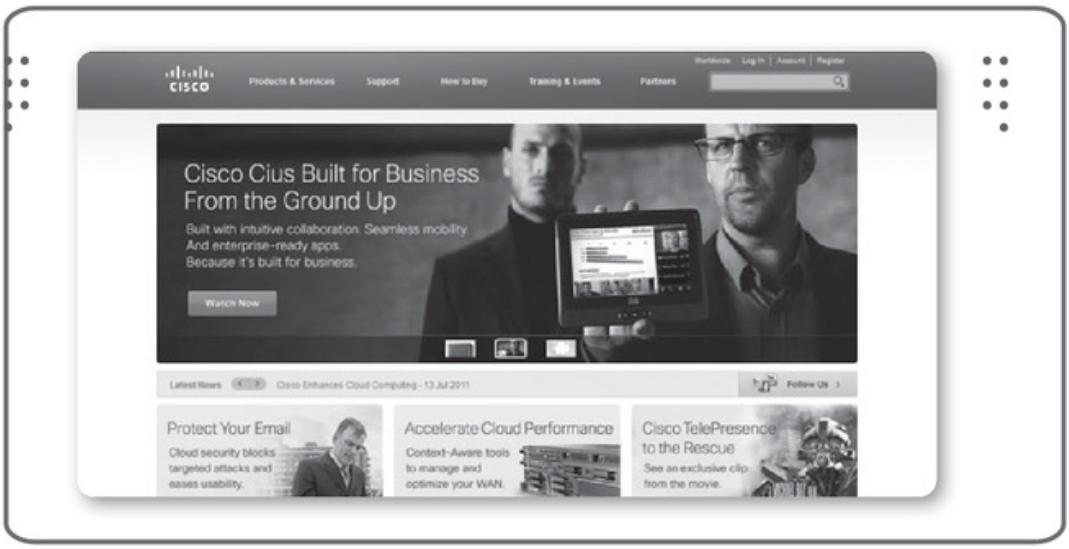
SKYANGEL ● http://skyangel.wikidot.com/emulators

Si necesitamos manuales y más emuladores de dispositivos inalámbricos para testear nuestras configuraciones antes de aplicarlas, podemos consultar este sitio web. Hay emuladores para fabricantes como Netgear, Linksys, D-Link, Belkin, entre otros. Además encontramos guías de configuración para tomar como ejemplo.



CISCO ● www.cisco.com

Sitio oficial del fabricante de dispositivos de red Cisco, que además de proporcionar información de nuevos productos nos ofrece el soporte para estos. En la pestaña Soporte del menú vamos a encontrar diferentes categorías así como un buscador donde podemos ingresar el número de nuestro dispositivo.



DD-WRT ● www.dd-wrt.com

El sitio oficial del proyecto DD-WRT tiene la información que necesitamos a la hora de actualizar el firmware de nuestro router inalámbrico para agregar funcionalidades. El firmware DD-WRT es una alternativa de firmware basada en Linux, que provee fácil manejo de las configuraciones y gran estabilidad.



WI-FI ALLIANCE ● www.wi-fi.org

Para estar actualizados en cuanto a novedades de la tecnología WiFi, podemos consultar el sitio oficial de la Wi-Fi Alliance. Entre muchas opciones disponibles, está la lista de empresas que son miembros de esta alianza y por lo tanto sus productos respetan los estándares recomendados por la organización IEEE.



Programas relacionados

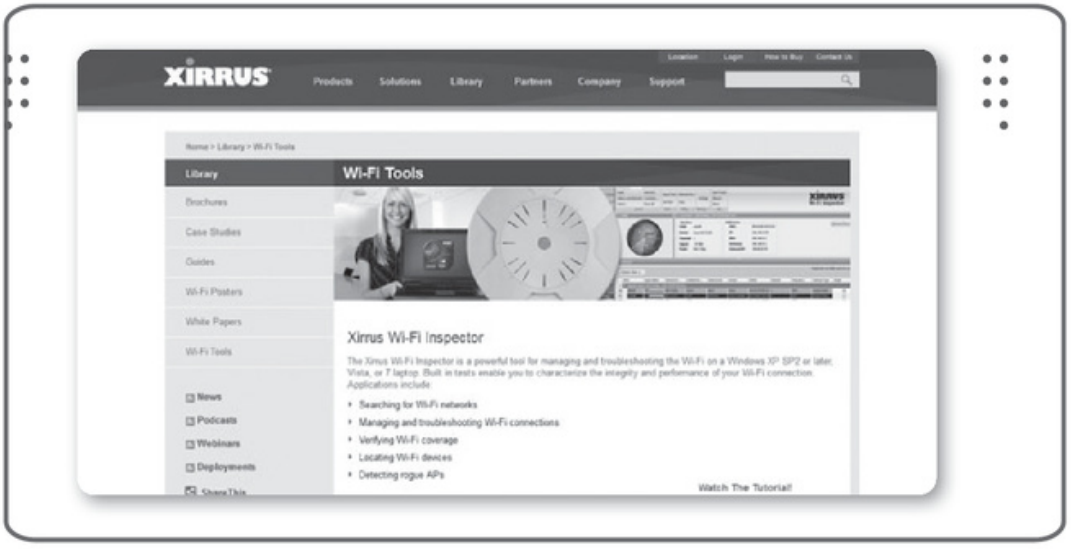
NETSTUMBLER ● www.netstumbler.com

Un analizador de redes inalámbricas es una de las herramientas más usadas por un administrador de redes. Netstumbler proporciona una interfaz fácil de utilizar a la hora de ver qué ocurre en el espectro.



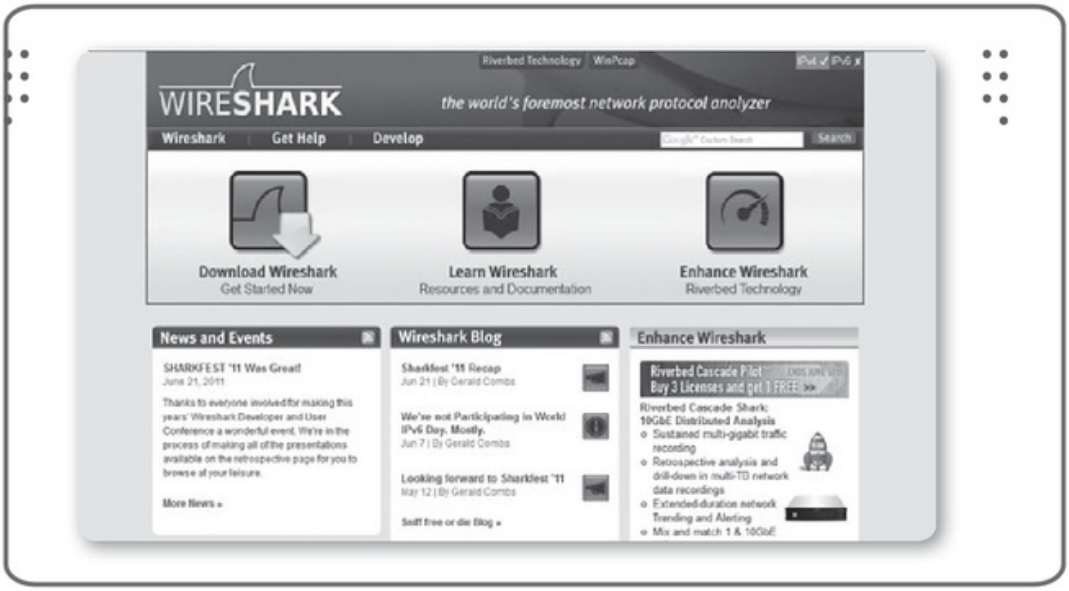
XIRRUS ● www.xirrus.com/library/wifitools.php

la empresa Xirrus nos proporciona una opción profesional y muy poderosa para monitorear el espectro. Podremos administrar y verificar problemas en la conexión inalámbrica desde una interfaz dinámica.



WIRESHARK ● www.wireshark.org

Cuando necesitamos ver qué pasa en nuestra red inalámbrica, podemos recurrir a este software. Wireshark analiza toda la información que circula por nuestra red en tiempo real y se encarga de presentarla de forma ordenada en la pantalla.



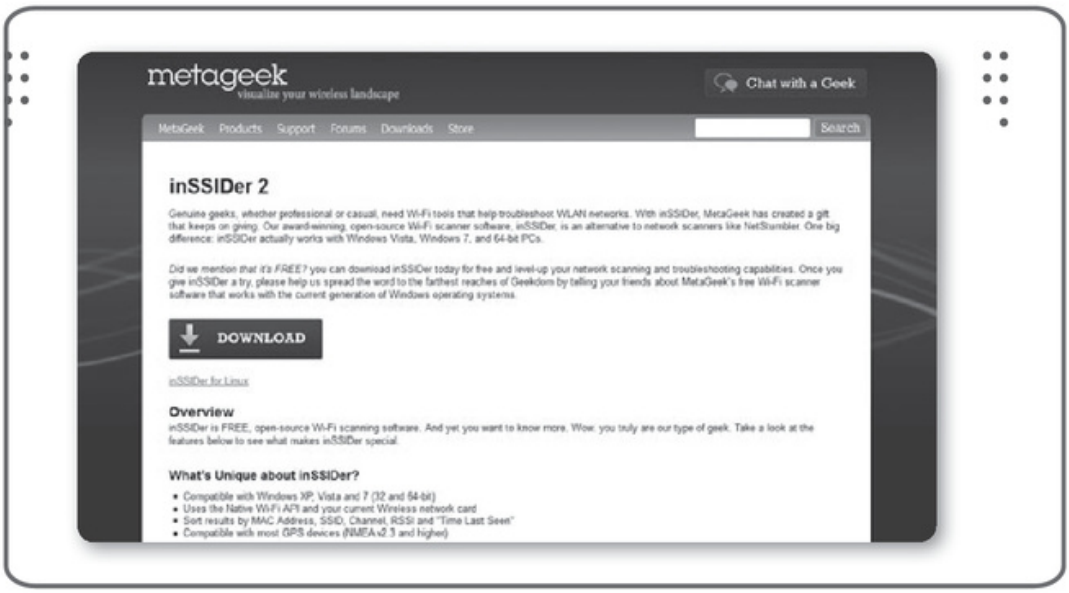
RADIO MOBILE ● www.g3tvu.co.uk/Radio_Mobile.htm

En este sitio web encontramos el instalador del programa Radio Mobile totalmente actualizado y customizado para ahorrarnos los pasos de configuración que necesita el software para quedar 100% funcional. Ian Brown es el creador de este sitio y quien mantiene el contenido al día.



INSSIDER ● www.metageek.net/products/inssider

Una alternativa a las herramientas para detectar redes inalámbricas es inSSIDer. Creada como una opción OpenSource, muy similar al famoso Kismet. Se presenta con una muy buena interfaz, fácil de usar. Corre sobre Windows Vista o superior.



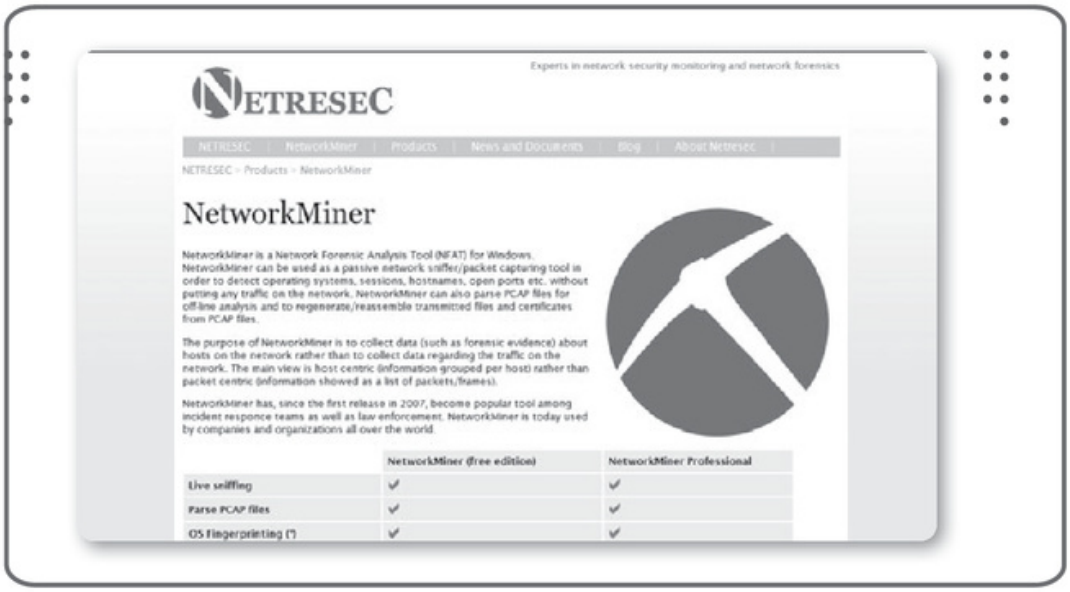
WEFI ● www.wefi.com

Si estamos cansados de hacer clics para probar diferentes conexiones WiFi públicas, intentando verificar cuál es la que funciona, necesitamos usar WeFi. Es un simple programa que automáticamente detecta y califica todas las conexiones WiFi cercanas conectándose a la de mejor calidad.



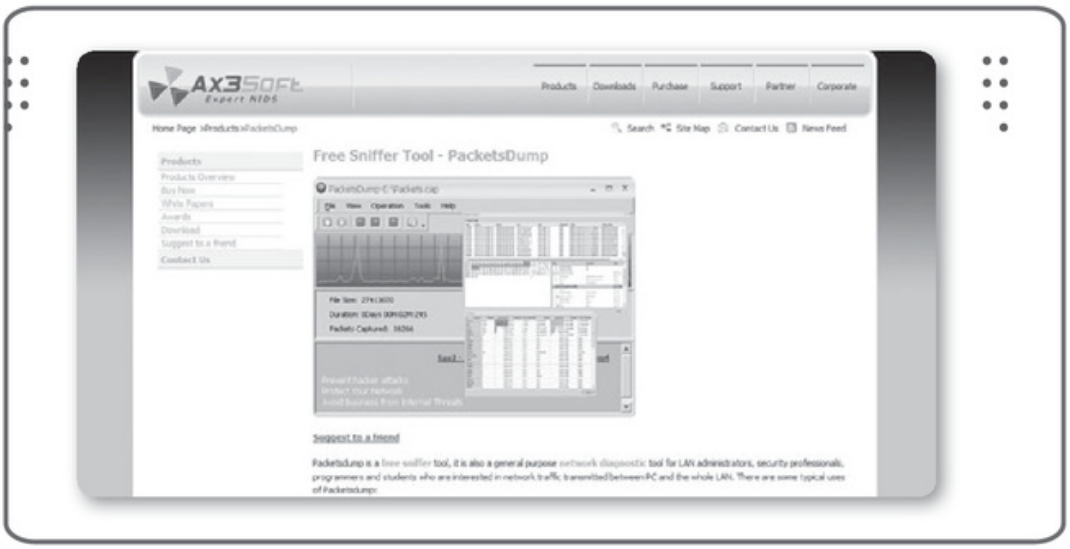
NETWORKMINER ● www.netresec.com/?page=NetworkMiner

Este programa es una herramienta de análisis para Windows muy poderosa. Similar a las funciones que presta el famoso Wireshark pero con mayores prestaciones. Puede ser usado en forma pasiva para escuchar y capturar paquetes, que luego serán analizados.



PACKETSDUMP ● www.ids-sax2.com/PacketsDump.htm

Folder Lock y Lock Folder XP, las mejores herramientas de encriptación de datos, son aplicaciones pesadas y lentas en lo que a la interface refiere. Si preferimos una herramienta que consuma pocos recursos, encontraremos en AxCrypt lo que estábamos necesitando.



CLAVES PARA COMPRAR
UN LIBRO DE COMPUTACIÓN

1 SOBRE EL AUTOR Y LA EDITORIAL

Revise que haya un cuadro "sobre el autor", en el que se informe sobre su experiencia en el tema. En cuanto a la editorial, es conveniente que sea especializada en computación.

2 PRESTE ATENCIÓN AL DISEÑO

Compruebe que el libro tenga guías visuales, explicaciones paso a paso, recuadros con información adicional y gran cantidad de pantallas. Su lectura será más ágil y atractiva que la de un libro de puro texto.

3 COMPARE PRECIOS

Suele haber grandes diferencias de precio entre libros del mismo tema; si no tiene el valor en tapa, pregunte y compare.

4 ¿TIENE VALORES AGREGADOS?

Desde un sitio exclusivo en la Red, un Servicio de Atención al Lector, la posibilidad de leer el sumario en la Web para evaluar con tranquilidad la compra, y hasta la presencia de adecuados índices temáticos, todo suma al valor de un buen libro.

5 VERIFIQUE EL IDIOMA

No solo el del texto; también revise que las pantallas incluidas en el libro estén en el mismo idioma del programa que usted utiliza.

usershop.redusers.com
VISITE NUESTRO SITIO WEB

» Vea información más detallada sobre cada libro de este catálogo.
» Obtenga un capítulo gratuito para evaluar la posible compra de un ejemplar.
» Conozca qué opinaron otros lectores.
» Compre los libros sin moverse de su casa y con importantes descuentos.
» Publique su comentario sobre el libro que leyó.
» Manténgase informado acerca de las últimas novedades y los próximos lanzamientos.

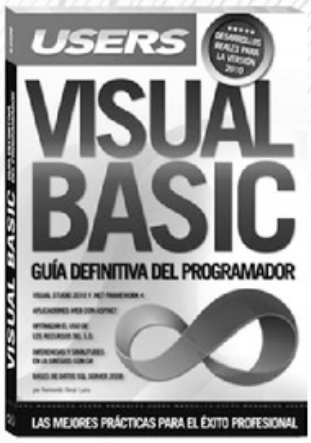
TAMBIÉN PUEDE CONSEGUIR NUESTROS LIBROS EN KIOSCOS O PUESTOS DE PERIÓDICOS, LIBRERÍAS, CADENAS COMERCIALES, SUPERMERCADOS Y CASAS DE COMPUTACIÓN.



LLEGAMOS A TODO EL MUNDO VÍA »OCA * Y DHL **
* SOLO VÁLIDO EN LA REPÚBLICA ARGENTINA // ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

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

usershop.redusers.com



Visual Basic

Este libro está escrito para aquellos usuarios que quieran aprender a programar en VB.NET. Desde el IDE de programación hasta el desarrollo de aplicaciones del mundo real en la versión 2010 de Visual Studio, todo está contemplado para conocer en profundidad VB.NET al finalizar la lectura.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / 978-987-1773-57-2



Microcontroladores

Este manual es ideal para aquellos que quieran iniciarse en la programación de microcontroladores. A través de esta obra, podrán conocer los fundamentos de los sistemas digitales, aprender sobre los microcontroladores PIC 16F y 18F, hasta llegar a conectar los dispositivos de forma inalámbrica, entre muchos otros proyectos.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / 978-987-1773-56-5



Programador.NET

Este libro está dirigido a todos aquellos que quieran iniciarse en el desarrollo bajo lenguajes Microsoft. A través de los capítulos del manual, aprenderemos sobre POO y la programación con tecnologías .NET, su aplicación, cómo interactúan entre sí y de qué manera se desenvuelven con otras tecnologías existentes.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / 978-987-1773-26-8



Photoshop: proyectos y secretos

En esta obra aprenderemos a utilizar Photoshop, desde la original mirada de la autora. Con el foco puesto en la comunicación visual, a lo largo del libro adquiriremos conocimientos teóricos, al mismo tiempo que avanzaremos sobre la práctica, con todos los efectos y herramientas que ofrece el programa.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / 978-987-1773-25-1



WordPress

Este manual está dirigido a todos aquellos que quieran presentar sus contenidos o los de sus clientes a través de WordPress. En sus páginas el autor nos enseñará desde cómo llevar adelante la administración del blog hasta las posibilidades de interacción con las redes sociales.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / 978-987-1773-18-3



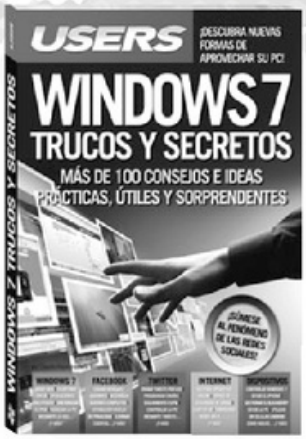
Administrador de servidores

Este libro es la puerta de acceso para ingresar en el apasionante mundo de los servidores. Aprenderemos desde los primeros pasos sobre la instalación, configuración, seguridad y virtualización; todo para cumplir el objetivo final de tener el control de los servidores en la palma de nuestras manos.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-1773-19-0

¡Léalo antes Gratis!

En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.



Windows 7: Trucos y secretos

Este libro está dirigido a todos aquellos que quieran sacar el máximo provecho de Windows 7, las redes sociales y los dispositivos ultraportátiles del momento. A lo largo de sus páginas, el lector podrá adentrarse en estas tecnologías mediante trucos inéditos y consejos asombrosos.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-1773-17-6



Desarrollo PHP + MySQL

Este libro presenta la fusión de dos de las herramientas más populares para el desarrollo de aplicaciones web de la actualidad: PHP y MySQL. En sus páginas, el autor nos enseñará las funciones del lenguaje, de modo de tener un acercamiento progresivo, y aplicar lo aprendido en nuestros propios desarrollos.

→ COLECCIÓN: MANUALES USERS
→ 432 páginas / ISBN 978-987-1773-16-9



Excel 2010

Este manual resulta ideal para quienes se inician en el uso de Excel, así como también para los usuarios que quieran conocer las nuevas herramientas que ofrece la versión 2010. La autora nos enseñará desde cómo ingresar y proteger datos hasta la forma de imprimir ahorrando papel y tiempo.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-1773-15-2



Técnico Hardware

Esta obra es fundamental para ganar autonomía al momento de reparar la PC. Aprenderemos a diagnosticar y solucionar las fallas, así como a prevenirlas a través del mantenimiento adecuado, todo explicado en un lenguaje práctico y sencillo.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1773-14-5



PHP Avanzado

Este libro brinda todas las herramientas necesarias para acercar al trabajo diario del desarrollador los avances más importantes incorporados en PHP 6. En sus páginas, repasaremos todas las técnicas actuales para potenciar el desarrollo de sitios web.

→ COLECCIÓN: MANUALES USERS
→ 400 páginas / ISBN 978-987-1773-07-7



AutoCAD

Este manual nos presenta un recorrido exhaustivo por el programa más difundido en dibujo asistido por computadora a nivel mundial, en su versión 2010. En sus páginas, aprenderemos desde cómo trabajar con dibujos predeterminados hasta la realización de objetos 3D.

→ COLECCIÓN: MANUALES USERS
→ 384 páginas / ISBN 978-987-1773-06-0

USERS PRESENTA...

¡EL PRIMER EBOOK USERS!

Sí, ya podés leer Hackers al descubierto en tu PC, notebook, Amazon Kindle, iPad, en el celular...

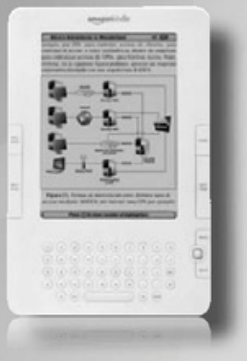
CONSEGUILO DESDE CUALQUIER PARTE DEL MUNDO

A UN PRECIO INCREÍBLE



¿QUÉ ESTÁS ESPERANDO?







¡LEELO DONDE QUIERAS!

INGRESA YA A USERSHOP.REDUSERS.COM Y ENTERATE MÁS

INSTALACIÓN Y VIRTUALIZACIÓN DE SERVIDORES CORPORATIVOS



Este libro es la puerta de acceso para ingresar en el apasionante mundo de los servidores. Aprenderemos desde los primeros pasos sobre la instalación, configuración, seguridad y virtualización; todo para cumplir el objetivo final de tener el control de los servidores en la palma de nuestras manos.

» DISEÑO / DESARROLLO
» 352 PÁGINAS
» ISBN 978-987-1773-19-0



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

USERS

REDES WIRELESS

Presentamos una obra fundamental para todos aquellos que quieran conocer a fondo las tecnologías inalámbricas y, así, poder manejar todos los dispositivos y equipos que nos rodean en el mundo actual.

A través de las páginas de este libro, repasaremos las cuestiones técnicas que alguna vez parecieron complejas, hasta llegar a las configuraciones puntuales para instalar y mantener redes inalámbricas. Para esto, veremos en detalle el modelo OSI y TCP/IP, los diferentes tipos de redes, así como también los estándares para esta tecnología y el hardware utilizado. Además, nos pondremos al tanto sobre las maneras de mantener la información segura y solucionaremos problemas de modo sencillo a través de un método práctico.

Al completar la lectura de este texto, el lector se encontrará capacitado para instalar y poner a punto una red inalámbrica, conociendo a fondo el detalle de sus características y funcionamiento, como solo un profesional puede hacerlo.



CONTENIDO

1 I INTRODUCCIÓN A LAS REDES INALÁMBRICAS
Modelo OSI / Modelo TCP/IP / Tipos de redes / Funcionamiento de las redes inalámbricas / Ventajas y desventajas / Puntos de acceso / Estándares / Abierto y cerrado / IEEE 802.11

2 I HARDWARE PARA REDES INALÁMBRICAS
Configuración de puntos de acceso / Instalar el hardware y actualizarlo / Configurar de acuerdo con el modelo OSI

3 I CONFIGURACIÓN EN WINDOWS
Instalar clientes / Instalación del hardware / Selección de la red / Configurar opciones de TCP/IP / Modo infraestructura / Configuración de una red ad-hoc

4 I SEGURIDAD EN LA RED
Seguridad inalámbrica de la información / Confidencialidad / Autenticación / Integridad / Disponibilidad / No repudio / WLAN / Atributos de seguridad / WEP, WPA y WPA2 / Integridad de datos / Las 10 amenazas más comunes

5 I RESOLUCIÓN DE PROBLEMAS
Enfoque metodológico / Pasos fundamentales / Tensión eléctrica / Actualizaciones / Nuestro método / Caso práctico / Herramientas

6 I ENLACES DE LARGA DISTANCIA
¿Qué es un radioenlace? / Tipos de enlaces / ¿Qué necesito para llegar más lejos? / Alineación de antenas / Cálculo de enlace / Radio mobile

7 I ENLACES DE CORTA DISTANCIA
Wireless Personal Area Network / Bluetooth / Infrarrojos / HomeRF / Zigbee

8 I ANTENAS Y CONECTORES
¿Qué es una antena? / Funcionamiento y características / Clasificación según el patrón y su construcción / Cables y conectores / Radiación y salud / ¿Es peligrosa la radiación electromagnética?

NIVEL DE USUARIO

PRINCIPIANTE | INTERMEDIO | AVANZADO | EXPERTO

RedUSERS.com

En este sitio encontrará una gran variedad de recursos y software relacionado, que le servirán como complemento al contenido del libro. Además, tendrá la posibilidad de estar en contacto con los editores, y de participar del foro de lectores, en donde podrá intercambiar opiniones y experiencias.

Si desea más información sobre el libro puede comunicarse con nuestro Servicio de Atención al Lector: usershop@redusers.com

WIRELESS NETWORKS

In this book, the reader will find an exhaustive theoretical and practical corpus about wireless networks. Every aspect of this technology, from short range networks to security issues and troubleshooting, is covered in this manual.

ISBN 978-987-1773-98-5

MANUALES USERS MANUALES USERS MANUA

CONVIÉRTASE EN UN EXPERTO EN REDES INALÁMBRICAS