



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

Índice Tema 14

1. Comunicaciones emergentes: protocolos 802.11B Wi-Fi.
2. Características funcionales y técnicas. Sistemas de expansión del espectro. Sistemas de acceso. Modos de operación.
3. Seguridad.
4. Normativa reguladora. Ventajas e inconvenientes.



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

TEMA 14

Comunicaciones emergentes: protocolos 802.11B Wi-Fi. Características funcionales y técnicas. Sistemas de expansión del espectro. Sistemas de acceso. Modos de operación. Seguridad. Normativa reguladora. Ventajas e inconvenientes.

1. COMUNICACIONES EMERGENTES: PROTOCOLOS 802.11B WI-FI.

El creciente uso de portátiles dentro de la empresa y del aumento de movilidad del trabajador ha aumentado la demanda de las redes inalámbricas. Hasta hace poco, la tecnología inalámbrica era un remiendo para sistemas incompatibles de ciertos proveedores. La tecnología era lenta, costosa y reservada para situaciones móviles o ambientes hostiles donde resultaba imposible cablear. Con el desarrollo de los estándares de la industria y del despliegue del hardware de redes inalámbricas ligeras a través de una amplia sección del mercado, la tecnología inalámbrica llega a nuestro tiempo.

El término red inalámbrica se refiere a la tecnología que permite a dos o más ordenadores comunicarse con protocolos de red estándares, pero sin necesidad de cable alguno. En sentido estricto, cualquier tecnología que haga esto se podría llamar establecimiento de una red inalámbrica. Sin embargo, generalmente se refiere a LANs inalámbricas. Esta tecnología, reforzada por la aparición de la industria de proveedores como IEEE 802.11, ha producido bastantes soluciones prácticas cada vez más populares en negocios y escuelas, así como usos sofisticados donde es imposible el cableado, por ejemplo almacenamiento de mercancías o en portátiles de uso en venta directa.

2. CARACTERÍSTICAS FUNCIONALES Y TÉCNICAS. SISTEMA DE EXPANSIÓN DEL ESPECTRO. SISTEMAS DE ACCESO. MODOS DE OPERACIÓN.

La arquitectura 802.11.

La arquitectura de 802.11 está basada en una arquitectura celular en la que el sistema se divide en celdas denominadas BSS (Basic Service Set), cada una de las cuales está gobernada por una estación base llamada punto de acceso o AP (Access Point). Los puntos de acceso se conectan a una especie de backbone que recibe el nombre de sistema de distribución (DS, Distribution System), que en la mayoría de los casos está basado en tecnología Ethernet (aunque también puede ser radioeléctrico). El con-

junto de todas las WLAN, con sus correspondientes celdas y puntos de acceso, se presenta a los niveles superiores como una unidad lógica llamada ESS (Extended Service Set). Además, el estándar también define el concepto de portal como un dispositivo de interconexión entre una red 802.11 y otra red LAN 802.x. Como cualquier protocolo 802.x, el estándar 802.11 especifica los requisitos para el nivel físico y el subnivel de MAC. Existen tres niveles físicos:

- FHSS en la banda de 2,4 GHz.
- DSSS también en la banda de 2,4 GHz.
- Y el último en la banda infrarroja.

Sobre el nivel físico se encuentra el nivel de MAC, encargado de funciones tales como la fragmentación, el arbitrio del acceso al medio compartido o la retransmisión de paquetes.

Nivel físico.

Las tres capas físicas originalmente definidas en el 802.11 incluyen dos espectros de radio y una especificación de infrarrojos. Los estándares basados en radio operan dentro de la banda 2.4 GHz ISM. Estas bandas de frecuencia son reconocidas por los reguladores internacionales, como FCC (EE.UU.), ETSI (Europa) y la MKK (Japón), como operaciones de radio sin licencia, para usos científicos, militares e industriales.

Las técnicas de espectro ensanchado, además de satisfacer los requerimientos mínimos, aumentan la seguridad, elevan el throughput y permiten que varios productos inconexos compartan el espectro sin cooperación explícita y con interferencia mínima.

El estándar 802.11 original define velocidades de 1 y 2 Mbps vía ondas de radio usando DSSS; el 802.11b permite hasta 11 Mbps, o hasta el doble la versión 802.11 g, compatible con la anterior. Además, se ha definido la variante IEEE 802.11a (Wireless ATM), incorporado recientemente a la especificación, que permite conseguir 54 Mbps en la banda de 5 GHz, con un ancho de banda de hasta 300 MHz y modulación OFDM, y que evolucionará a la 802.11 e/h.

Nivel de MAC.

La capa de gestión MAC controlará aspectos tales como la sincronización y los algoritmos del DS. El nivel de MAC se compone de dos funcionalidades básicas: la función de coordinación puntual (PCF) y la función de coordinación distribuida (DCF).

De manera genérica, se define la función de coordinación como la funcionalidad que determina, dentro de una BSS, cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo a nivel MAC a través del medio inalámbrico. En el nivel inferior del subnivel MAC se encuentra la función de coordinación distribuida (DCF), y su funcionamiento se basa en técnicas de acceso aleatorias de contienda por el medio. El tráfico que se transmite bajo esta funcionalidad es de carácter asíncrono ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles no tolerados por los servicios síncronos.

Por encima de la funcionalidad DCF se sitúa la función de coordinación puntual, PCF, asociada a las transmisiones libres de contienda que utilizan técnicas de acceso deterministas. El estándar IEEE 802.11, en concreto, define una técnica de encuesta desde el punto de acceso. Esta funcionalidad está pensada para servicios de tipo síncrono que no toleran retardos aleatorios en el acceso al medio. Estos dos métodos de acceso pueden operar conjuntamente dentro de una misma celda o BSS.

Otro aspecto importante en el funcionamiento de la DFC es el conocimiento del medio, muy importante en el algoritmo de contienda. Los nodos saben cuándo la estación que en estos momentos tiene el control del medio, porque está transmitiendo o recibiendo, va a finalizar su período de reserva del canal. Esto se hace a través de una variable llamada NAV (Network Allocation Vector), que mantendrá una predicción de cuándo quedará liberado el medio. Tanto al enviar un RTS como al recibir un CTS, se envía el campo Duración/ID con el valor reservado para la transmisión y el subsiguiente reconocimiento. Las estaciones que estén a la escucha modificarán su NAV según el valor de este campo Duración/ID. En realidad, hay una serie de normas para modificar el NAV. Una de ellas es que el NAV siempre se situará al valor más alto de entre los disponibles.

Las tramas MAC contienen los siguientes componentes básicos: una cabecera MAC que comprende campos de control: duración, direccionamiento y control de secuencia, un cuerpo de trama de longitud variable que contiene información específica del tipo de trama y una secuencia checksum (FCS) que contiene un código de redundancia CRC de 32 bits.

Por otra parte, las tramas MAC se pueden clasificar según tres tipos:

- Tramas de datos.
- Tramas de control (por ejemplo, reconocimientos o ACK, las tramas para multiacceso RTS y CTS y las tramas libres de contienda).
- Tramas de gestión (por ejemplo, el servicio de asociación las tramas de beacon o portadora y las tramas TIM o de tráfico pendiente en el punto de acceso).

A nivel de MAC, un aspecto muy importante es el direccionamiento. El caso más complejo se produce cuando una estación quiere transmitir a otra ubicada en otro BSS. Para resolver cualquier problema de direccionamiento se hace uso del campo bit ToDS/FromDS del campo de control de la trama de MAC. Este campo identifica si la trama se envía o se recibe al/del sistema de distribución. En redes *ad hoc*, tanto ToDS como FromDS están a cero. El caso más complejo contempla el envío entre dos estaciones a través del sistema de distribución. Para ello situamos a uno tanto ToDS como FromDS.

En este caso los campos ToDS=FromDS=1 y las direcciones de cada uno de los componentes por los que pasa la trama toman el siguiente valor en la trama MAC, quedando la dirección 1 como el nodo destino, la dirección 2 será la del punto de acceso final, la dirección 3 sería la del punto de acceso origen y, por último, la dirección 4 será la del nodo origen.

Servicios del DS.

La especificación IEEE 802.11 define el DS como la arquitectura encargada de interconectar diferentes BSS o redes inalámbricas independientes.

El componente fundamental de este sistema de distribución es el punto de acceso, y además, la especificación define lo que llama servicios de distribución. Los cinco primeros los implementa el punto de acceso y los cuatro últimos el nodo.

Estos servicios son:

- Distribución. Se encarga de llevar un paquete del punto de acceso de origen al de destino.
- Integración. Se encarga de la función de pasarela con otros sistemas IEEE802.x. En concreto, define el componente portal que se encargará de aspectos necesarios como el redireccionamiento.

- Asociación. Servicio necesario para que una estación pueda adherirse a una configuración con punto de acceso y utilizar sus servicios.
- Reasociación. Muy similar al anterior, se utiliza para cambiar las características de asociación entre el nodo y el punto de acceso, por ejemplo, durante el roaming.
- Autenticación y desautenticación. Proceso necesario para que la estación se pueda conectar a la WLAN y consiste en la identificación de la estación. El proceso, pues, de conexión pasa por la autenticación previamente a la asociación.
- Privacidad. Este servicio utilizará WEP para el encriptado de los datos en el medio.
- Reparto de MSDU entre STA. Éste es el servicio básico de intercambio.

Roaming.

El roaming es el proceso por el cual un nodo puede desplazarse físicamente de una celda (o BSS) a otra sin pérdida de la conexión. En redes WLAN es muy similar al llevado a cabo en redes de telefonía móvil, aunque presenta dos diferencias principales. En primer lugar, una red LAN está basada en paquetes, por lo que el roaming puede efectuarse en los intervalos de transmisión entre paquetes, a diferencia de lo que ocurre en las redes telefónicas, en las que el roaming se produce durante la conversación. Este hecho facilita notablemente el proceso. Por otra parte, en una red de voz una pérdida temporal de la conexión no afecta a la conversación, mientras que en una red basada en paquetes reduce considerablemente las prestaciones de la red debido a las retransmisiones de información que harán las capas superiores.

El estándar 802.11 no define mecanismos concretos de roaming, pero especifica las herramientas básicas para ello, entre las que se encuentran los servicios de asociación.

Sincronización.

La sincronización de los nodos de la red resulta fundamental para tareas vitales (sincronización de los saltos en frecuencia, control de potencia, etc.). De mantener la sincronización se va a encargar la función de sincronización (TSF, Time Synchronization Function), y su modo de trabajo va a depender de la topología de la red, ya que el tratamiento de la sincronización depende de si la configuración de la red es *ad hoc* o con punto de acceso.

En una configuración con punto de acceso, consiste, básicamente, en que todos los nodos actualicen sus relojes de acuerdo con el reloj del punto de acceso. Periódicamente, el punto de acceso (AP) transmite unas tramas especiales, llamadas tramas de beacon, que contienen el valor del reloj del AP en el momento de la transmisión. El nodo receptor comprueba el valor de su reloj en el momento de la recepción y lo corrige para sincronizarlo con el valor de reloj del AP. Este proceso de obtención puede tener carácter pasivo si la estación espera a recibir la trama de beacon del punto de acceso, o bien ser un proceso activo si la estación trata de encontrar el punto de acceso transmitiendo tramas de prueba y esperando la respuesta del punto de acceso.

En el modo *ad hoc*, el funcionamiento es más complejo. Por una parte, la estación que instancie la red establecerá un intervalo de beacon, esto es, una tasa de transferencia de portadoras que permitan la sincronización. Sin embargo, en este caso, el control está distribuido y entre todos los nodos se intentará mantener la sincronización. Para ello, el nodo estación que no detecte en un determinado tiempo de backoff una trama de beacon enviará una para intentar que no se desincronice la red.

Gestión de potencia.

En WLAN y en todo tipo de redes móviles en general, la batería es un recurso escaso, por lo que debe optimizarse su empleo.

El estándar 802.11 define un funcionamiento en modo limitado de potencia según el cual las estaciones pueden permanecer «dormidas» sin pérdida de información.

La idea básica es que el punto de acceso mantenga una lista de las estaciones que, en un momento dado, se encuentren trabajando en este modo y que almacene los paquetes destinados a dichas estaciones hasta que éstas soliciten el envío de los paquetes que les corresponden o hasta que cambien a un nodo de potencia normal.

Periódicamente, el AP envía, formando parte de la trama de beacon, información sobre las estaciones en modo limitado de potencia de las que tiene almacenados paquetes. Al recibir la trama de beacon, las estaciones deben despertar y, si existiera alguna indicación de que las estaciones tienen algunos paquetes pendientes de recepción, deberán enviar un mensaje solicitando al AP que les sean enviados dichos paquetes. Cuando el punto de acceso decida enviarle el paquete, lo hará enviándole una trama TIM (Traffic Indication Map) a la estación para que despierte en el próximo intervalo de portadora. De esta manera, estas estaciones recibirán la información con un desgaste mínimo de potencia.

Otra posibilidad es que sea el punto de acceso quien despierte a la estación. Esta situación se plantea en la distribución de paquetes multicast o broadcast. En este caso, todas las estaciones destino deberán despertar antes de un tiempo predeterminado.

Seguridad.

Las redes inalámbricas son inseguras aunque sólo sea porque el medio de transporte que emplean es el aire; por tanto, un elemento esencial a tener en cuenta en este tipo de redes al utilizarse la radio es la encriptación.

En general, se utiliza WEP (Wired Equivalent Privacy o protocolo de encriptación inalámbrico), aunque también existen otros mecanismos. Se trata de un sistema de encriptación y autenticación especificado en el estándar IEEE 802.11 para garantizar la seguridad de las comunicaciones entre los usuarios y los puntos de acceso. La clave de acceso estándar es de 40 bits, pero existe otra opcional de 128 bits, y se asigna de forma estática o manual (no dinámica), tanto para los clientes, que comparten todos el mismo conjunto de cuatro claves predeterminadas, como para los puntos de acceso a la red, lo que genera algunas dudas sobre su eficacia. WEP utiliza un esquema de cifrado simétrico en el que la misma clave y algoritmo se utilizan tanto para el cifrado de los datos como para su descifrado.

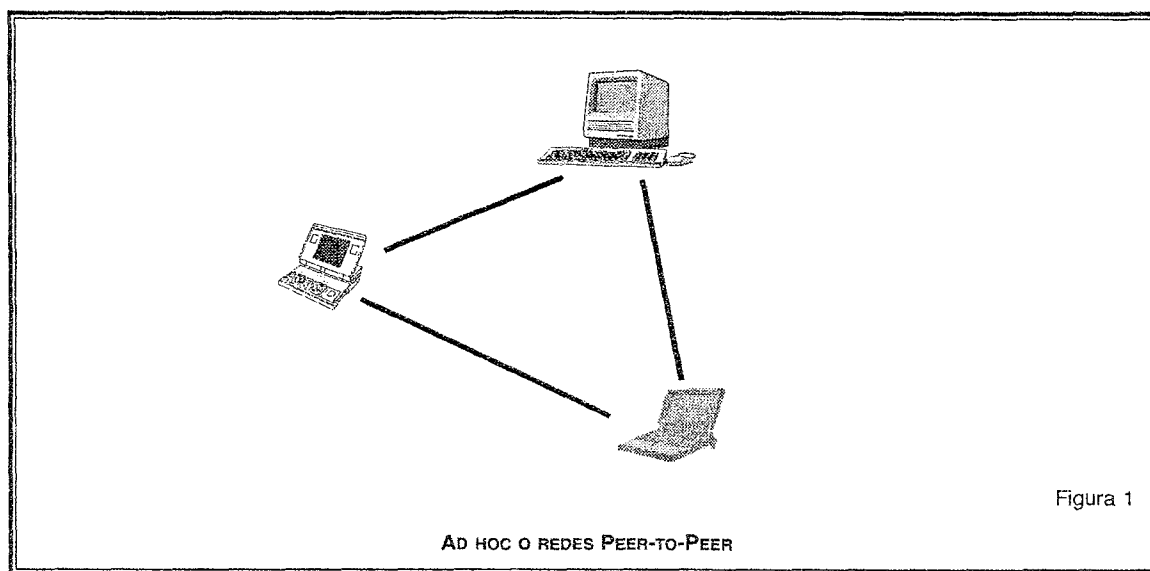
Pero se ha descubierto que WEP no es tan seguro como todo el mundo pensaba. Como parte del estándar Wi-Fi, las redes inalámbricas pueden anunciar (literalmente, transmitir) sus nombres de red, para que sea más fácil encontrarlas y unirse a ellas. Este anuncio se conoce como el identificador (SSID). El primer paso para ofrecer cierta forma de seguridad sería no transmitir este nombre o elegir un nombre que no pudiera ser adivinado con facilidad.

La conclusión de toda esta incertidumbre sobre la seguridad es que se ha convertido muy rápidamente en una preocupación para las empresas cliente que desean desplegar una solución inalámbrica. Para resolver esto en el área de los estándares se formó el subcomité IEEE 802.11i, cuyo objetivo es ofrecer una forma interoperable y estándar de garantizar la seguridad de los datos inalámbricos. Al mismo tiempo, existe cierto número de soluciones propietarias de fabricantes que están dirigidas a resolver este mismo problema.

La seguridad especificada en 802.11i utilizará probablemente alguna forma de encriptación potente, ampliamente aceptada, como AES o algo similar. En el futuro, para que 802.11a sea realmente aceptada como una tecnología inalámbrica para ser utilizada en la empresa, debe incluir 802.11i para ofrecer una capacidad de seguridad potente y basada en estándares.

Hay dos clases de redes inalámbricas:

- a) Una red inalámbrica *ad hoc*, o «peer-to-peer» consiste en un conjunto de ordenadores cada uno equipado con una tarjeta de interfaz inalámbrica de red. Cada ordenador puede comunicarse directamente con todos los demás ordenadores inalámbricos instalados. Pueden compartir archivos e impresoras, pero pueden no tener acceso a recursos alámbricos de la LAN, a menos que uno de los ordenadores actúe como puente a la LAN alámbrica usando un software especial.



Cada ordenador inalámbrico puede comunicarse directamente con los otros.

- b) Una red inalámbrica puede también utilizar un punto de acceso. En este tipo de red el punto de acceso actúa como un cubo, proporcionando conexión a los ordenadores inalámbricos. Puede conectarse a la LAN inalámbrica o con una LAN alámbrica, permitiendo el acceso inalámbrico del ordenador a los recursos de la LAN, como servidores de archivos o a una conexión existente a Internet.

Hay dos tipos de puntos de acceso:

- Puntos de acceso dedicados de hardware (HAP) por ejemplo WaveLAN de Lucent, estación base del aeropuerto de Apple o AviatorPRO de WebGear (véase Cuadro 2). Los puntos de acceso ofrecen un amplio soporte para la mayoría de las características inalámbricas, pero comprueban sus requisitos cuidadosamente.
- Los puntos de acceso del software que funcionan en un ordenador equipado con una tarjeta de interfaz inalámbrica de red igual que la utilizada en una red *ad hoc* o peer-to-peer (véase cuadro 3).

Con el soporte apropiado de la red, los usuarios en la LAN inalámbrica pueden compartir archivos e impresoras de la LAN alámbrica y viceversa.

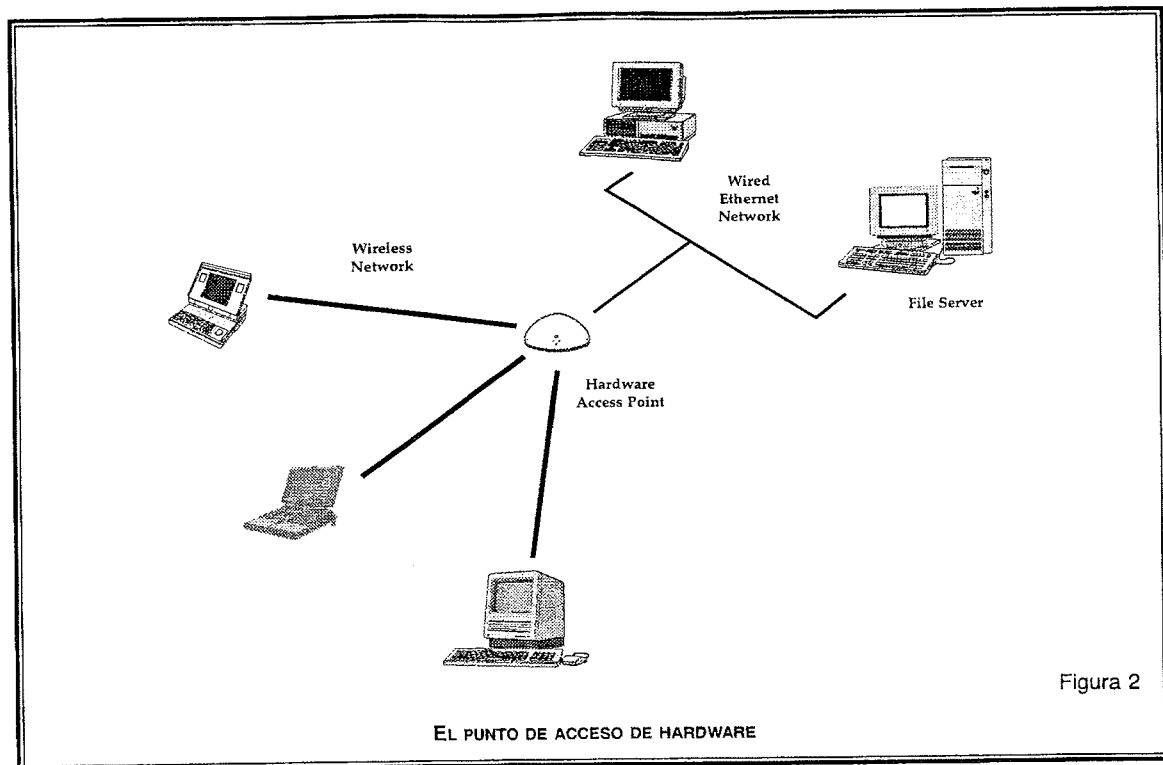


Figura 2

Ordenadores conectados inalámbricamente a través de un punto de acceso de hardware.

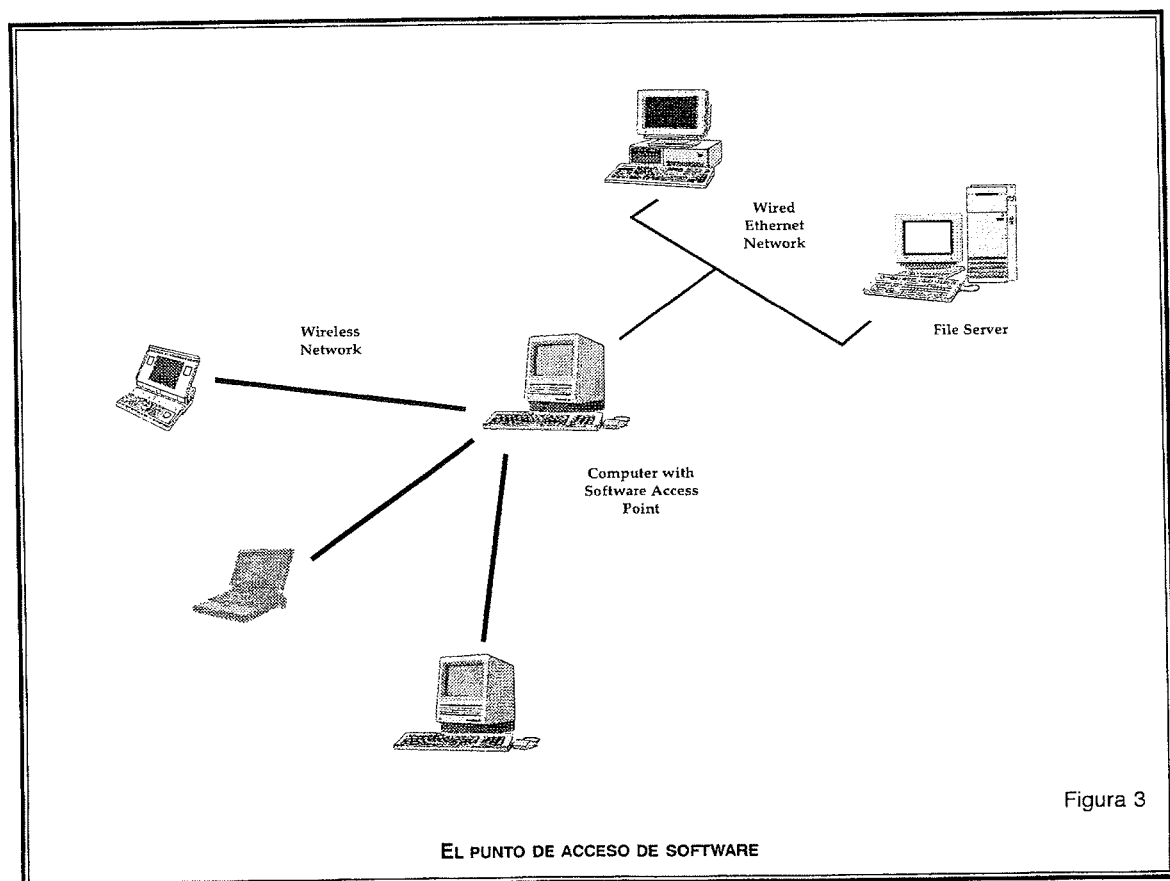


Figura 3

Ordenadores conectados inalámbricamente a través de un punto de acceso de software.

El hardware de red requiere el uso de la tecnología subyacente que se ocupa de las radiofrecuencias así como de la transmisión de datos. El estándar más extendido es 802.11, elaborado por el instituto de ingenieros eléctricos y electrónicos (IEEE). Es un estándar que define todos los aspectos del establecimiento de una red inalámbrica de radiofrecuencia.

Dado que la mayoría de los proveedores de hardware inalámbrico de red se apoyan en el estándar 802.11 es factible el que puedan interoperar entre ellos. El estándar es bastante reciente, y especifica dos métodos para las comunicaciones inalámbricas: Hopping Frequency (FH) y Direct Sequence Spread Spectrum (DSSS o DS), que no son compatibles.

Al comprar el hardware inalámbrico de una red con diferentes proveedores hay que asegurarse de obtener garantías de estos proveedores de su compatibilidad con los estándares. Esperamos que en breve todas las tarjetas inalámbricas nuevas, como las tarjetas de Ethernet, lleguen a ser baratas y compatibles entre sí.

Además merece la pena destacar que la última versión del estándar define una red de 11 mbps y 5.5 mbps, que soporta el antiguo estándar 1 mbps y las velocidades 2 mbps. Esto provee de cierta compatibilidad con diferentes equipos. Observe que este nuevo estándar cubre las redes del tipo DS, no del FH.

Los puntos de acceso del software, tales como InterGate, que utilicen el interfaz inalámbrico del ordenador huésped no deben tener ningún problema de compatibilidad con hardware inalámbrico de un tercero, mientras se sigan los estándares. Normalmente el hardware inalámbrico se identifica al software como interfaz de la red, y por lo tanto se puede utilizar de la misma manera que cualquier otra tarjeta de la red.

Para que un ordenador conectado a una red LAN inalámbrica pueda comunicarse con los ordenadores de otra red LAN alámbrica, se necesitará cierta clase de puente entre la red inalámbrica y la alámbrica. Esto se puede efectuar bien con un punto de acceso del hardware o un punto de acceso del software. Los puntos de acceso del hardware están disponibles en varios tipos de interfaces de la red, tales como Ethernet o token ring, pero casi siempre requieren hardware adicional si sus requisitos de la red cambian.

Si los requisitos de la red son interconectar una red alámbrica a una pequeña red inalámbrica, un punto de acceso del software puede ser la mejor solución.

Un punto de acceso del software no limita el tipo o número de los interfaces de red que utiliza. Puede también proporcionar flexibilidad considerable en el abastecimiento del acceso a diversos tipos de red, redes de Ethernet, de la radio y del token ring. Tal conexión estará solamente limitada por el número de ranuras o interfaces en la computadora que va a realizar esta tarea.

Siguiendo con esto, el punto de acceso del software puede incluir características adicionales significativas tales como acceso compartido a Internet, captación de webs o filtración de contenidos, proporcionando ventajas significativas a usuarios y administradores.

Cada punto de acceso tiene una gama finita dentro de la cual una conexión inalámbrica se puede mantener entre el ordenador del cliente y el punto de acceso. La distancia real varía dependiendo del ambiente;

los fabricantes indican típicamente las gamas de interior y al aire libre para dar una indicación razonable de los límites del funcionamiento. También debe ser observado que al funcionar cerca de los límites, el rendimiento puede caer, pues la calidad de la conexión se deteriora y la red inalámbrica deja de ser operativa.

Las gamas de interior típicas son 150-300 pies, pero pueden ser más cortas si la construcción de edificios interfiere con las transmisiones de radio. Gamas más largas son posibles, pero el funcionamiento se degradará con la distancia.

Las gamas al aire libre llegan hasta 1000 pies, pero depende otra vez del ambiente. Hay maneras de prolongar el rango de operación básico de comunicaciones inalámbricas, usando más de un solo punto de acceso o usando un punto inalámbrico de extensión.

El número de ordenadores que pueden utilizar un solo punto de acceso, depende del fabricante. Algunos puntos de acceso del hardware tienen un límite recomendado de 10, con otros puntos de acceso más costosos soportando hasta 100 conexiones inalámbricas. Usar más ordenadores de los recomendados degradará el funcionamiento y la confiabilidad. Los puntos de acceso del software pueden también imponer limitaciones al usuario, pero éste depende del software específico y de la capacidad del ordenador huésped de procesar la información requerida.

Los puntos de acceso múltiples se pueden conectar con una LAN alámbrica, o incluso una segunda LAN inalámbrica si el punto de acceso lo soporta. En la mayoría de los casos, los puntos de acceso separados se interconectan vía LAN alámbrica, proporcionando conexión inalámbrica en áreas específicas tales como oficinas o aulas, pero están conectados con una LAN alámbrica para el acceso a los recursos de la red, tales como servidores de archivos (véase Cuadro 4).

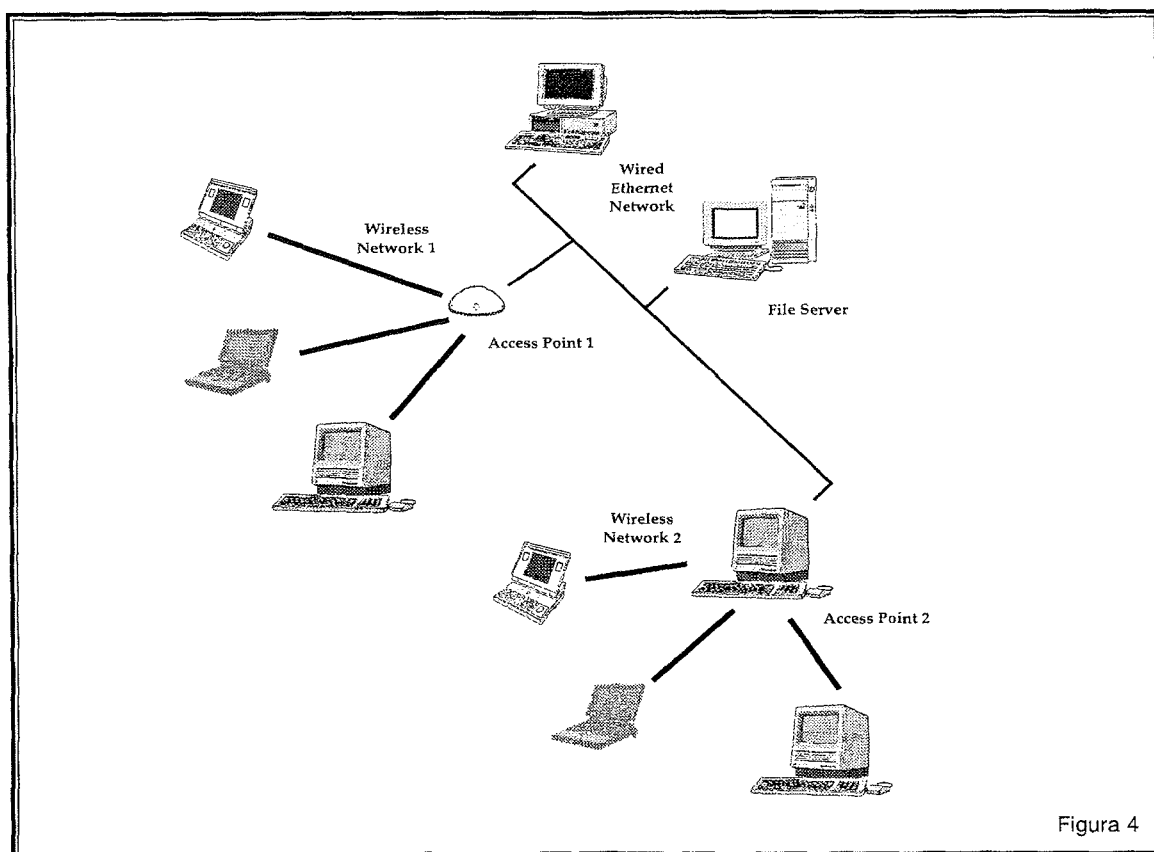
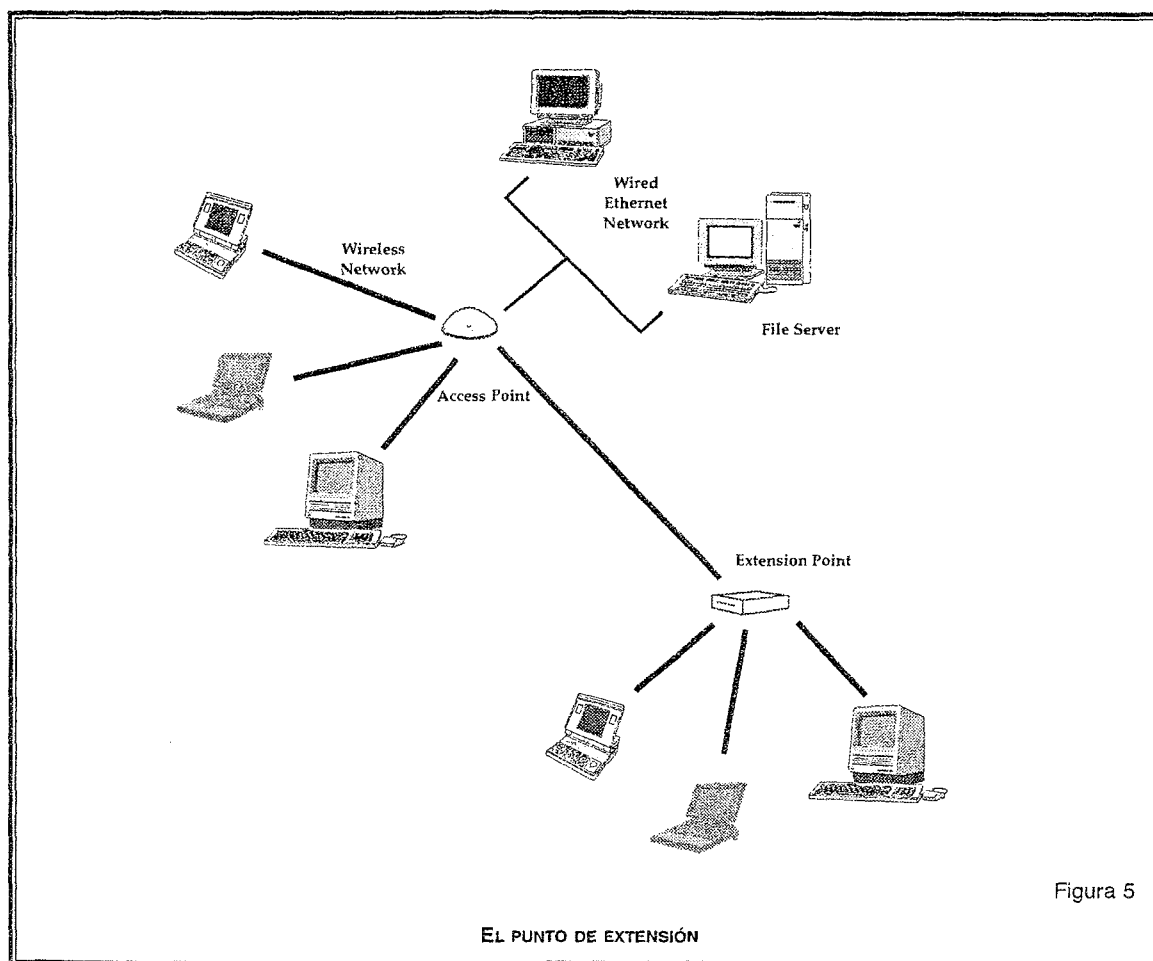


Figura 4

Se conectan varios ordenadores usando múltiples puntos de acceso.

Si una sola área es demasiado grande para ser cubierta por un solo punto de acceso, entonces podemos utilizar los múltiples puntos de acceso o los puntos de extensión. Observe que un «punto de la extensión» no está definido en el estándar inalámbrico, pero han sido diseñados por algunos fabricantes. Al usar puntos de acceso múltiples, cada área inalámbrica del punto de acceso debe solaparse a sus vecinos. Esto proporciona un área sin márgenes para que los usuarios puedan hacer «roaming».

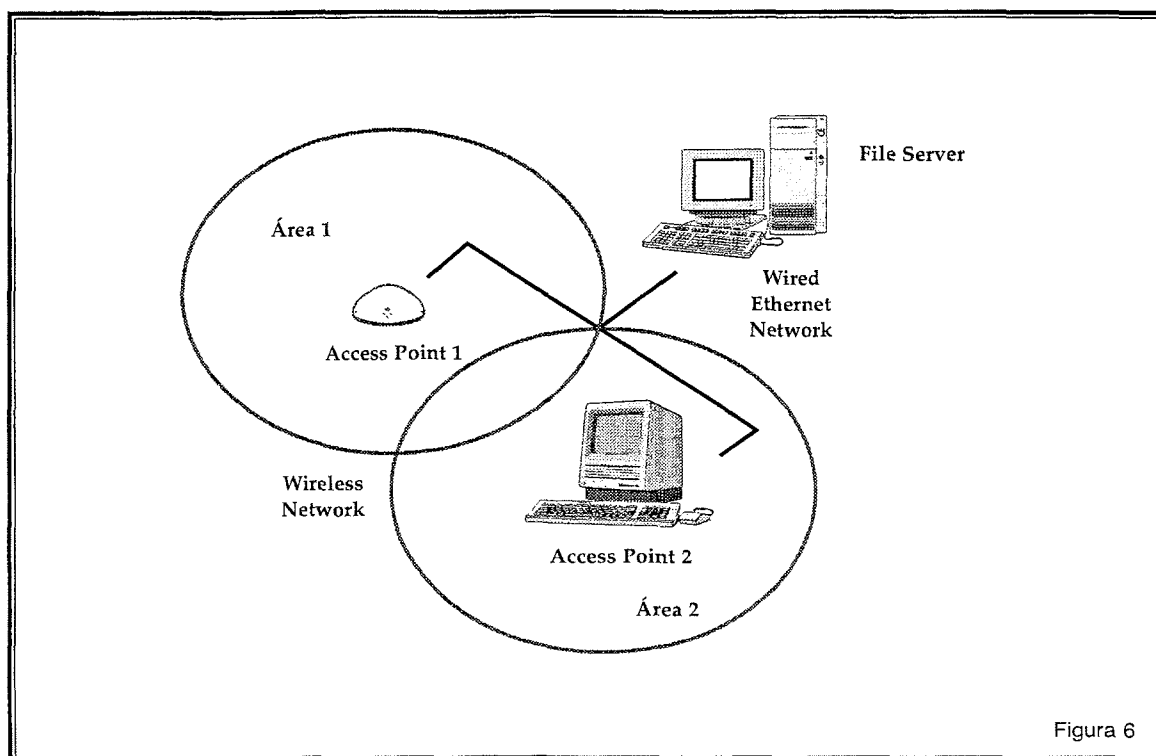
Algunos fabricantes producen puntos de extensión, que actúan como un inalámbrico, prolongando la gama de un solo punto de acceso. Los puntos múltiples de extensión pueden encadenarse juntos para proporcionar el acceso inalámbrico a las localizaciones alejadas del punto de acceso central (véase Cuadro 5).



Se conectan los ordenadores usando un punto de acceso y un punto de extensión.

Un ordenador inalámbrico puede «vagar» (roaming) de un punto de acceso a otro, gracias al software y al hardware, manteniendo una conexión de red constante, supervisando la fuerza de la señal de los puntos de acceso dentro del rango, bloqueándolos en el que mejor calidad tenga. Esto es por regla

general totalmente transparente al usuario; no están enterados que otro punto de acceso se está utilizando al pasar de área a otra área. Algunas configuraciones del punto de acceso requieren la autenticación de la seguridad al intercambiar puntos de acceso, generalmente en la forma de una caja de diálogo de la contraseña. Los puntos de acceso se requieren para tener áreas inalámbricas enlazadas como puede ser visto en el diagrama siguiente:



El usuario puede moverse del área 1 al área 2 de manera transparente. El hardware inalámbrico de red intercambia automáticamente al punto de acceso con la mejor señal.

No todos los puntos de acceso son capaces de ser configurados para roaming. También cabe destacar que deberíamos tratar con un único proveedor para vagar, ya que no hay estándar definido en este caso.

Para poder, con una red inalámbrica interconectar dos LANs se requieren dos puntos de acceso. Cada punto de acceso actúa como un puente que conecta su propio LAN con la conexión inalámbrica. Esta conexión permite que los dos puntos de acceso se comuniquen el uno con el otro y por lo tanto interconecta los dos LANs.

Un punto de acceso inalámbrico del hardware proporciona conexión inalámbrica a ordenadores locales y a un punto de acceso del software. El punto de acceso del software proporciona el acceso alámbrico de los ordenadores de la red de Ethernet 2 a la red alámbrica 1. Observe que no todos los puntos de acceso del hardware tienen la capacidad de interconectar directamente a otro punto de acceso del hardware y que el tema de interconectar las conexiones inalámbricas es complejo y está más allá del alcance de esta introducción.

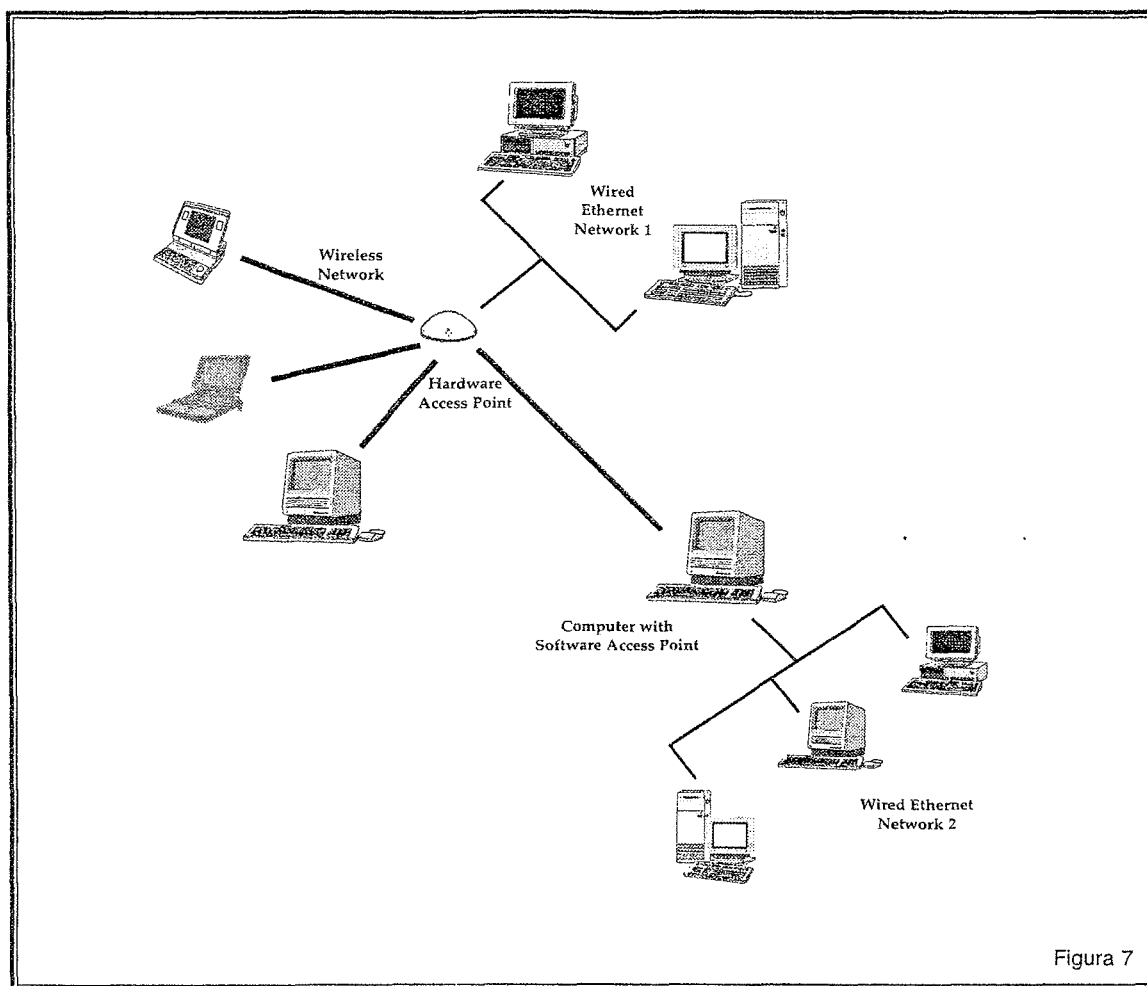


Figura 7

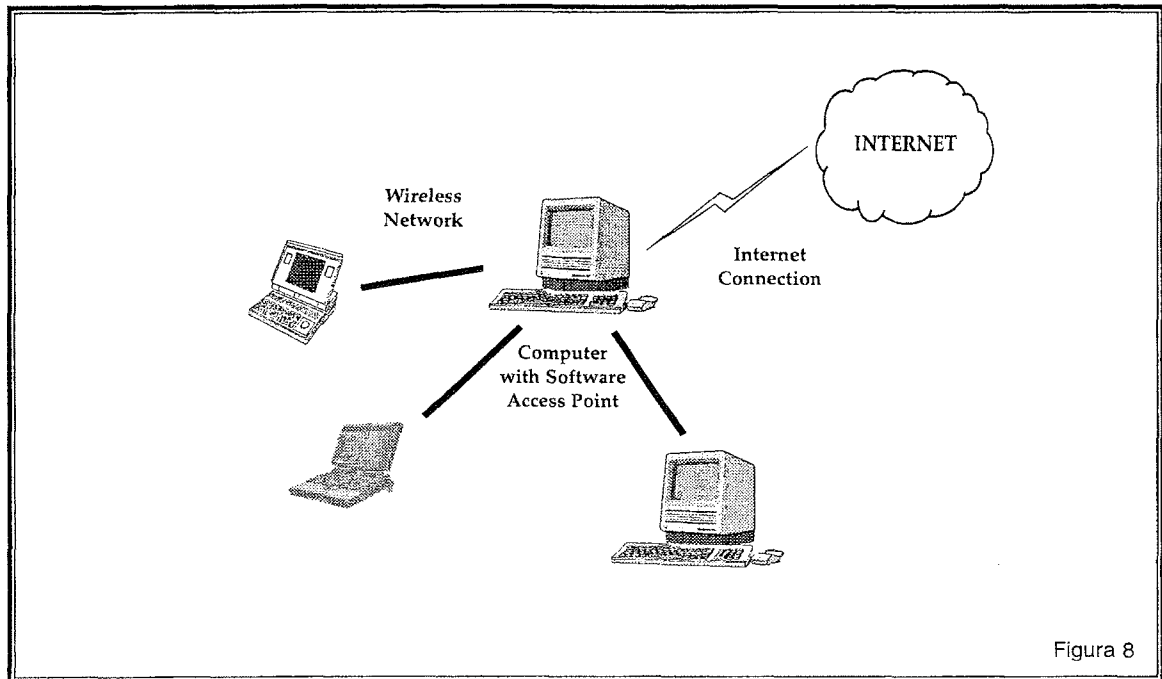
Aunque el establecimiento de una red inalámbrica ofrece ventajas obvias a los usuarios de ordenadores portátiles que se mueven de localización en localización durante el día, también ofrece ventajas para los usuarios de ordenadores fijos de mesa: muchas escuelas y negocios tienen las estructuras civiles o las paredes inadecuadas en el edificio que hacen difícil o imposible construir una red alámbrica. El establecimiento de una red inalámbrica en estos ambientes es una alternativa muy rentable que proporciona una gran flexibilidad. En los casos donde un número pequeño de ordenadores se separa de una red principal, un acoplamiento inalámbrico puede ser más rentable que la red cableada, aunque esto último es perfectamente factible. LANs inalámbricas temporales se pueden crear fácilmente para exposiciones, escuelas o proyectos de negocio, todas sin tirar ningún cable.

Para compartir una conexión a Internet a través de una LAN se necesitan dos cosas:

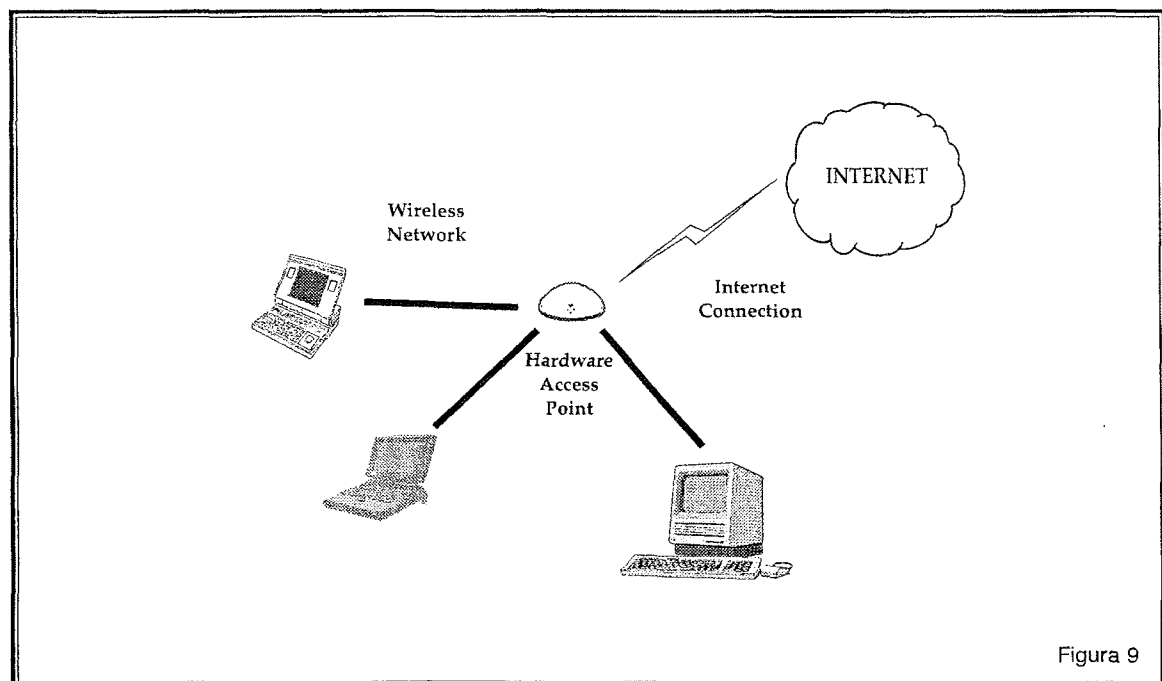
- Un dispositivo de hardware para compartir la conexión a Internet o programa de software.
- Una LAN.

Si su LAN es inalámbrica se aplican los mismos criterios. Se necesita un punto de acceso del hardware o del software y una LAN inalámbrica. Cualquier ordenador equipado de una tarjeta inalámbrica de la red para Internet que comparta apropiadamente el software, puede utilizarse como punto de

acceso del software (véase cuadro 8). Numerosos proveedores ofrecen puntos de acceso del hardware. Un punto de acceso del hardware puede proporcionar capacidad para compartir Internet a los ordenadores de conexión alámbrica LAN, pero no proporciona generalmente mucha flexibilidad más allá de configuraciones muy simples (véase cuadro 9).



El punto de acceso del software inalámbrico conecta los ordenadores usando un punto de acceso del software para el acceso compartiendo a la vez Internet.



El punto de acceso inalámbrico del hardware conecta los ordenadores usando un punto de acceso del hardware para el acceso compartiendo Internet.

Si una LAN conectada con cable tiene ya una conexión a Internet, los puntos de acceso del hardware conectan simplemente con su LAN y permiten que los ordenadores inalámbricos tengan acceso a la conexión existente a Internet de la misma manera que los ordenadores conectados con cable de LAN.

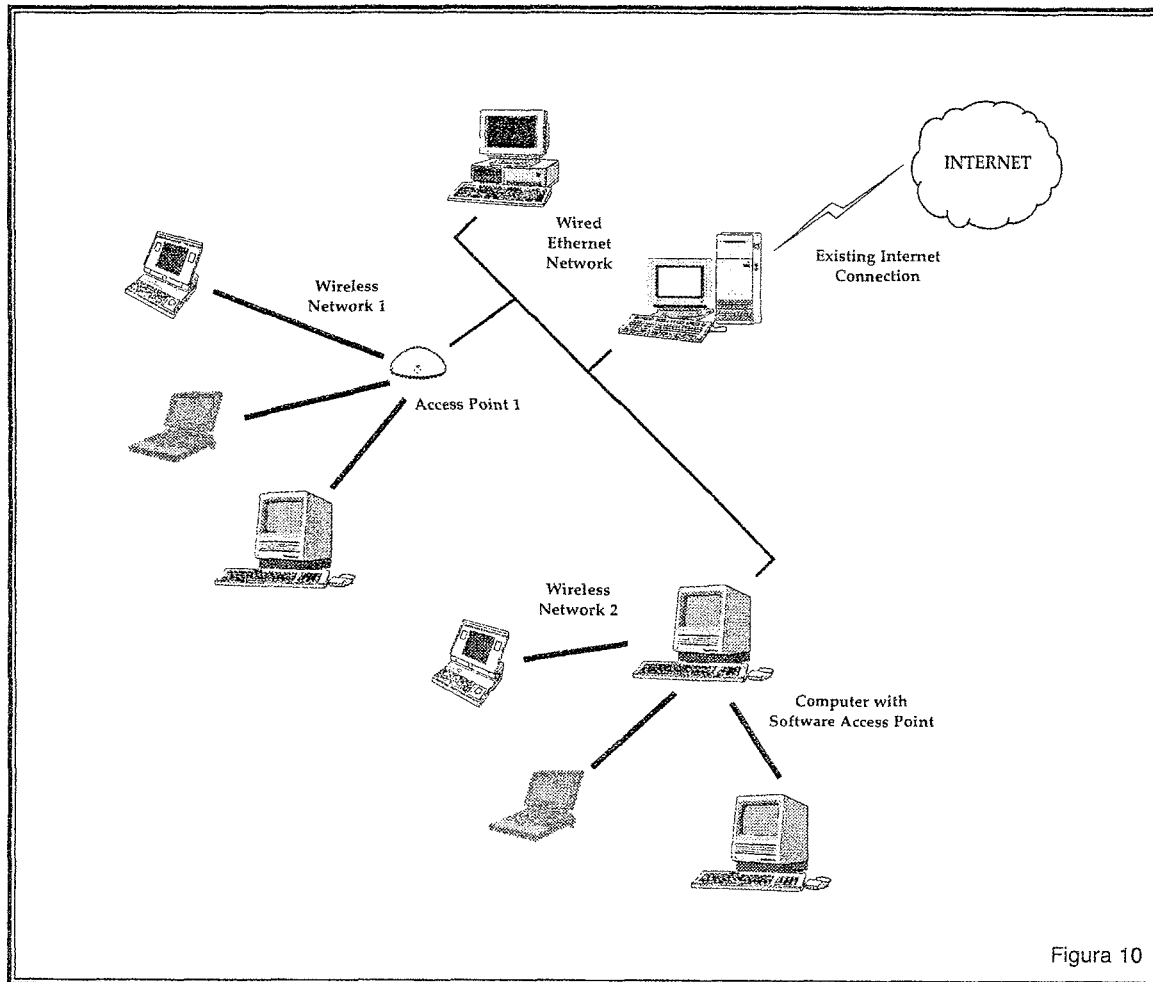


Figura 10

Los puntos de acceso inalámbrico múltiples conectan las computadoras usando puntos de acceso múltiples. Si no hay conexión existente a Internet, entonces éste depende del punto de acceso:

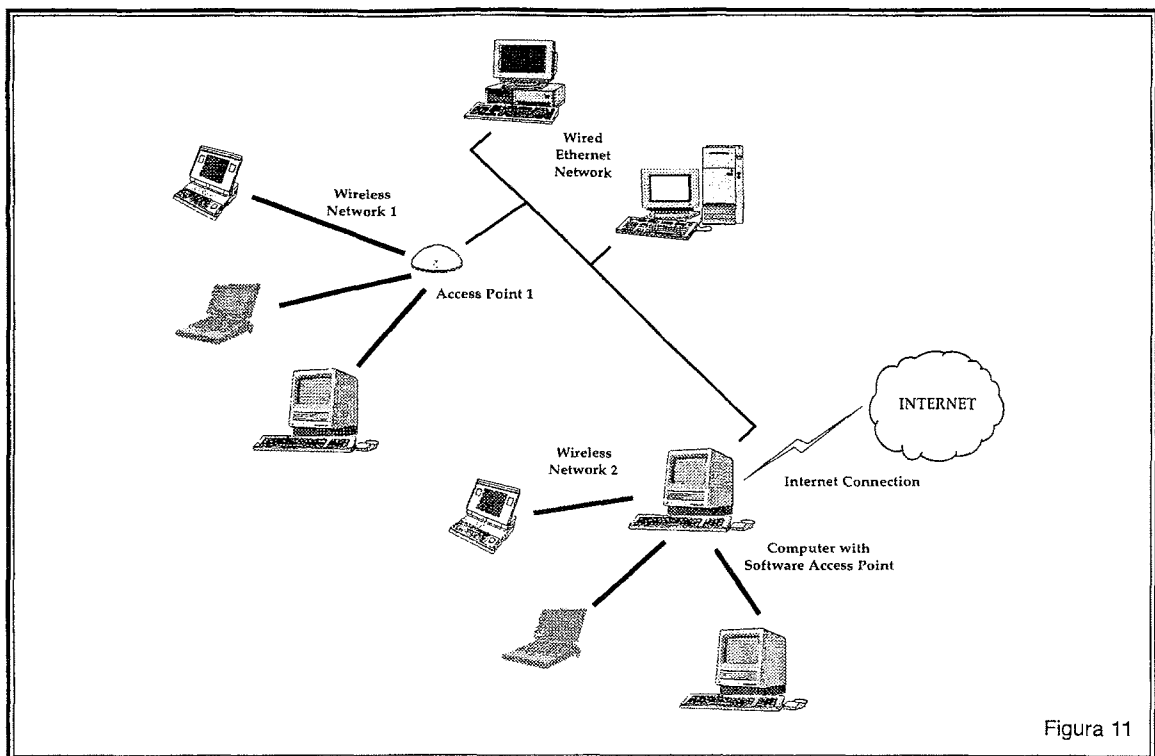


Figura 11

El punto de acceso del software comparte una conexión inalámbrica a Internet

Todos los ordenadores conectados con cable y los inalámbricos tienen acceso a Internet a través de un solo punto de acceso del software. Si un punto de acceso proporciona una conexión de Internet que se comparte, entonces, teniendo conexión múltiple, tales puntos de acceso conectados con una LAN conectada por cable pueden requerir una cierta configuración especial, o pueden requerir posiblemente una conexión a Internet adicional que comparta programa del dispositivo o del software.

Si se utiliza una red inalámbrica para conectarse a Internet, la parte inalámbrica se refiere solamente a su LAN. El puente de comunicaciones de su LAN al proveedor del servicio de Internet (ISP) sería idéntico se tenga o no una red inalámbrica. Por ejemplo, si uno se conecta a una red de Ethernet con Internet vía un módem 56K, cuando se añada una red inalámbrica, se usaría igualmente el mismo módem 56K para conectar a Internet.

Las tarjetas inalámbricas se asemejan a las tarjetas de Ethernet para la red. De hecho, las tarjetas inalámbricas de red tienen direcciones únicas del hardware del MAC que son formateadas como las direcciones del hardware de Ethernet.

3. SEGURIDAD.

Las comunicaciones inalámbricas proporcionan, obviamente, seguridad, pues un intruso no necesita el acceso físico a la red alámbrica tradicional para acceder a las comunicaciones de datos. Sin embargo, a través del estándar 802.11 las comunicaciones inalámbricas no se pueden recibir -descifrar mucho menos- por los exploradores, los receptores de la onda corta, etc. Esto ha conducido a la falsa idea común de que las comunicaciones inalámbricas no se pueden investigar. Sin embargo, es posible investigarlas con un equipo especialista.

Para protegerse contra cualquier problema de seguridad potencial, 802.11 las comunicaciones inalámbricas tienen una función llamada WEP (privacidad equivalente alámbrica), una forma de encriptación que proporciona la privacidad comparable a la de una red alámbrica tradicional. Si la red inalámbrica debe estar segura, debe utilizarse WEP, asegurándose de que los datos se protejan a los mismos niveles que los de una red alámbrica tradicional. También debe tenerse en cuenta que las técnicas virtuales de privacidad tradicional (VPN) trabajan con redes inalámbricas de la misma manera que con las redes alámbricas tradicionales.

4. NORMATIVA REGULADORA. VENTAJAS E INCONVENIENTES.

A) Normativa reguladora.

STANDARD	TASA DATOS	MODULACIÓN	SEGURIDAD	PROS/CONTRAS
IEEE 802.11	Hasta 2 Mbps en 2.4 GHz	FHSS o DSSS	WEP y WPA	Extensión 802.11b
IEEE 802.11a (Wi-Fi)	Hasta 54 Mbps en 5 GHz	OFDM	WEP y WPA	Menos interferencias RF que 802.11b y 802.11g. Mejor 802.11b para multimedia No interopera con 802.11b.
IEEE 802.11b (Wi-Fi)	Hasta 11 Mbps en 2.4 GHz	DSSS con CCK	WEP y WPA	No interopera con 802.11a. Requiere menos access points que 802.11a. 14 canales disponibles en 2.4GHz.
IEEE 802.11g (Wi-Fi)	Hasta 54 Mbps en 5 GHz	OFDM encima 20Mbps, DSSS con CCK debajo 20Mbps	WEP y WPA	Puede reemplazar a la 802.11b. Seguridad mejorada sobre 802.11. Compatible con 802.11b. 14 canales en 2.4GHz
Bluetooth	Hasta 2 Mbps en 2.45 GHz	FHSS	PPTP, SSL o VPN	No soporta TCP/IP. No fue originalmente diseñada para soportar wireless LAN, sí para conectar PDAs, teléfonos y PC a corta distancia.
HomeRF	Hasta 10 Mbps en 2.4 GHz	FHSS		No tiene ya soporte por los proveedores.
HiperLAN/1 (Europe)	Hasta 20 Mbps en 5 GHz	CSMA/CA	Por sesión encriptación y autenticación individual.	HiperLAN es total <i>ad hoc</i> , No garantiza anchura de banda.
HiperLAN/2 (Europe)	Hasta 54 Mbps en 5 GHz	OFDM	Por sesión encriptación y autenticación individual y encriptación.	Diseñada para ATM, IP, Firewire (IEEE 1394) y voz digital. Mejor servicio que HiperLAN/1 y garantiza anchura de banda.

802.11b:

802.11b tiene un alcance de cerca de 50 metros con antenas omnidireccionales low-gain usadas por los dispositivos 802.11b. Su máxima potencia es de 11 Mbit/s, en la práctica alrededor de 5.5 Mbit/s. El metal, el agua y sobre todo los muros espesos absorben las señales 802.11b y decrece el alcance de una manera dramática. Con antenas externas de alta ganancia, este protocolo puede ser utilizado en escenarios punto a punto fijos con un alcance de 8 km, así como hasta 80-120 km en línea que tenga visibilidad directa y puede servir para reemplazar las líneas punto a punto dedicadas o a las costosas líneas de comunicaciones por microondas. La empresa señera en este estándar es Apple Computer con la marca AirPort.

802.11a:

El estándar 802.11a utiliza la banda de los 5 GHz y es capaz de operar a una velocidad bruta de 54 Mbits/s. No ha alcanzado una gran base de utilización debido a que ha privado el estándar 802.11b. En Europa tenemos HIPERLAN que no es interoperable con 802.11b.

802.11g:

El estándar 802.11G utiliza la banda de los 2.4 GHz y es capaz de operar a una velocidad bruta de 54 Mbits/s. Ha alcanzado una gran base de utilización. La empresa señera en este estándar es Apple Computer con la marca AirPortExtreme.

HIPERLAN:

Es un estándar WLAN, una alternativa europea para los estándares IEEE 802.11 (IEEE es América). Está definida por el European Telecommunications Standards Institute (ETSI). En ETSI los estándares son definidos por el proyecto BRAN (Broadband Radio Access Networks).

HIPERLAN/1:

HIPERLAN/1, High PERFORMANCE Radio LAN version 1 es un estándar ETSI. El estándar fue aprobado en 1996. El estándar cubre las partes MAC y física de las capas de enlace (Data Link) como 802.11. Aparece una nueva subcapa conocida como «Channel Access and Control sublayer» (CAC). Esta subcapa se encarga de gestionar los accesos a los canales.

Características:

- Alcance 50m.
- Movilidad lenta (1.4 m/s).
- Soporta tráfico asíncrono y síncrono.
- Sonido 32 kbit/s, 10 ns latencia.
- Video 2 Mbit/s, 100 ns latencia.
- Datos 10 Mbit/s.

HIPERLAN/2:

La especificación fue terminada en febrero de 2000. La versión 2 ha sido diseñada como una conexión rápida inalámbrica para muchos tipos de redes. Son los «backbone» de las redes UMTS, ATM e IP. HIPERLAN/2 utiliza la banda de 5 GHz y con una tasa de 54 Mbit/s de datos. Los servicios básicos son transmisión de datos, sonido y video.

Los datos se aseguran mediante cifrado con los algoritmos DES o 3DES. El punto de acceso y los terminales inalámbrico pueden autenticar uno al otro.

Redes Comunes Inalámbricas.

Las redes comunes inalámbricas permiten enlazar redes de ordenadores mediante las tecnologías inalámbricas, dando lugar así a ciudades enlazadas a través de dichas redes, empleando el estándar 802.11b (Wi-Fi). Además, algunas se utilizan para comunicarse con la red de redes Internet de una manera muy cómoda, algunos participantes tienen o pueden tener una conexión a Internet vía ADSL o módem cable y, enlazándose a estas redes inalámbricas, pueden distribuir los costes de conexión a Internet a cambio de compartir la conexión inalámbrica.

Estos proyectos son, en muchos sentidos, una evolución de la radio amateur y más específicamente de la radio, así como del crecimiento de la comunidad de software libre. Han compartido ambas un espíritu de libertad, experimentación y de adaptación cultural.

El punto clave de esta tecnología es la utilización de antenas de ganancia alta. Los productos comerciales son relativamente caros y no están fácilmente disponibles, por ello estas comunidades han dedicado un gran esfuerzo en la construcción de antenas caseras. Un diseño espectacular «cantenna» que lleva a cabo sus funciones mejor que muchos diseños comerciales.

Muchas de estas comunidades están coordinadas por grupos de usuarios que libremente intercambian información y se ayudan por medio de Internet. A continuación tenemos una lista de direcciones de Internet para estas comunidades inalámbricas.

- COMMUNITY WIRELESS NETWORK, URBANA-CHAMPAIGN: <http://wireless.ucimc.org/>
- WIRELESS WARRIOR: <http://www.wireless-warrior.org/>
- BAWUG, SAN FRANCISCO: <http://www.bawug.org/>
- CONSUME THE NET, LONDON: <http://consume.net/>
- ELEKTROSMOG, STOCKHOLM: <http://elektrosmog.nu/>
- EUROPEOPEN: <http://www.europeopen.net/>
- GUERRILLANET: <http://205.159.169.11/>
- PDX WIRELESS, PORTLAND, OREGON: <http://www.pdxwireless.org/>
- PERSONAL TELCO, PORTLAND, OREGON: <http://www.personaltelco.net/> (wiki)

- SEATTLE WIRELESS: <http://www.seattlewireless.net/> (wiki)
- SFLAN, SAN FRANCISCO: <http://www.sflan.org/>
- SYDNEY WIRELESS, SYDNEY AUSTRALIA: <http://www.sydneywireless.com/>
- WLAN ORG UK, BATH UNITED KINGDOM ORIGINAL: <http://www.wlan.org.uk/>
- BRISTOL WIRELESS, BRISTOL, UK: <http://www.bristolwireless.net/>
- NODEDB FAQ.
- PERSONAL TELCO'S LIST OF WIRELESS COMMUNITIES AT: <http://www.personaltelco.net/index.cgi/WirelessCommunities>
- BUILDING A BUILDING A WIRELESS COMMUNITY NETWORK.
- SAM CHURCHILL'S WIRELESS LAN REVOLUTION.
- METROPOLITAN AREA NETWORK.
- COMPUTER NETWORKS.

Bluetooth es una especificación industrial para PAN inalámbricas, desarrollada inicialmente por Ericsson y posteriormente formalizada por el Bluetooth SIG. El sistema se denomina igual que el rey danés Harald Blåtand, también conocido como Harold Bluetooth. Es un estándar de radio diseñado principalmente para un bajo consumo con un rango o alcance de hasta 10 m. Puede ser utilizado para conectar inalámbricamente periféricos como impresoras, teclados, cámaras digitales o teléfonos móviles al ordenador o PDA.

El protocolo opera en la banda libre de licencia ISM a 2,45 GHz. Alcanza velocidades de 723,3 Kbps de bajada con una subida simultánea de 57,6 Kbps. Para prevenir interferencias con otros protocolos que pudieran utilizar la banda de 2,45 GHz, el protocolo Bluetooth divide la banda en 79 canales y cambia de canal hasta 1.600 veces por segundo.

Cada dispositivo Bluetooth puede mantener simultáneamente hasta 7 conexiones. Cada dispositivo puede ser configurado para anunciar constantemente su presencia a los dispositivos próximos, en orden a establecer una conexión. También se puede proteger por contraseña una conexión entre dos dispositivos, de forma que ningún otro lo pueda escuchar.

Bluetooth puede ser comparado con WiFi, un protocolo más rápido que requiere equipos más caros que cubren mayor distancia y usan el mismo grupo de frecuencias.

Los últimos modelos de móviles a precios accesibles ya cuentan de serie con bluetooth, con lo que se hace un acceso más fácil y sencillo a la red de internet, así como la personalización de las funciones del móvil (con las tecnologías acompañantes previas, como GPRS, MMS, WAP, etc.).

Bluechat es una charla o chat entre dos o más usuarios, donde cada uno utiliza un dispositivo bluetooth (un teléfono móvil GSM o un PDA) y lo nombra con lo que será su alias. El dispositivo se utiliza generalmente en un espacio público y poblado (como un pub, una calle, plaza etc.).

Para comenzar la charla, debe ir al menú conectividad en su dispositivo y encender el puerto bluetooth. Posteriormente, debe buscar (y añadir) nuevos dispositivos bluetooth (sus contertulios). Para enviar un mensaje tiene que ir al programa organizador, crear una nueva nota y enviarla al otro dispositivo/usuario. En todo caso, puede ocultar la visibilidad de su dispositivo y utilizar el vibrador para recibir los mensajes.

Usted puede tener elementos de presentación guardados en una nota de su teléfono móvil (como edad o rango de edad, sexo, orientación sexual, lengua, etc.) formando parte del su alias o (ya que puede ser algo largo) como parte de una nota general de perfil del usuario. También se pueden añadir otros elementos de contacto, como direcciones de e-mail. En algunos establecimientos, se pueden crear bluechat-LANs (por ejemplo en un hotel, hospital, etc.), para una red bluechat más amplia.

B) Ventajas e inconvenientes.

En los últimos años, conforme la tecnología lo permite, este tipo de redes están empezando a gozar de una gran popularidad. Hasta hace poco tiempo, a pesar de llevar varios años en el mercado, no habían terminado de despegar debido a varios factores. En un principio eran soluciones muy verticales, tenían un elevado precio y además ofrecían un ancho de banda muy pequeño, lo que hacía las tecnologías móviles poco adecuadas para la casi totalidad de aplicaciones corporativas. Si, además, a eso unimos la incompatibilidad entre la gran mayoría de los dispositivos del mercado, tendremos los obstáculos con que se han encontrado las tecnologías inalámbricas.

Las ventajas que poseen las WLAN son:

- Flexibilidad. Dentro de la zona de cobertura de la red inalámbrica los nodos se podrán comunicar y no estarán atados a un cable para poder estar comunicados por el mundo.
- Poca planificación. Con respecto a las redes cableadas. Antes de tablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas, mientras que con una red inalámbrica sólo nos tenemos que preocupar de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.
- Diseño. Los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo, etc. También presentan un consumo de energía muy reducido.
- Robustez frente eventos inesperados (tropezón de un usuario con un cable, terremoto, etc.) ante los que una red cableada podría llegar a quedar completamente inutilizada. En estos casos, una red inalámbrica puede aguantar bastante mejor este tipo de percances.

Inconvenientes:

- Calidad de servicio. Las redes inalámbricas ofrecen peor calidad que sus homólogas cableadas. Estamos hablando de velocidades que no superan habitualmente los 10 Mbps, frente a los 100 que puede alcanzar una red convencional. Por otra parte, hay que tener en cuenta también la tasa de error debida a las interferencias. Hay 6 órdenes de magnitud de diferencia (aproximadamente de cada megabit transmitido, 1 kbit será erróneo). Esto puede llegar a ser imposible de implantar en algunos entornos industriales con fuertes campos electromagnéticos y ciertos requisitos de calidad.

- Mayor coste. Aunque, cada vez más, se están abaratando los costes asociados a estas tecnologías, todavía resultan más caras que las redes cableadas en la mayoría de los casos.
- Restricciones. Estas redes requieren de la asignación de una banda dentro del espectro radioeléctrico. Éste está muy saturado hoy día y las redes deben amoldarse a las reglas que existan dentro de cada país.
- Seguridad. En dos vertientes:
 - Por una parte, seguridad e integridad de la información que se transmite. Este campo es bastante criticado en casi todos los estándares actuales que, según dicen, no se debe utilizar en entornos críticos en los que un «robo» de datos pueda ser peligroso.
 - Por otra parte, este tipo de comunicación podría interferir en otras redes de comunicación (policía, bomberos, hospitales, etc.), y esto hay que tenerlo en cuenta en el diseño.



