UNIVERSIDAD DE SOTAVENTO, A.C.

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INFORMÁTICA

"PROPUESTA DE HOTSPOT DE ALTA SEGURIDAD PARA EL HOTEL BEST WESTERN"

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

DANIEL CÓRDOVA OSORIO

ASESOR DE TESIS

LIC. JUAN JOSÉ GUTIERREZ QUIROZ

COATZACOALCOS, VER. ABRIL 2007

ESTRUCTURA DE LA TESIS

El desarrollo del hombre desde el nivel físico de su evolución, pasando por su crecimiento en las áreas sociales y científicas hasta llegar a la era moderna se ha visto apoyado por herramientas que extendieron su funcionalidad y poder como ser viviente.

Sintiéndose conciente de su habilidad creativa, metódicamente elaboró procedimientos para organizar su conocimiento, sus recursos y manipular su entorno para su comodidad, impulsando las ciencias y mejorando su nivel de vida a costa de sacrificar el desarrollo natural de su ambiente, produciendo así todos los adelantos que un gran sector de la población conoce: automóviles, aeroplanos, trasatlánticos, teléfonos, televisiones, etc.

En el transcurso de todo este desarrollo, también evolucionó dentro del sector tecnológico el cómputo electrónico. Este nació con los primeros ordenadores en la década de los años 40, porque la necesidad del momento era extender la rapidez del cerebro humano para realizar algunos cálculos aritméticos y procedimientos repetitivos.

Este esfuerzo para continuar avanzando, se reflejó en crear unidades de procesamiento cada vez más veloces, divididas en cuatro generaciones bien definidas: la primera con tubos al vacío, la segunda con transistores, la tercera con circuitos integrados y la cuarta con circuitos integrados que permitieron el uso de computadoras personales y el desarrollo de las redes de datos.

Este último elemento, las redes de ordenadores, consisten en "compartir recursos", y uno de sus objetivos principales es hacer que todos los programas, datos y hasta los propios equipos estén disponibles para cualquier usuario que así lo solicite, sin importar la localización física del recurso y del propio usuario.

En el desarrollo de la tesis que continuación presento nos enfocaremos a la nueva era de la comunicación sin cables y a los recursos compartidos igualmente inalámbricos con sus beneficios y sus problemas... pues a toda acción encontraremos una reacción tomando esta frase de las ciencias físicas y aplicándolas siempre a cualquier acontecimiento

A continuación se expone precisamente una de las necesidades básicas del ser humano hoy en día....y es la comunicación constante y deseable desde cualquier rincón del planeta, olvidando las distancias y solicitando lo placentero de la comodidad, desde tu casa, tu trabajo y en este caso que expongo...desde la habitación del hotel de tu preferencia.

En este mismo escrito puntualizo sobre los problemas de seguridad que siempre existirán en un servicio "público" o "abierto" como han de referirse los

expertos en computación y algunas medidas que he tomado para minimizar los mismos.

En el **Capítulo 1** se encuentra la Introducción del tema, donde se describen los antecedentes de los problemas en cuanto a la seguridad de la información refiere.

En el **Capítulo 2** se realiza el planteamiento del problema, comprendiendo la justificación, hipótesis y objetivos presentes del trabajo, incluyendo posteriormente mi investigación teórica y mi propuesta práctica

En el **Capítulo 3** hago un repaso o referencia a conocimientos teóricos que se deben obtener y comprender antes de continuar con la lectura del presente escrito, pues es necesario conocer los fundamentos y bases de la computación y redes informáticas para entender mi propuesta.

En el **Capítulo 4** se expone el desarrollo y la implementación de la seguridad vía software y hardware así como una descripción de cada proceso realizado, desde la instalación de la red, hasta la configuración del ruteador ayudándome de ilustraciones varias.

En el **Capítulo 5** anuncio algunas recomendaciones para mantener una red inalámbrica segura hasta donde es posible así como mi conclusión de este trabajo.

En términos generales lo que presento con este trabajo es una alternativa para el mejoramiento del Internet compartido en cuanto a seguridad refiere, tratar de generar conciencia al usuario a tomar medidas de seguridad cuando utiliza espacios públicos y principalmente cambiar la mentalidad de los empresarios en cuanto a la informática en general, al hacerles notar que los equipos o el área de sistemas debe ser un recurso en el que siempre se ha de invertir y capacitar para no presentar incomodidades que a la larga les generará altos costos.

Con afecto y respeto:

Para mis maestros que con sus enseñanzas e instrucciones me guiaron por el camino del conocimiento.

A mi familia, mi madre y mi hermano que me motivaron muy a su estilo y he tomado como ejemplo de superación.

A todos los que estuvieron en mi trayecto escolar, desde la educación básica hasta la universitaria, gracias por ser parte de mi historia y a los que siguen ahí...gracias por seguir acompañándome.

ÍNDICE

ESTRUCTURA DE LA TESIS

CAPÍTULO 1 INTRODUCCIÓN

CAPÍTULO 2 PLANTEAMIENTO DEL PROBLEMA
2.1 JUSTIFICACIÓN
2.2 HIPÓTESIS
2.3 OBJETIVO GENERAL
2.4 OBJETIVOS ESPECÍFICOS

CAPÍTULO 3 MARCO TEÓRICO
3.1 ANTECEDENTES
3.2 REDES INFORMÁTICAS
- 3.2.1 CARACTERÍSITICAS DE UNA RED LOCAL
- 3.2.2 MEDIOS DE TRANSMISIÓN
- 3.2.3 TOPOLOGÍA
- 3.2.4 MÉTODOS DE ACCESO
- 3.2.5 DATAGRAMAS
- 3.2.6 PROTOCOLOS
- 3.2.7 ROUTER, BRIDGE Y REPEATER

3.3 INTERNET
- 3.3.1 CLIENTES Y SERVIDORES
- 3.3.2 CÓMO SE TRANSMITE LA INFORMACIÓN EN INTERNET
- 3.3.3 PROTOCOLO TCP/IP Y PAQUETES DE INFORMACIÓN
- 3.3.4 EL SISTEMA DE NOMBRES POR DOMINIO
  - 3.3.4.1 EL NOMBRE DE LOS ORDENADORES EN INTERNET
  - 3.3.4.2. DOMINIOS DE PRIMER NIVEL
  - 3.3.4.3 DETERMINACIÓN DEL No IP A PARTIR DEL NOMBRE

3.4 REDES INALÁMBRICAS
- 3.4.1 TOPOLOGÍAS DE REDES INALÁMBRICAS LAN
- 3.4.2 SEGURIDAD
- 3.4.3 AUTENTICACIÓN DE PUNTOS DE ACCESO Y DE LOS USUARIOS
- 3.4.4 IEEE 802.11
- 3.4.5 SEGURIDAD 802.1X
- 3.4.6 ROMPIENDO CANDADOS
- 3.4.7 AUTENTICACIÓN

CAPÍTULO 4 IMPLEMENTACIÓN DE LA RED
4.1 PLANEACIÓN
4.2 DISEÑO
4.3 INSTALACIÓN
- 4.3.1 PROBANDO LA CALIDAD DE LA CONEXIÓN
- 4.3.2 MONTANDO LA RED

4.4 CONFIGURACIÓN
- 4.4.1 TARJETA DE RED
- 4.4.2 PUNTOS DE ACCESO
  - 4.4.2.1 CREAR INTERCONEXIÓN WDS
- 4.4.3 HOTSPOT

CAPÍTULO 5 CONCLUSIONES Y RECOMENDACIONES
5.1 RECOMENDACIONES
5.2 CONCLUSIÓN

GLOSARIO

BIBLIOGRAFÍA

ÍNDICE DE IMÁGENES

MARCO TEÓRICO

FIGURA 3.1 CAPACIDAD DEL MEDIO: ANCHO DE BANDA

IMPLEMENTACIÓN DE LA RED

FIGURA 4.1 INSTALACIONES GENERALES DEL BEST WESTERN
FIGURA 4.2 COLOCACIÓN DE DISPOSITIVOS
FIGURA 4.3 ANTENA PRINCIPAL
FIGURA 4.4 ANTENAS LATERALES
FIGURA 4.5 PUNTO DE ACCESO DE PASILLO
FIGURA 4.6 DISPOSITOVOS EN RECEPCIÓN (SITE)
FIGURA 4.7 WDS
FIGURA 4.8 PROPIEDADES TCP/IP
FIGURA 4.9 REDES INALÁMBRICAS DISPONIBLES
FIGURA 4.10 ENCRIPTACIÓN WEP EN NIC 1
FIGURA 4.11 ENCRIPTACIÓN WEP EN NIC 2
FIGURA 4.12 ENCRIPTACIÓN WEP EN NIC 3
FIGURA 4.13 CONFIGURACIÓN DE RED DE PUNTO DE ACCESO
FIGURA 4.14 CONFIGURACIÓN DE WIRELESS DE PUNTO DE ACCESO
FIGURA 4.15 CONFIGURACIÓN DE SEGURIDAD DE PUNTO DE ACCESO
FIGURA 4.16 CONFIGURACIÓN DE WIRELESS WDS
FIGURA 4.17 DIRECCIÓN IP DE PUNTOS DE ACCESO
FIGURA 4.18 PANTALLA DE INICIO DE HOTSPOT
FIGURA 4.19 PANTALLA DE STATUS DE HOTSPOT
FIGURA 4.20 PANTALLA DE CONFIGURACIÓN DE AUTENTICIDAD
FIGURA 4.21 PANTALLA DE RADIUS
FIGURA 4.22 PANTALLA DE CONFIGURACIÓN DE TEXTO BIENVENIDA
FIGURA 4.23 PANTALLA DE CONFIGURACIÓN DE TICKET
FIGURA 4.24 PANTALLA DE FIREWALL Y FILTROS
FIGURA 4.25 PANTALLA DE BIENVENIDA EN EXPLORADOR DE INTERNET
FIGURA 4.26 VENTANA DE AVISO EN CONEXIÓN EXITOSA

CAPÍTULO 1

INTRODUCCIÓN

La falta de políticas y procedimientos en seguridad es uno de los problemas más graves que confrontan las empresas hoy día en lo que se refiere a la protección de sus activos de información frente a peligros externos e internos. La políticas de seguridad son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, detección de intrusos, etcétera…

Si bien las políticas varían considerablemente según el tipo de organización de que se trate, en general incluyen declaraciones generales sobre metas, objetivos, comportamiento y responsabilidades de los empleados en relación a las violaciones de seguridad. A menudo las políticas van acompañadas de normas y procedimientos.

Las políticas son obligatorias, mientras que las recomendaciones o directrices son más bien opcionales. De hecho, las declaraciones de políticas de seguridad pueden transformarse fácilmente y de forma equivocada en recomendaciones reemplazando la palabra "debe" con la palabra "debería".

Por otro lado las políticas son de jerarquía superior a las normas, estándares y procedimientos que también requieren ser acatados. Las políticas consisten de declaraciones genéricas, mientras las normas hacen referencia específica a tecnologías, metodologías, procedimientos de implementación y otros aspectos en detalle. Además las políticas deberían durar durante muchos años, mientras que las normas y procedimientos duran menos tiempo.

Las normas y procedimientos necesitan ser actualizadas más a menudo que las políticas porque hoy día cambian muy rápidamente las tecnologías informáticas, las estructuras organizativas, los procesos de negocios y los procedimientos. Por ejemplo, una norma de seguridad de cifrado podría especificar el uso del estándar DES (Data Encryption Standard). Esta norma probablemente deberá será revisada o reemplazada en los próximos años.

Las políticas son distintas y de un nivel superior a los procedimientos, que son los pasos operacionales específicos que deben llevarse a cabo para lograr una cierta meta. Como ejemplo, hay procedimientos específicos para realizar copias de seguridad de la información contenida en los discos duros de los servidores.

Una declaración sobre políticas describe sólo la forma general de manejar un problema específico, pero no debe ser demasiado detallada o extensa, en cuyo caso es casi seguro que terminaría o se convertiría en un procedimiento.

Las políticas también son diferentes de las medidas de seguridad o de los mecanismos de control. Un ejemplo de esto último sería un sistema de cifrado para las comunicaciones o para los datos confidenciales guardados en discos y cintas. En muchos casos las políticas definen metas u objetivos generales que posteriormente se alcanzan gracias o, por medio de medidas de seguridad.

En general, las políticas definen las áreas sobre las cuales debe enfocarse la atención en lo que concierne a la seguridad. Las políticas podrían dictar que todo el software desarrollado o adquirido se pruebe a fondo antes de utilizarse. Se necesitará tomar en cuenta varios detalles sobre cómo aplicar esta política. Por ejemplo, la metodología que irrefutablemente se usará para probar el software.

Un documento sobre políticas de seguridad contiene, entre muchos aspectos: definición de seguridad para los activos de información, responsabilidades, planes de contingencia, gestión de contraseñas, sistema de control de acceso, respaldo de datos, manejo de virus e intrusos. También puede incluir la forma de comprobar el cumplimiento y las eventuales medidas disciplinarias.

Una empresa necesita de documentación sobre políticas, definiciones de responsabilidades, directrices, normas y procedimientos para que se apliquen las medidas de seguridad, los mecanismos de evaluación de riesgos y el plan de seguridad. Las políticas y una estimación preliminar de los riesgos son el punto de partida para establecer una infraestructura organizativa apropiada, es decir, son los aspectos esenciales desde donde se derivan los demás.

Internet y el desarrollo de las tecnologías de la información y la comunicación suponen una nueva frontera. El paradigma social del futuro próximo en los países desarrollados está construyéndose a partir de: una ciudadanía conectada, la información y el conocimiento como base del valor en la producción y en los servicios; la dependencia estrecha de la red de la organización de los servicios públicos esenciales, y una organización del trabajo ajena a los modos de producción industrial vigentes a lo largo del siglo pasado.

La integridad de la red y de la información, el buen funcionamiento de los sistemas operativos, la preservación de la confidencialidad de las comunicaciones y de los datos, corporativos y comerciales, la seguridad física, jurídica y mercantil, son ya, y lo serán cada vez más, elementos fundamentales para el desarrollo de la Sociedad de la Información.

La magnitud de los riesgos no se compadece con la escasa percepción que de los mismos tienen los usuarios habitualmente. La cultura de la seguridad está lejos de alcanzar la extensión que sería necesaria, sobre todo para facilitar la financiación de dispositivos costosos y de medidas que requieren pautas de comportamiento generalizadas. Los costes de actuaciones como la interceptación de comunicaciones, el acceso no autorizado a ordenadores o redes, la saturación malintencionada de las mismas o los ataques a los servidores de nombres de dominio se multiplican enormemente con la interconexión creciente de las redes. La generalización de redes domésticas, soporte de funciones autoorganizadas de cuya integridad dependerán decisiones "delegadas" por el usuario pueden multiplicar en el futuro la vulnerabilidad del entorno individual si no se adoptan comportamientos y medidas de seguridad.

Al desinterés general por la seguridad contribuyen otros factores: los costes de los dispositivos, una vigencia en ocasiones impredecible debida a la rapidez de los cambios tecnológicos, la todavía precaria articulación de mecanismos jurídicos, así como la vulnerabilidad inevitable que para los usuarios comprometidos con la seguridad supone el descuido de la gran mayoría.

La cooperación para la seguridad y la intervención pública son imprescindibles. Ya hoy los operadores y los proveedores de servicios se ven obligados a garantizar determinados niveles de seguridad en materia de protección de datos y de confidencialidad de las telecomunicaciones sobre la base de criterios comunes para todo el país. En el futuro, la necesidad de reunir una masa crítica suficiente para, entre otras cosas, garantizar la financiación de dispositivos y de medidas de seguridad costosos, así como de prevenir distorsiones en los mercados mundiales de servicios y de telecomunicaciones, cada vez más integrados, exigirán de México la adopción de políticas comunes de seguridad en la red, así como la difusión entre los ciudadanos mexicanos de una cultura de la responsabilidad individual en las telecomunicaciones.

La seguridad ha sido el principal concerniente a tratar cuando una organización desea conectar su red privada al Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el numero de usuarios de redes privadas por la demanda del acceso a los servicios de Internet tal es el caso del World Wide Web (WWW), Internet Mail (e-mail), Telnet, y File Transfer Protocol (FTP). Adicionalmente los corporativos buscan las ventajas que ofrecen las paginas en el WWW y los servidores FTP de acceso publico en el Internet.

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de sus red a los Expertos de Internet (Internet *Crakers*). Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de la información. Todavía, aun si una organización no esta conectada al Internet, esta debería establecer una política de

seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta.

Hoy en día, las Wireless Lan se están convirtiendo poco a poco en partes esenciales de las redes LAN tradicionales pues proveen mayor movilidad para los usuarios, bajos costos de instalación, así como grandes agujeros en la seguridad de la red. Por esa razón, si las Wireless LANs (WLANs) no están implementadas de una manera eficiente los datos sensibles o confidenciales en los sistemas pueden quedar comprometidos.

Misión

Ante la situación en la que nos encontramos; en un mundo con comunicaciones abiertas y con un exceso de información no siempre de calidad, presto mis servicios profesionales de Informática para dar complemento a las necesidades que presenta el Hotel Best Western en cuanto a la seguridad de la información de sus empleados y huéspedes vía Internet.

CAPÍTULO 2

PLANTEAMIENTO DEL PROBLEMA

2.1 JUSTIFICACIÓN
2.2 HIPÓTESIS
2.3 OBJETIVO GENERAL
2.4 OBJETIVOS ESPECÍFICOS

El Hotel Best Western mundialmente es uno de los más prestigiosos desde hace muchos años y actualmente podemos encontrar una filial del mismo ubicado en el inicio de la avenida principal de Coatzacoalcos. Es el primer hotel dentro de la ciudad. Su ubicación permite el fácil acceso a los puntos más importantes de la ciudad como son: El Centro Comercial, Oficinas Estatales y Federales, Complejos Industriales, etc.

La ubicación del hotel permite a sus huéspedes, tanto que viajan en automóvil como los que se trasladan por otros medios, un fácil acceso a los sitios de interés de la ciudad. Sobre la misma avenida se llega al centro de la ciudad donde está ubicada la Catedral de San José, el parque principal, el Palacio Municipal, importantes casas comerciales y el Malecón de la rivera del Río Coatzacoalcos.

Las habitaciones cubren las exigencias del cliente que siempre busca la comodidad cuando viaja con la familia o por cuestiones laborales, ofreciendo el hotel diferentes opciones en cuanto a precio y espacios, pero siempre garantizando la calidad en el servicio y la satisfacción del visitante. Toma también en cuenta el aspecto de los negocios así como el de recreación invitando no sólo a conocer su alberca, bar y restaurante, pues ofrece dos salones que siempre han cumplido con las expectativas para los negocios.

2.1 Justificación

Actualmente el hotel sólo ofrece la posibilidad de conexión a Internet por módem en cada habitación habilitando o dejando accesible una roseta telefónica y cobrando la llamada correspondiente al hacer el marcado. Desafortunadamente la velocidad de envío y recepción de paquetes por este medio es desesperadamente lenta e inestable, además de ser incómoda y poco práctica, nada comparable con una conexión inalámbrica.

El sistema actual del máximo proveedor de Internet en el país ofrece un Internet compartido con escasas medidas de seguridad que una persona con conocimientos moderados de computación puede penetrar con presumible facilidad, alarmante la transmisión de datos de forma inalámbrica es todavía más indefensa y el Hotel Best Western por política de mejora a la calidad ha decidido implementar este servicio en sus habitaciones para la comodidad de sus clientes

Es por esto que el Hotel Best Western ha requerido los servicios de Internet inalámbrico de alta velocidad solicitando también la seguridad de la información de sus clientes y deseando únicamente que ellos tengan acceso a estos recursos y

que nadie en el radio de transmisión de ondas de la señal de Internet pueda robar los servicios que la empresa ofrece únicamente a sus clientes.

2.2 Hipótesis

Como profesionista activo, egresado de la faculta de Informática y como usuario constante del Internet y su opción inalámbrica me ha surgido la inquietud en cuanto seguridad de la información se refiere y he leído múltiples publicaciones de lo más interesantes. Teniendo esta oportunidad a la mano con una empresa con la que ya tengo una relación laboral de antecedente he decidido aportar y aplicar la teoría y conocimientos adoptados con la siguiente hipótesis:

"La instalación de una red inalámbrica con encriptación de datos protegerá la confidencialidad de los datos del usuario o hará al menos más difícil la labor de la piratería al restringir el uso del Internet únicamente a los clientes del hotel". Además de hacer más cómoda la estancia y más práctico el uso del Internet de esta manera y sin necesidad de cables y del módem.

2.3 Objetivo General

"La implementación de una red inalámbrica para uso múltiple de los clientes del hotel Best Western que proteja la integridad de sus información/datos y que sea exclusiva para ellos, así mismo llevar el control de las sesiones en curso, dejando la decisión libre del empresario si se cobrará por el uso de este servicio o será gratuito mediante la administración de ticket para ello"

2.4 Objetivos específicos

- Presentar las deficiencias que se encuentran en el servicio de Internet que actualmente ofrecen.

- Describir las características y ventajas que ofrece una red inalámbrica bien instalada y con altas medidas de seguridad y restricciones.

- Efectuar el análisis correspondiente de las Infraestructura del hotel para la instalación de antenas y puntos de acceso, buscando siempre que la señal sea adecuada y adaptándose a la arquitectura de la empresa.

- Instalar el quipo necesario para la amplificación de señal en el hotel así como la configuración de los módems y la puerta de enlace que hará función de Hotspot.

CAPÍTULO 3

MARCO TEÓRICO

3.1 ANTECEDENTES
3.2 REDES INFORMÁTICAS
- 3.2.1 CARACTERÍSITICAS DE UNA RED LOCAL
- 3.2.2 MEDIOS DE TRANSMISIÓN
- 3.2.3 TOPOLOGÍA
- 3.2.4 MÉTODOS DE ACCESO
- 3.2.5 DATAGRAMAS
- 3.2.6 PROTOCOLOS
- 3.2.7 ROUTER, BRIDGE Y REPEATER

3.3 INTERNET
- 3.3.1 CLIENTES Y SERVIDORES
- 3.3.2 CÓMO SE TRANSMITE LA INFORMACIÓN EN INTERNET
- 3.3.3 PROTOCOLO TCP/IP Y PAQUETES DE INFORMACIÓN
- 3.3.4 EL SISTEMA DE NOMBRES POR DOMINIO
  - 3.3.4.1 EL NOMBRE DE LOS ORDENADORES EN INTERNET
  - 3.3.4.2. DOMINIOS DE PRIMER NIVEL
  - 3.3.4.3 DETERMINACIÓN DEL NÚMERO IP A PARTIR DEL NOMBRE

3.4 REDES INALÁMBRICAS
- 3.4.1 TOPOLOGÍAS DE REDES INALÁMBRICAS LAN
- 3.4.2 SEGURIDAD
- 3.4.3 AUTENTICACIÓN DE PUNTOS DE ACCESO Y DE LOS USUARIOS
- 3.4.4 IEEE 802.11
- 3.4.5 SEGURIDAD 802.1X
- 3.4.6 ROMPIENDO CANDADOS
- 3.4.7 AUTENTICACIÓN

3.1 Antecedentes

Todos tenemos una en nuestra casa, en nuestra oficina, el mundo esta lleno de computadoras, por eso es necesario, entenderlas y entender como funcionan…empezando desde sus orígenes.

El origen de las máquinas de calcular está dado por el ábaco chino, éste era una tablilla dividida en columnas en la cual la primera, contando desde la derecha, correspondía a las unidades, la siguiente a la de las decenas, y así sucesivamente. A través de sus movimientos se podía realizar operaciones de adición y sustracción.

Otro de los hechos importantes en la evolución de la informática lo situamos en el siglo XVII, donde el científico francés Blas Pascal inventó una máquina calculadora. Ésta sólo servía para hacer sumas y restas, pero este dispositivo sirvió como base para que el alemán Leibnitz, en el siglo XVIII, desarrollara una máquina que, además de realizar operaciones de adición y sustracción, podía efectuar operaciones de producto y cociente. Ya en el siglo XIX se comercializaron las primeras máquinas de calcular. En este siglo el matemático inglés Babbage desarrolló lo que se llamó "Máquina Analítica", la cual podía realizar cualquier operación matemática. Además disponía de una memoria que podía almacenar 1000 números de 50 cifras y hasta podía usar funciones auxiliares, sin embargo seguía teniendo la limitación de ser mecánica.

Recién en el primer tercio del siglo XX, con el desarrollo de la electrónica, se empiezan a solucionar los problemas técnicos que acarreaban estas máquinas, reemplazándose los sistemas de engranaje y varillas por impulsos eléctricos, estableciéndose que cuando hay un paso de corriente eléctrica será representado con un “1” y cuando no haya un paso de corriente eléctrica se representaría con un “0”.

Con el desarrollo de la segunda guerra mundial se construye el primer ordenador, el cual fue llamado Mark I y su funcionamiento se basaba en interruptores mecánicos.

En 1944 se construyó el primer ordenador con fines prácticos que se denominó Eniac.

En 1951 son desarrollados el Univac I y el Univac II (se puede decir que es el punto de partida en el surgimiento de los verdaderos ordenadores, que serán de acceso común a la gente).

Primera generación: 1946-1955. La tecnología de esta generación se basaba en grandes y pesadas válvulas de vacío; las cuales se sobre calentaban, y había que cambiarlas con frecuencias.

El ingreso y salida de los datos se realizaba mediante tarjetas o cintas perforadas, por lo que el procesamiento de la información era lento y secuencial.

Segunda generación: 1956-1964. En esta generación las computadoras utilizaban transistores que eran mucho más pequeños y confiables que las válvulas de vacío. El tamaño de las computadoras se redujo considerablemente. Los datos comenzaron en cilindros y cintas magnéticas. También aparece un nuevo periférico de salida, la impresora y se desarrollan los primeros lenguajes de alto nivel: Fortran, Cofol y comenzaron a usarse con fines comerciales.

Tercera generación: 1965-1970. Esta generación se caracteriza por la utilización de chips de circuitos integrados. Un chip permite agrupar miles de transistores en una oblea de silicio apenas más grande que un transistor. De ese modo, la velocidad de procesamiento se incrementó sustancialmente, asimismo, se mejoran los sistemas de almacenamiento existentes y se desarrollaron nuevos lenguajes de programación: Pascal; Basic; logo. Las computadoras se comenzaron a utilizar con fines múltiples.

Cuarta generación: 1971-2000. Durante esta generación se optimizaron los sistemas de producción de chips logrando circuitos integrados de alta escala de integración (LSI) y muy alta escala de integración (VLSI). Surgieron las PC, y las hogareñas, con lo cual su usó y se popularizó el Internet (que existía de la generación anterior). Se volvió también accesible a los hogares, y todo el mundo comenzó a estar conectado con un precio bajo.

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de los ordenadores (computadores), así como a la puesta en orbita de los satélites de comunicación.

A medida que avanzamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.

La industria de ordenadores ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo ordenador para satisfacer todas las

necesidades de cálculo de una organización se está reemplazando con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de ordenadores. Estas nos dan a entender una colección interconectada de ordenadores autónomos. Se dice que los ordenadores están interconectados, si son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, el uso de láser, microondas y satélites de comunicaciones. Al indicar que los ordenadores son autónomos, excluimos los sistemas en los que un ordenador pueda forzosamente arrancar, parar o controlar a otro, éstos no se consideran autónomos.

Las redes en general, consisten en "compartir recursos", y uno de sus objetivo es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 km de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico. Los ordenadores pequeños tienen una mejor relación costo / rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces mas rápidas que el mas rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas constituidos por poderosos ordenadores personales, uno por usuario, con los datos guardados una o mas máquinas que funcionan como servidor de archivo compartido.

Este objetivo conduce al concepto de redes con varios ordenadores en el mismo edificio. A este tipo de red se le denomina LAN (red de área local), en contraste con lo extenso de una WAN (red de área extendida), a la que también se conoce como red de gran alcance.

Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual a medida que crece la carga, simplemente añadiendo más procesadores. Con máquinas grandes, cuando el sistema esta lleno, deberá reemplazarse con uno mas grande, operación que por lo normal genera un gran gasto y una perturbación inclusive mayor al trabajo de los usuarios.

Otro objetivo del establecimiento de una red de ordenadores, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre si. Con el ejemplo de una red es relativamente fácil para dos o mas personas que viven en lugares separados, escribir informes juntos. Cuando un autor hace un cambio inmediato, en lugar de esperar varios días para recibirlos por carta. Esta rapidez hace que la cooperación entre grupos de individuos que se encuentran alejados, y que anteriormente había sido imposible de establecer.

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja (que nos discutiremos en este trabajo), actualmente está siendo ampliamente investigado. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos. No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica, sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.

Es en entonces que a lo largo de la historia los ordenadores (o las computadoras) nos han ayudado a realizar muchas aplicaciones y trabajos, el hombre no satisfecho con esto, buscó mas progreso, logrando implantar comunicaciones entre varias computadoras, o mejor dicho: "implantar Redes en las computadoras"; hoy en día la llamada Internet es dueña de las redes, en cualquier parte del mundo una computadora se comunica, comparte datos, realiza transacciones en segundos, gracias a las redes., y es de esto y sus todavía asombrosos avances lo que abordaremos a continuación.

3.2 Redes Informáticas

A mediados de los 70 diversos fabricantes desarrollaron sus propios sistemas de redes locales. Es en 1980 cuando Xerox, en cooperación con Digital Equipment Corporation e Intel, desarrolla y publica las especificaciones del primer sistema comercial de red denominado EtherNet. En 1986 IBM introdujo la red TokenRing. La mayor parte del mercado utiliza hoy día la tecnología del tipo EtherNet.

En 1982 aparecen los ordenadores personales, siendo hoy una herramienta común de trabajo. Esta difusión del ordenador ha impuesto la necesidad de compartir información, programas, recursos, acceder a otros sistemas informáticos dentro de la empresa y conectarse con bases de datos situadas físicamente en otros ordenadores, etc. En la actualidad, una adecuada interconexión entre los usuarios y procesos de una empresa u organización, puede constituir una clara ventaja competitiva. La reducción de costes de periféricos, o la facilidad para compartir y transmitir información son los puntos claves en que se apoya la creciente utilización de redes.

Una red es un conjunto de ordenadores conectados entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los distintos dispositivos. A través de una red se pueden ejecutar procesos en otro ordenador o acceder a sus ficheros, enviar mensajes, compartir programas...

Los ordenadores suelen estar conectados entre sí por cables. Pero si la red abarca una región extensa, las conexiones pueden realizarse a través de líneas telefónicas, microondas, líneas de fibra óptica e incluso satélites.

Cada dispositivo activo conectado a la red se denomina *nodo*. Un dispositivo activo es aquel que interviene en la comunicación de forma autónoma, sin estar controlado por otro dispositivo. Por ejemplo, determinadas impresoras son autónomas y pueden dar servicio en una red sin conectarse a un ordenador que las maneje; estas impresoras son nodos de la red.

Dependiendo del territorio que abarca una red se clasifican en:

- LAN: Local Area Network. Está constituida por un conjunto de ordenadores independientes interconectados entre sí, pueden comunicarse y compartir recursos. Abarcan una zona no demasiado grande, un edificio o un campus.
- WAN: Wide Area Network, comprenden regiones más extensas que las LAN e incluso pueden abarcar varios países.

También un conjunto de redes puede conectarse entre sí dando lugar a una red mayor.

3.2.1 Características de una red local

Los ordenadores conectados a una red local pueden ser grandes ordenadores u ordenadores personales, con sus distintos tipos de periféricos. Aunque hay muchos tipos de redes locales entre ellas hay unas características comunes:

- Un medio de comunicación común a través del cual todos los dispositivos pueden compartir información, programas y equipo, independientemente del lugar físico donde se encuentre el usuario o el dispositivo. Las redes locales están contenidas en una reducida área física: un edificio, un campus, etc.
- Una velocidad de transmisión muy elevada para que pueda adaptarse a las necesidades de los usuarios y del equipo. El equipo de la red local puede transmitir datos a la velocidad máxima a la que puedan comunicarse las estaciones de la red, suele ser de un Mb por segundo.
- Una distancia entre estaciones relativamente corta, entre unos metros y varios kilómetros.
- La posibilidad de utilización de cables de conexión normales.
- Todos los dispositivos pueden comunicarse con el resto y algunos de ellos pueden funcionar independientemente.
- Un sistema fiable, con un índice de errores muy bajo. Las redes locales disponen normalmente de su propio sistema de detección y corrección de errores de transmisión.
- Flexibilidad, el usuario administra y controla su propio sistema.

Los dos tipos básicos de dispositivos que pueden conectarse a una red local son las estaciones de trabajo y los servidores:

- Una estación de trabajo es un ordenador desde donde el usuario puede acceder a los recursos de la red.
- Un servidor es un ordenador que permite a otros ordenadores que accedan a los recursos de que dispone. Estos servidores pueden ser:
    - Dedicados: son usados únicamente para ofrecer sus recursos a otros nodos
    - No dedicados: pueden trabajar simultáneamente como servidor y estación de trabajo.

Existe un tipo de servidor un poco especial que se tratará por separado, es el servidor de comunicaciones. Este servidor permite que cualquiera de los equipos de una red se comunique con dispositivos o sistemas externos. A su vez, se dividirá en dos grandes grupos: *bridges y gateways.* De forma general, en una red, al nodo que pide un servicio o inicia una comunicación, se le denomina *cliente*. Al nodo que responde a la petición se le denomina *servidor*.

3.2.2 Medio de transmisión

Por medio de transmisión se entiende el soporte físico utilizado para el envío de datos por la red. La mayor parte de las redes existentes en la actualidad utilizan como medio de transmisión cable coaxial, cable bifilar o par trenzado y el cable de fibra óptica. También se utiliza el medio inalámbrico que usa ondas de radio, microondas o infrarrojos, estos medios son más lentos que el cable o la fibra óptica.

Cualquier medio físico o no, que pueda transportar información en forma de señales electromagnéticas se puede utilizar en redes locales como medio de transmisión.

Las líneas de transmisión son la espina dorsal de la red, por ellas se transmite la información entre los distintos nodos. Para efectuar la transmisión de la información se utilizan varias técnicas, pero las más comunes son: la banda base y la banda ancha.

Los diferentes tipos de red: EtherNet, TokenRing, FDDI, etc. pueden utilizar distintos tipos de cable y protocolos de comunicación.

Cable coaxial

Hasta hace poco, era el medio de transmisión más común en las redes locales. El cable coaxial consiste en dos conductores concéntricos, separados por un dieléctrico y protegido del exterior por un aislante (similar al de las antenas de TV).

Existen distintos tipos de cable coaxial, según las redes o las necesidades de mayor protección o distancia. Este tipo de cable sólo lo utilizan las redes EtherNet.

Existen dos tipos de cable coaxial:

- Cable *Thick* o cable grueso: es más voluminoso, caro y difícil de instalar, pero permite conectar un mayor número de nodos y alcanzar mayores distancias.
- Cable *Thin* o cable fino, también conocido como *cheapernet* por ser más económico y fácil de instalar. Sólo se utiliza para redes con un número reducido de nodos.

Ambos tipos de cable pueden ser usados simultáneamente en una red. La velocidad de transmisión de la señal por ambos es de 10 Mb.

Ventajas del cable coaxial:

- La protección de las señales contra interferencias eléctricas debida a otros equipos, fotocopiadoras, motores, luces fluorescentes, etc.
- Puede cubrir distancias relativamente grandes, entre 185 y 1500 metros dependiendo del tipo de cable usado.

Cable bifilar o par trenzado

El par trenzado consta como mínimo de dos conductores aislados trenzados entre ellos y protegidos con una cubierta aislante. Un cable de este tipo habitualmente contiene 1, 2 ó 4 pares, es decir: 2, 4 u 8 hilos.

Los cables trenzados o bifilares constituyen el sistema de cableado usado en todo el mundo para telefonía. Es una tecnología bien conocida. El cable es bastante barato y fácil de instalar y las conexiones son fiables. Sus ventajas mayores son por tanto su disponibilidad y bajo coste.

En cuanto a las desventajas están la gran atenuación de la señal a medida que aumenta la distancia y que son muy susceptibles a interferencias eléctricas. Por este motivo en lugar de usar cable bifilar paralelo se utiliza trenzado y para evitar las interferencias, el conjunto de pares se apantalla con un conductor que hace de malla. Esto eleva el coste del cable en sí, pero su instalación y conexionado continúa siendo más barato que en el caso de cables coaxiales. Tanto la red EtherNet como la TokenRing pueden usar este tipo de cable.

Fibra óptica

Es el medio de transmisión más moderno y avanzado. Utilizado cada vez más para formar la "espina dorsal" de grandes redes. Las señales de datos se transmiten a través de impulsos luminosos y pueden recorrer grandes distancias (del orden de kilómetros) sin que se tenga que amplificar la señal.

Por su naturaleza, este tipo de señal y cableado es inmune a las interferencias electromagnéticas y por su gran ancho de banda (velocidad de transferencia), permite transmitir grandes volúmenes de información a alta velocidad.

Estas ventajas hacen de la fibra óptica la elección idónea para redes de alta velocidad a grandes distancias, con flujos de datos considerables, así como en instalaciones en que la seguridad de la información sea un factor relevante.

Como inconveniente está, que es el soporte físico más caro. De nuevo, no debido al coste del cable en sí, sino por el precio de los conectores, el equipo requerido para enviar y detectar las ondas luminosas y la necesidad de disponer de técnicos cualificados para realizar la instalación y mantenimiento del sistema de cableado.

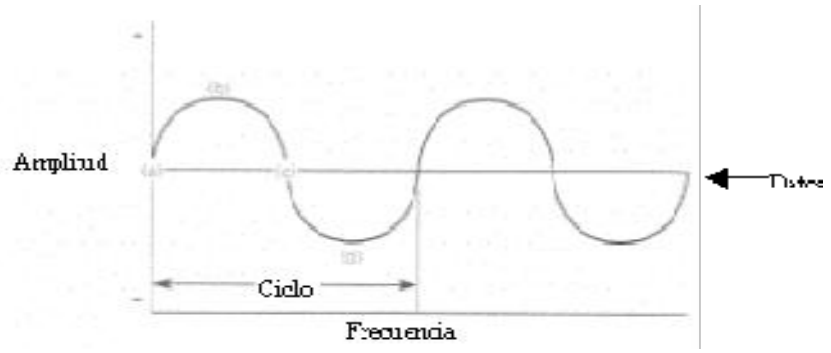
Capacidad del medio: Ancho de banda

El método de transmisión hace relación a la capacidad del medio para transmitir información. El ancho de banda nos indica la capacidad máxima del medio.

Ancho de banda: es la diferencia entre la frecuencia más alta y más baja de una determinada onda. El término ancho de banda hace referencia a la capacidad del medio de transmisión, cuanto mayor es el ancho de banda, más rápida es la transferencia de datos.

Por encima del ancho de banda las señales crean una perturbación en el medio que interfiere con las señales sucesivas. En función de la capacidad del medio, se habla de transmisión en banda base o transmisión en banda ancha.

Figura 3.1



Las redes en banda base generalmente trabajan con mayor velocidad de transmisión que las redes de banda ancha, aunque la capacidad de estas últimas de transmitir por varios canales simultáneamente pueden hacer que el flujo total de datos sea prácticamente el mismo en ambos sistemas.

La transmisión de banda base utiliza señales digitales sobre una frecuencia. Utiliza toda la capacidad del canal de comunicaciones para transmitir una única señal de datos.

3.2.3 Topología

Por *topología* de una red habitualmente se entiende la forma de la red, es decir, la forma en que se lleva a cabo la conexión. Las topologías más utilizadas son: en bus (lineal), en estrella, en árbol y en anillo.

Bus lineal

La topología en bus es un diseño sencillo en el que un solo cable, que es conocido como "bus", es compartido por todos los dispositivos de la red. El cable

va recorriendo cada uno de los ordenadores y se utiliza una terminación en cada uno de los dos extremos. Los dispositivos se conectan al bus utilizando generalmente un conector en T.

Las ventajas de las redes en bus lineal son su sencillez y economía. El cableado pasa de una estación a otra. Un inconveniente del bus lineal es que si el cable falla en cualquier punto, toda la red deja de funcionar. Aunque existen diversos procedimientos de diagnóstico para detectar y solventar tales problemas, en grandes redes puede ser sumamente difícil localizar estas averías.

Estrella

Los nodos de la red se conectan con cables dedicados a un punto que es una caja de conexiones, llamada *HUB* o *concentradores*. En una topología en estrella cada estación de trabajo tiene su propio cable dedicado, por lo que habitualmente se utilizan mayores longitudes de cable.

La detección de problemas de cableado en este sistema es muy simple al tener cada estación de trabajo su propio cable. Por la misma razón, la resistencia a fallos es muy alta ya que un problema en un cable afectará sólo a este usuario.

Árbol

La topología en *árbol* se denomina también topología en *estrella distribuida*. Al igual que sucedía en la topología en estrella, los dispositivos de la red se conectan a un punto que es una caja de conexiones, llamado HUB.

Estos suelen soportar entre cuatro y doce estaciones de trabajo. Los hubs se conectan a una red en bus, formando así un árbol o pirámide de hubs y dispositivos. Esta topología reúne muchas de las ventajas de los sistemas en bus y en estrella.

Anillo

En una red en *anillo* los nodos se conectan formando un círculo cerrado. El anillo es unidireccional, de tal manera que los paquetes que transportan datos circulan por el anillo en un solo sentido

En una red local en anillo simple, un corte del cable afecta a todas las estaciones, por lo que se han desarrollado sistemas en anillo doble o combinando topologías de anillo y estrella.

La red EtherNet cuando utiliza cable coaxial sigue una topología en bus lineal tanto físico como lógico. En cambio al instalar cable bifilar, la topología lógica sigue siendo en bus pero la topología física es en estrella o en estrella distribuida.

3.2.4 Método de acceso

El *método de acceso* a red es la manera de controlar el tráfico de mensajes por la red. Hay dos métodos de acceso de uso generalizado en redes locales: el acceso por contención, llamado también acceso aleatorio y el acceso determinístico.

Básicamente, el método de acceso por contención permite que cualquier usuario empiece a transmitir en cualquier momento siempre que el camino o medio físico no esté ocupado. En el método determinístico, cada estación tiene asegurada su oportunidad de transmitir siguiendo un criterio rotatorio.

Acceso por contención, aleatorio o no determinístico

Los métodos aleatorios o por contención utilizan redes con topología en bus; su señal se propaga por toda la red y llega a todos los ordenadores. Este sistema de enviar la señal se conoce como *broadcast*.

El método de contención más común es el *CSMA (Carrier Sense Multiple Access)* o en castellano *Acceso Multiple Sensible a la Portadora*. Opera bajo el principio de escuchar antes de hablar, de manera similar a la radio de los taxis. El método CSMA está diseñado para redes que comparten el medio de transmisión. Cuando una estación quiere enviar datos, primero escucha el canal para ver si alguien está transmitiendo. Si la línea esta desocupada, la estación transmite. Si está ocupada, espera hasta que esté libre.

Cuando dos estaciones transmiten al mismo tiempo habrá, lógicamente, una colisión. Para solucionar este problema existen dos técnicas diferentes, que son dos tipos de protocolos CSMA: uno es llamado CA - *Collision Avoidance*, en castellano *Prevención de Colisión* y el otro CD - *Collision Detection, Detección de Colisión*. La diferencia entre estos dos enfoques se reduce al envío –o no– de una señal de agradecimiento por parte del nodo receptor:

•*Collision Avoidance (CA).* Es un proceso en tres fases en las que el emisor:

1) Escucha para ver si la red está libre.

2) Transmite el dato.

3) Espera un reconocimiento por parte del receptor.

Este método asegura así que el mensaje se recibe correctamente. Sin embargo, debido a las dos transmisiones, la del mensaje original y la del reconocimiento del receptor, pierde un poco de eficiencia. La red EtherNet utiliza este método.

•*Collision Detection (CD).* Es más sencillo, recuerda al modo de hablar humano. Después de transmitir, el emisor escucha si se produce una colisión. Si no oye nada asume que el mensaje fue recibido. Aunque al no haber reconocimiento, no hay garantía de que el mensaje se haya recibido correctamente. Cuando varias personas mantienen una conversación, puede haber momentos en los que hablen a la vez dos o más personas. La que intenta comunicar, al detectar que su conversación ha *colisionado* con otra, debe iniciar de nuevo la conversación. La red AppleTalk (Local Talk) de Apple utiliza este método.

Si dos estaciones inician la transmisión simultáneamente se produce una colisión de las señales. La estación emisora, cuando detecta la colisión, bloquea la red para asegurar que todas las estaciones involucradas procesan el envío como erróneo. Entonces, cada estación espera un periodo corto de tiempo fijado aleatoriamente, antes de intentar transmitir de nuevo.

Aunque estos métodos puedan parecer imprecisos son de hecho muy exactos. Bajo condiciones de carga normales, raras veces ocurren colisiones y cuando aparecen, el emisor lo reintentará hasta que envíe su mensaje.

Acceso determinístico

El segundo de los métodos más usados es el de *acceso determinístico*. El sistema especifica (determina) qué estación es la que puede transmitir en cada instante de tiempo.

El método determinístico más usado es el *Token Passing* o paso de testigo. En una red Token Passing una secuencia especial de bits, el testigo, recorre la red de una estación a otra siguiendo un orden predeterminado. Cuando una estación quiere transmitir, espera que le llegue el testigo y lo guarda; envía su mensaje que circula por toda la red hasta volver a la estación emisora, entonces libera el testigo que viaja hasta la siguiente estación de red.

Los sistemas Token Passing están diseñados para resistir fuertes cargas de trabajo. Al ser un sistema ordenado, una red local usando el método Token Passing puede aprovechar el ancho de banda de trabajo hasta en un 90%. En principio, en un sistema con mucho tráfico, los retardos son menores usando métodos de acceso determinístico (Token Passing) que por contención (CSMA/CA-CD). Sin embargo, en un sistema sin mucha carga el método de contención es bastante más rápido y eficaz.

Uno de los factores más importantes que se deben tener en cuenta para evaluar el comportamiento de una red es el número de estaciones. En las redes con acceso determinístico el Token (testigo) circula a través de la red, teniendo cada estación derecho a transmitir antes de que se inicie una segunda vuelta. En una red de acceso por contención (aleatorio) el factor crítico será la carga de la

red. La degradación del rendimiento es más predecible en una red Token Passing que en una CSMA/CD.

Algunos ejemplos de redes de acceso determinístico son la TokenRing de IBM y la Arcnet de Datapoint.

3.2.5 Datagramas

Cada red tiene perfectamente definido el sistema físico de transporte de información. El bloque de información *básico* que circula por la red se denomina *datagrama*, y tiene una estructura y tamaño *característico* para cada red:

• Cabecera o *header*: tiene un tamaño definido y contiene la dirección de origen, la dirección de destino, el tamaño real de la información que transporta y tipo de servicio (protocolo o layer) que atiende. También contiene los datos temporales.

• Segmento de datos o *body*: Tiene un tamaño definido, aunque no necesariamente ocupado. Normalmente la información que se quiere enviar debe dividirse siendo necesario emplear varios datagramas.

Algunas redes emplean más de un tipo de datagramas. Así por ejemplo, las redes con método de acceso determinístico emplean datagramas distintos para el Token y para la información.

3.2.6 Protocolos

Se entiende por protocolo el conjunto de normas o reglas necesarias para poder establecer la comunicación entre los ordenadores o nodos de una red. Un protocolo puede descomponerse en niveles lógicos o capas denominados *layers*.

El comité 802 del IEEE (Institute of Electrical and Electronic Engineers) desarrolla protocolos estándares divididos en capas que se corresponden con el modelo de 7 niveles de la ISO (International Standards Organization).

Los protocolos establecen todas las reglas correspondientes al transporte en sus distintos niveles. Cada nivel de abstracción corresponde a un layer.

En un nivel se trabaja con la aplicación que maneja la información que se desea transportar; en otro se carga la información en los datagramas; otro nivel controla el acceso al medio… En el ordenador que recibe la información, los layers trabajan de forma análoga al que envía, pero en sentido inverso: controla el acceso al medio, lee los datagramas, reagrupa la información, y pasa los datos a la aplicación

3.2.7 Router, Bridge y Repeater

¿Qué hay que hacer para conectar dos redes distintas? El hecho de que sean redes distintas quiere decir que tienen *distinto* medio de transmisión, distinta *estructura* de la información que transmiten, *distintas* velocidades. Además, como puede intuirse con los ejemplos de transporte mencionados al hablar de protocolos, puede haber problemas de encaminamiento cuando la información pasa de una red a otra: dependiendo del tráfico, los paquetes de información pueden enviarse por caminos alternativos.

Un *Router* o *Gateway* es un dispositivo conectado en la red que une redes distintas. Por tanto, sus funciones son:

• Adaptar la estructura de información de una red a la otra (datagramas con tamaños y estructuras distintas)

• Pasar información de un soporte físico a otro (distintas velocidades y soportes físicos)

• Encaminar información por la ruta óptima

• Reagrupar la información que viene por rutas distintas

Un *bridge* une dos segmentos lógicos distintos de una misma red física. Dicho de otro modo: divide una red en dos subredes lógicas. El empleo de un bridge aísla el tráfico de información innecesaria entre segmentos, de forma que reduce las colisiones.

Un *repeater* amplifica la señal. Permite usar longitudes mayores de cable.

3.3 Internet

La idea de crear una red como Internet existe desde hace más de 20 años. Los primeros conceptos acerca de la red se desarrollaron en el año 1973, realizándose las primeras pruebas de interconexión de redes en julio de 1977. Se puede considerar que Internet ya estaba en actividad en los Estados Unidos, alrededor de 1982 y a finales de la década de los 80 comienza a expandirse internacionalmente, incluyendo usuarios y redes de distintas partes del mundo.

Sin embargo, hasta alrededor del año 1993, el uso de Internet estaba, en su mayor parte, limitado a círculos técnicos, científicos y académicos. La gran mayoría de la población, incluidas personas familiarizadas con la informática y el uso de ordenadores, nunca habían oído hablar de Internet. En determinado momento se produce un punto de inflexión en el cual todos los medios de difusión comienzan a hablar de Internet, el gran público empieza a interesarse por el tema, la Red comienza a insertarse en los distintos ámbitos de la sociedad y a tener

implicaciones económicas importantes. Surge World Wide Web, la telaraña mundial.

El auge de Internet se debe en gran medida a la aparición de World Wide Web (WWW, W3 o simplemente Web), pero hay otros factores tecnológicos que contribuyeron a este fenómeno. El desarrollo de ordenadores cada vez más veloces, con más capacidad y a bajos precios, junto con el perfeccionamiento del software correspondiente, unido al avance de las telecomunicaciones, hace posible que en los países desarrollados se generalice el uso doméstico de Internet.

La creación de W3 y su continuo desarrollo y los avances tecnológicos que la hacen posible, son dos hechos intrínsecamente relacionados, en el que cada uno tira del otro.

World Wide Web fue desarrollada inicialmente en el CERN (Laboratorio Europeo de Física de Partículas) en Ginebra. Los trabajos iniciales comenzaron en 1989 y entre finales de 1990 y comienzos de 1991 aparecen el primer servidor Web y un browser (navegador) para interfaces de tipo texto. El objetivo perseguido entonces era que los físicos europeos en el ámbito de altas energías, cuyos grupos de trabajo estaban dispersos por varios países, pudiesen intercambiar conocimientos y datos de modo eficiente.

El sistema se extendió rápidamente por todo el mundo abarcando a las instituciones más diversas y permitiendo el acceso a todo tipo de información.

Quizás uno de los principales factores que contribuyó a la rápida aceptación y al crecimiento de W3 fue la aparición, en septiembre de 1993 del primer navegador gráfico. Éste permitía visualizar documentos que combinaban texto e imágenes en un formato muy atractivo.

Además del WWW, Internet ofrece otros servicios más antiguos como el correo electrónico, grupos de noticias, FTP, Telnet y Wais.

Internet es una red mundial de redes de ordenadores, que permite a éstos comunicarse de forma directa y transparente, compartiendo información y servicios a lo largo de la mayor parte del mundo.

Para que dos ordenadores conectados a Internet puedan comunicarse entre sí es necesario que exista un lenguaje en común entre los dos ordenadores. Este lenguaje en común o protocolo es un conjunto de convenciones que determinan cómo se realiza el intercambio de datos entre dos ordenadores o programas.

Los protocolos usados por todas las redes que forman parte de Internet se llaman abreviadamente TCP/IP y son:

- Un protocolo de transmisión: TCP (*Transmission Control Protocol*)
- El protocolo Internet: IP (*Internet Protocol*)

Internet no es una red de ordenadores en el sentido usual, sino una red de redes, donde cada una de ellas es independiente y autónoma. Abarca a la mayor parte de los países, incluyendo miles de redes académicas, gubernamentales, comerciales, privadas, etc.

Se conoce como anfitrión o host a cualquier ordenador conectado a la red, que disponga de un número IP que presta algún servicio a otro ordenador.

Ordenador local (local host o local computer): es el ordenador en el que el usuario comienza su sesión de trabajo y el que se utiliza para entrar en la red. Es el punto de partida desde el cual se establecen las conexiones con otros ordenadores

Ordenadores remotos (remote host): aquellos con los que el usuario establece contacto a través de Internet y pueden estar situados físicamente en cualquier parte del mundo.

3.3.1 Clientes y servidores

El modelo cliente-servidor es uno de los mecanismos habituales para el intercambio de servicios e información en las redes de ordenadores y, en particular en Internet.

Cuando se utiliza un servicio en Internet como visualizar un documento de hipertexto se establece un proceso en el cual entran en juego dos partes:

El programa cliente. El usuario ejecuta en el ordenador local una aplicación que se pone en contacto con el ordenador remoto para solicitar la información deseada.

El programa servidor. Es el programa del ordenador remoto que provee la información requerida por el usuario local.

Los términos cliente y servidor se usan también para referirse a los ordenadores en los que se ejecutan esos programas:

- Ordenador cliente: el ordenador que solicita un servicio
- Ordenador servidor: el que responde al pedido

Funciones del programa cliente

Gestionar la comunicación con el servidor:

- Solicita un servicio
- Recibe los datos enviados por el servidor
- Gestiona los datos a nivel local

Manejar la interfaz con el usuario:

- Presenta los datos en el formato adecuado.
- Dota al usuario de las herramientas y los comandos necesarios para poder utilizar las prestaciones del servidor de forma sencilla.

Funciones del programa servidor

Transmite la información de forma eficiente, sin tener que preocuparse de atender a cada uno de los usuarios conectados. Así, un mismo servidor puede atender a varios clientes al mismo tiempo.

3.3.2 Cómo se transmite la información en Internet

Para que se pueda transmitir información a través de Internet son necesarios tres elementos:

Direcciones IP

Para que dos ordenadores, situados en cualquier parte del mundo, puedan comunicarse entre sí, es necesario que estén identificados de forma conveniente a través de una dirección.

Cada ordenador conectado a Internet tiene una dirección exclusiva y que lo distingue de cualquier otro ordenador del mundo, llamada *dirección IP o número IP.*

Dos ordenadores no pueden tener el mismo número IP, pero un ordenador sí puede tener varios números IP (*dot quad notation)*.

Las direcciones IP están formadas por cuatro números separados por puntos, cada uno de los cuales puede tomar valores entre 0 y 255. Por ejemplo:

192.168.100.112

Cada vez que se ejecuta una aplicación para utilizar un servicio en Internet, el software de comunicaciones del ordenador local necesita conocer la dirección IP del ordenador remoto con el que se quiere entrar en contacto.

Como memorizar números resulta complicado existe un sistema de identificación por nombres.

Encaminadores o Routers en Internet

Al ser Internet una red de redes, cada una de ellas es independiente, cuando se quiere enviar datos desde un ordenador (A) perteneciente a una red determinada, hasta un ordenador (B) situado en otra red; deben ser conducidos hasta él de alguna forma.

Los encaminadores o routers permiten interconectar las distintas redes y encaminar la información por el camino adecuado.

El esqueleto de Internet está formado por un gran número de routers y la información va pasando de uno a otro hasta llegar a su destino.

Existen muchos caminos posibles para llegar desde A hasta B. Cuando un router recibe un paquete decide cuál es el camino adecuado a seguir y lo envía al siguiente router. Éste vuelve a decidir y lo envía. El proceso se repite hasta que el paquete llega al destino final.

3.3.3 Protocolos TCP/IP y paquetes de información

Cuando se transfiere información de un ordenador a otro ésta no se transmite de una sola vez, sino que se divide en pequeños paquetes. Así las líneas de transmisión, los routers y los servidores no se monopolizan por un solo usuario durante demasiado tiempo.

Generalmente por los cables de la red viajan paquetes de información provenientes de diferentes ordenadores y con destinos diferentes. Esta forma de transmitir información se denomina "conmutación de paquetes". Cada paquete de datos contiene:

- Una porción de la información real que se quiere transmitir.
- Otros datos necesarios para el control de la transmisión.
- Las direcciones IP de los ordenadores de destino y de partida.

Todas las operaciones relacionadas con el encaminamiento de los paquetes de información y la inclusión de etiquetas con las direcciones IP de origen y destino están determinadas por el protocolo IP.

Para que los ordenadores puedan hablar entre sí es necesario el protocolo de control de transmisión (TCP). Este protocolo:

- Divide la información en paquetes del tamaño adecuado.
- Numera esos paquetes para que puedan volver a unirse en el orden correcto.

- Añade cierta información extra, necesaria para la transmisión y posterior descodificación del paquete. También para detectar posibles errores en la transmisión.

El software de TCP en el ordenador remoto se encarga de extraer la información de los paquetes recibidos, estos no tienen por qué llegar en el orden en el que fueron enviados, TCP se encarga de ensamblarlos en el orden correcto.

3.3.4 El sistema de nombres por dominio

Además del número IP existe otra forma de identificar a cada ordenador (host) en Internet, más fácil de memorizar y que permite descifrar intuitivamente la situación geográfica, la pertenencia o el propósito del ordenador en cuestión. Esto se consigue mediante el sistema de nombres por dominio.

3.3.4.1 El nombre de los ordenadores en Internet

El número IP es la forma que tienen las máquinas de llamarse entre sí, el nombre de dominio es la forma en que las personas suelen referirse a los ordenadores.

El sistema de nombres por dominio (Domain Name System, DNS) es un método para asignar nombres a los ordenadores a través de una estructura jerárquica.

Los nombres están formados por palabras separadas por puntos. Cada palabra representa un subdominio (FQDN: *Full Qualified Domain Server*) que a su vez está comprendido en un subdominio de alcance mayor:

web5.cti.unav.es

La primera palabra que aparece a la izquierda, por ejemplo: web5, es el nombre del ordenador, su nombre lo distingue de otros ordenadores que están dentro del mismo subdominio.

Cada una de las palabras que siguen corresponde a subdominios cada vez más amplios y que contienen a los anteriores. La última palabra, a la derecha, es el dominio principal o de primer nivel o de nivel superior.

Igual que las direcciones IP, los nombres por dominio de los ordenadores son exclusivos, no puede haber dos ordenadores distintos que tengan el mismo nombre. Sí es posible que un ordenador tenga más de un nombre que corresponda a un único número IP.

3.3.4.2 Los dominios de primer nivel

Los nombres de los subdominios son generalmente arbitrarios porque dependen de los administradores de las redes locales. Sin embargo los dominios de nivel superior y algunos subdominios amplios tienen reglas establecidas.

Existen diversos dominios de primer nivel convencionales:

-Nacionales: constan de dos letras que denotan a qué país pertenece el ordenador. España: es, Francia: fr, Gran Bretaña: uk...

-Internacionales y genéricos:

Internacionales: están reservados para las organizaciones de carácter internacional. Por el momento sólo existe uno: int.

Genéricos: pueden ser utilizados por entidades cuya actividad se extiende a uno o varios países. Comercial: com, organizaciones no comerciales: org, recursos de red: net.

Estados Unidos es una excepción ya que no se usa la terminación us como dominio principal. El motivo es que Internet tuvo su origen en las redes nacionales de Estados Unidos, por eso se utilizan dominios de primer nivel especiales:

edu: educación

mil: militar

gov: gobierno (no militar)

3.3.4.3 Determinación del número IP a partir de su nombre: el servidor DNS

El sistema de nombres por dominio constituye una forma idónea de nombrar a los ordenadores. Sin embargo, las máquinas necesitan el número IP para establecer contacto entre sí.

Para traducir los nombres por dominio a sus correspondientes números IP existen los servidores de nombres por dominio (DNS servers).

Debido a la gran cantidad de ordenadores que hay en la red y a los cambios constantes de estos es imposible mantener una base de datos centralizada que contenga todos los nombres por dominio existente. Sí existe una base de datos distribuida. Cada dominio principal, muchos subdominios y redes locales disponen

de un servidor DNS con los datos de ordenadores que le pertenecen: sus nombres y sus números IP para poder traducir.

Cuando un ordenador local necesita conocer el número IP de un ordenador remoto se inicia un proceso:

- El ordenador local envía un mensaje al servidor DNS más cercano. En el mensaje incluye el nombre por dominio que se desea traducir y se solicita el número IP correspondiente.
- El servidor DNS si tiene la dirección solicitada la envía inmediatamente. Si no la tiene establece una conexión y realiza la consulta a otro servidor de nombres, los servidores DNS se preguntan entre ellos hasta que se localiza el nombre por dominio. Cuando se localiza se envía al primer servidor DNS que lo solicitó.
- Cuando el servidor de nombres local dispone del número IP solicitado transmite esta información al ordenador que ha efectuado el pedido.

Si el nombre por dominio del ordenador remoto es incorrecto el servidor de nombres (DNS) no podrá determinar el número IP correspondiente, y el usuario recibirá un mensaje de error: "ERROR: the requested URL could not be retrieved", "DNS name lookup failure", etc.

3.4 Redes Inalámbricas

Actualmente podemos comunicar ordenadores mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja (que nos discutiremos en este trabajo), está siendo ampliamente investigado. Las Redes Inalámbricas facilitan la operación donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos. No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica, sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una " Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina. Existen dos amplias categorías de Redes Inalámbricas:

- De Larga Distancia.- Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps.
- De Corta Distancia.- Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no

se encuentran muy retirados entre si, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

Las redes inalámbricas de alta velocidad pueden proporcionar beneficios de conectividad en red sin las restricciones de estar ligadas a una ubicación o tejidas por cables. Existen muchos escenarios en donde esta puede ser una alternativa interesante, incluyendo los siguientes:

Las conexiones inalámbricas pueden ampliar o reemplazar una infraestructura cableada en situaciones en donde es costoso o está prohibido tender cables. Las instalaciones temporales son un ejemplo de cuándo una red inalámbrica puede tener sentido o hasta ser requerida. Algunos tipos de edificios o códigos de construcción pueden prohibir el uso de cables, haciendo de las redes inalámbricas una alternativa importante.

Y por supuesto el fenómeno de "no tener cables nuevos" que se relaciona con una instalación inalámbrica, conjuntamente con la red de líneas telefónicas y hasta la red eléctrica, se ha vuelto un catalizador principal para las redes en el hogar y la experiencia de un hogar conectado.

Los usuarios que cada vez son más móviles se vuelven un candidato evidente para una red inalámbrica. El acceso móvil a redes inalámbricas se puede lograr utilizando computadoras portátiles y tarjetas de red inalámbricas. Esto permite al usuario viajar a distintas ubicaciones - salas de reuniones, pasillos, vestíbulos, cafeterías, salas de clases, etc. - y aún tener acceso a los datos en red. Sin un acceso inalámbrico, el usuario tendría que llevar molestos cables y encontrar un punto de red para conectarse.

Más allá del campo corporativo, el acceso a Internet y hasta los sitios corporativos podrían estar disponibles a través de puntos de redes inalámbricas en lugares públicos. Aeropuertos, restaurantes, estaciones de ferrocarril y áreas comunes en una ciudad pueden contar con este servicio. Cuando el profesional que viaja llega a su destino, quizás para reunirse con un cliente en su oficina corporativa, él podría tener acceso limitado a través de una red local inalámbrica. La red puede reconocer al usuario de otra empresa y crear una conexión que quede aislada de la red local corporativa, pero que proporcione acceso a Internet al visitante.

En todos estos escenarios, vale la pena destacar que las redes inalámbricas actuales basadas en estándares operan a altas velocidades; las mismas velocidades que se consideraron de última tecnología para redes cableadas hace tan sólo unos años. El acceso que el usuario tiene típicamente es mayor a 11 MB o cerca de 30 a 100 veces más rápido que las tecnologías estándares de conexión discada o de redes cableadas WAN. Este ancho de banda ciertamente es adecuado para proveer una gran experiencia al usuario con varias aplicaciones o servicios a través de una PC o dispositivos portátiles. Además, los

avances continuos con estos estándares inalámbricos siguen aumentando el ancho de banda, con velocidades de hasta 22 MB.

Muchos proveedores de infraestructura están cableando áreas públicas en el mundo. En los próximos 12 meses, la mayoría de los aeropuertos, centros de conferencia y muchos hoteles proporcionarán acceso 802.11b a sus visitantes.

Actualmente, existen dos soluciones prevalecientes de redes inalámbricas que se están implementando. Estas soluciones son los estándares IEEE 802.11, principalmente 802.11b, y la solución propuesta por el grupo de trabajo HomeRF. Estas dos soluciones no Interactúan entre sí o con otras soluciones de redes inalámbricas. Si bien HomeRF está diseñada exclusivamente para el ambiente del hogar, 802.11b está diseñada y se puede implementar en hogares, pequeñas, medianas y grandes empresas, así como en un número cada vez mayor de lugares públicos con redes inalámbricas. Muchos de los principales fabricantes de PCs portátiles ya incluyen o tienen planes de ofrecer sistemas con tarjetas de red internas 802.11b.

3.4.1 Topologías de redes inalámbricas LAN

Las redes inalámbricas se construyen utilizando dos topologías básicas. Estas topologías se llaman de distintas formas, incluyendo administradas y no administradas, "hosted" y de punto a punto ("peer-to-peer"), así como de infraestructura y ad-hoc. En este documento utilizaremos los términos "infraestructura" y "ad-hoc". Estos términos se relacionan esencialmente con las mismas funciones básicas de la topología.

Una topología de infraestructura es una que amplía una red cableada existente a dispositivos inalámbricos, proporcionando una estación base (llamada punto de acceso). El punto de acceso se une a las redes inalámbricas y cableadas, actuando como un controlador central para la red inalámbrica. El punto de acceso coordina la transmisión y la recepción de múltiples dispositivos inalámbricos dentro de un rango específico. El rango y cantidad de dispositivos dependen del estándar inalámbrico que se utilice y el producto del proveedor. En la infraestructura puede haber varios puntos de acceso para cubrir una gran área o sólo un punto único de acceso para un área pequeña, como por ejemplo una casa o un edificio pequeño.

Una topología ad-hoc es una en la cual se crea una red LAN únicamente por los dispositivos inalámbricos mismos, sin controlador central o punto de acceso. Cada dispositivo se comunica directamente con los demás dispositivos en la red, en lugar de que sea a través de un controlador central. Esto es útil en lugares en donde pequeños grupos de computadoras pueden congregarse y no se necesita acceso a otra red. Por ejemplo, un hogar sin una red cableada o un cuarto de conferencia en donde se reúnen regularmente equipos para intercambiar ideas, son ejemplos en los que puede ser útil una red inalámbrica ad-hoc.

Por ejemplo, cuando se combinan la nueva generación de software y las soluciones inteligentes de punto a punto, estas redes inalámbricas ad-hoc pueden permitir a los usuarios que viajan colaborar, disfrutar de juegos con varios participantes, transferir archivos o comunicarse de alguna otra forma entre sí, utilizando sus PCs o dispositivos inteligentes de manera inalámbrica.

Descripción general de funcionamiento - Modalidad de Infraestructura

Una portátil o dispositivo inteligente, que se caracteriza como una "estación" en términos inalámbricos de una red, primero tiene que identificar los puntos y las redes disponibles de acceso. Esto se hace a través del monitoreo de cuadros 'beacon' desde puntos de acceso, anunciándose así mismo o probando activamente una red en particular utilizando cuadros de prueba.

La estación elige una red de las que están disponibles y sigue a través de un proceso de autenticación con el punto de acceso. Una vez que se han verificado entre sí el punto de acceso y la estación, se inicia el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y capacidades. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso en la red para dispersar conocimiento de la ubicación actual de la estación en la red. Sólo después de terminar la asociación la estación puede transmitir o recibir cuadros en la red.

En la modalidad de infraestructura, todo el tráfico en red de las estaciones inalámbricas en la red pasa a través de un punto de acceso para llegar a su destino y una red LAN ya sea cableada o inalámbrica.

El acceso a la red se maneja utilizando un protocolo de telecomunicación con sensor y evasión de colisiones. Las estaciones escucharán transmisiones de datos por un período específico de tiempo antes de intentar ejecutar la transmisión. La estación debe esperar un período específico de tiempo después de que la red quede limpia o quede lista antes de hacer la transmisión. Luego se genera un reconocimiento de la transmisión por parte de la estación receptora, indicando una recepción exitosa de la parte que evita colisión del protocolo. Observe que en esta modalidad de infraestructura, el transmisor o el receptor es siempre el punto de acceso.

Debido a que algunas estaciones no pueden escucharse entre sí, ahora que ambas están en el rango de punto de acceso, se deben hacer consideraciones especiales para evitar colisiones. Esto incluye un tipo de intercambio de reservación que puede tomar lugar antes de que se transmita un paquete, utilizando una solicitud para enviar y limpiar el intercambio de cuadros, así como un vector de asignación de red que se mantenga en cada estación de la red. Aún si una estación no puede escuchar la transmisión de la otra, escuchará la

autorización para enviar la transmisión desde el punto de acceso y puede evitar transmisiones durante ese intervalo.

El proceso de roaming desde un punto de acceso al otro no queda definido completamente por el estándar. Sin embargo, las guías y los sondeos que se utilizan para localizar puntos de acceso y un proceso de reasociación que permite que la estación se asocie con un punto de acceso diferente, en combinación con otros protocolos específicos de otros proveedores entre puntos de acceso, proporcionan una transición sin problemas.

La sincronización entre las estaciones en la red se maneja por los cuadros periódicos enviados por el punto de acceso. Estos cuadros contienen el valor de reloj del punto de acceso al momento de la transmisión, de tal manera que pueden utilizarse para verificar cualquier desviación en la estación de recepción. Se requiere de sincronización por distintas razones que tienen que ver con los protocolos inalámbricos y los esquemas de modulación.

Descripción general del funcionamiento - Modalidad ad-hoc

Una vez que se ha explicado la operación básica de la modalidad de infraestructura, se puede explicar la modalidad ad-hoc simplemente diciendo que no hay un punto de acceso. En esta red sólo están presentes los dispositivos inalámbricos. Muchas de las responsabilidades previamente manejadas por el punto de acceso, como los cuadros y la sincronización, las maneja una estación. Algunas mejoras no están disponibles en la red ad-hoc, como frame relays entre dos estaciones que no se puedan escuchar entre sí.

Siempre existen nuevos retos que surgen cuando se introduce un nuevo medio en un ambiente de redes. Con las redes inalámbricas esto es especialmente cierto. Algunos retos surgen de las diferencias entre las redes cableadas e inalámbricas. Por ejemplo, existe una medida de seguridad inherente en una red cableada en donde los datos los contiene la planta del cable. Las redes inalámbricas presentan nuevos retos, ya que los datos viajan a través del aire por ondas de radio.

Otros retos surgen de las capacidades únicas de las redes inalámbricas. Con la libertad de movimiento que se obtiene al remover los cables, los usuarios pueden caminar de un lugar a otro, ir de un edificio a otro, viajar de una ciudad a otra, etc., siempre requiriendo y esperando un nivel de conectividad continuo.

Algunos retos siempre han existido en las redes, pero se vuelven más complejos con las redes inalámbricas. Por ejemplo, debido a que la configuración es más fácil, las redes inalámbricas agregan funciones (algunas veces para resolver otros retos) y mediciones que se incorporan a los parámetros de configuración.

3.4.2 Seguridad

Con una red cableada existe una seguridad inherente en el hecho de que un ladrón potencial de datos tiene que tener acceso a la red a través de una conexión cableada, lo que normalmente quiere decir que necesita un acceso físico a la planta de cables de la red. Además de este acceso físico, se pueden estratificar otros mecanismos de seguridad.

Cuando la red ya no está formada por cables, la libertad adquirida por los usuarios de la red también puede ampliarse al robo potencial de datos. Ahora, la red puede estar disponible en los pasillos, áreas inseguras de espera, hasta afuera de un edificio. En un ambiente doméstico (en casa), su red puede ampliarse a las casas de sus vecinos si la red no adopta mecanismos adecuados de seguridad o si no se usa apropiadamente.

Desde su creación, 802.11 ha proporcionado algunos mecanismos básicos de seguridad para que esta mayor libertad no sea una amenaza potencial. Por ejemplo, los puntos de acceso de 802.11 (o conjuntos de puntos de acceso) se pueden configurar con un identificador de conjunto de servicio (SSID). Este SSID también debe conocerlo la tarjeta de red para poder asociarlo con el AP y así proceder con la transmisión y recepción de datos en la red. Esto es una seguridad muy débil, si es que existe tal, porque:

- El SSID es reconocido por todas las tarjetas de red y APs
- El SSID se envía a través del aire de manera libre (aún con lineamientos del AP)
- Independientemente de que se permita la asociación si el SSID no es reconocido, el mismo puede ser controlado por la tarjeta de red o controlador de manera local
- No se proporciona ninguna encriptación a través de este esquema

Si bien puede haber otros problemas con este esquema, esto ya es suficiente para no detener a ninguno de los piratas más inexpertos.

Se proporciona seguridad adicional a través de las especificaciones 802.11 por medio del algoritmo WEP. WEP proporciona 802.11 con servicios de autenticación y encriptación. El algoritmo WEP define el uso de una clave secreta de 40 bits para autenticación y encriptación y muchas implementaciones IEEE 802.11 también permiten claves secretas de 104 bits. Este algoritmo proporciona la mayor protección contra peligros y cuenta con atributos físicos de seguridad comparables con los de una red cableada.

Una limitación principal de este mecanismo de seguridad es que el estándar no define un protocolo para la administración de claves en la distribución de las mismas. Esto supone que las claves secretas y compartidas se entregan a la estación inalámbrica a través de un canal seguro independiente de IEEE 802.11.

Esto se vuelve un reto aún mayor cuando participa un gran número de estaciones, como en el caso de un campus corporativo.

Para proporcionar un mejor mecanismo en el control y seguridad de acceso, es necesario incluir un protocolo de administración de claves en la especificación. El estándar 802.1x, el cual se describe más adelante en este documento, se desarrolló específicamente para abordar este asunto.

Piense una cosa, nuestros datos son transmitidos como las ondas que recibimos en nuestra televisión o radio, si alguien tiene un receptor puede ver nuestros datos o si quiere estropearnos nuestro radio de transmisión.

3.4.3 Autentificación de puntos de acceso y de los usuarios.

Extensible Authentication Protocol (AP) o Extendido de Servicios (Extended Service Set - ESS) son formas de establecer una buena barrera de seguridad para poder identificar redes inalámbricas intrusas en una red o usuarios no permitidos. Utilizar estas opciones es muy recomendable ya que se establecen unos valores de seguridad usando la compatibilidad de nuestros propios productos. Si nuestra red es de una misma marca podemos escoger esta opción para tener un punto mas de seguridad, esto hará que nuestro posible intruso tenga que trabajar con un modelo compatible al nuestro, también se determina si los dispositivos de control pertenecen a nuestra red o al conjunto Extendido de Servicios, el AP revisa si el identificador de ESS es idéntico al nuestro, si no lo son, aún siendo el mismo fabricante y mismo modelo de AP, no podrán participar en la red y no puede recibir ni enviar ningún paquete de datos.

3.4.4 IEEE 802.11

El protocolo IEEE 802.11 o WI-FI es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación que utilizan todos los mismos protocolos. El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz. En la actualidad no se fabrican productos sobre este estándar. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11legacy." La siguiente modificación apareció en 1999 y es designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, también trabajaba en la frecuencia de 2,4 GHz. También se realizó una especificación sobre una frecuencia de 5 Ghz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la b y por motivos técnicos casi no se desarrollaron productos. Posteriormente se incorporó un estándar a esa velocidad

y compatible con el b que recibiría el nombre de 802.11g. En la actualidad la mayoría de productos son de la especificación b y de la g. El siguiente paso se dará con la norma 802.11n que sube el límite teórico hasta los 600 Mbps.

Actualmente ya existen varios productos que cumplen un primer borrador del estándar N con un máximo de 300 Mbps (80-100 estables). La seguridad forma parte del protocolo desde el principio y fue mejorada en la revisión 802.11i. Otros estándares de esta familia (c–f, h–j, n) son mejoras de servicio y extensiones o correcciones a especificaciones anteriores. El primer estándar de esta familia que tuvo una amplia aceptación fue el 802.11b. En 2005, la mayoría de los productos que se comercializan siguen el estándar 802.11g con compatibilidad hacia el 802.11b.

Los estándares 802.11b y 802.11g utilizan bandas de 2,4 giga hercios (Ghz) que no necesitan de permisos para su uso. El estándar 802.11a utiliza la banda de 5 GHz. El estándar 802.11n hará uso de ambas bandas, 2,4 GHz y 5 GHz. Las redes que trabajan bajo los estándares 802.11b y 802.11g pueden sufrir interferencias por parte de hornos microondas, teléfonos inalámbricos y otros equipos que utilicen la misma banda de 2,4 Ghz.

3.4.5 Seguridad 802.1X

Para proporcionar un nivel de seguridad más allá del que proporciona WEP, el equipo de red de Windows XP está trabajando con IEEE, proveedores de redes y otras entidades para definir IEEE 802.1X. 802.1X es un estándar previo para el control de acceso a redes basado en puertos, el cual se utiliza para proporcionar acceso autenticado a redes Ethernet. Este control de acceso a redes basado en puertos utiliza las características físicas de la infraestructura de las redes interconectadas para autenticar los dispositivos conectados a un puerto LAN. El acceso al puerto puede evitarse si falla el proceso de autenticación. Si bien este estándar está diseñado para redes Ethernet cableadas, también aplica a redes LAN inalámbricas 802.11.

Específicamente para el caso de redes inalámbricas, el punto de acceso puede actuar como un autenticador de accesos a la red, utilizando el servidor RADIUS para autenticar las identificaciones del cliente. La comunicación se realiza a través de un "puerto no controlado" o canal lógico en el punto de acceso, con el propósito de validar las identificaciones y obtener claves de acceso a la red a través de un "puerto lógico controlado". Las claves que están disponibles al punto de acceso y al cliente como resultado de este intercambio, permite que los datos del cliente se encripten y sean identificados por el punto de acceso. De esta manera, hemos agregado el protocolo de administración de claves a la seguridad de 802.11.

Los siguientes pasos delinean el enfoque genérico que se utilizaría para autenticar la máquina de un usuario, con el fin de que tenga acceso inalámbrico a la red.

- Sin una clave válida de autenticación, un punto de acceso prohíbe todo el flujo de tráfico hacia el mismo. Cuando una estación inalámbrica entra en el rango del punto de acceso, el punto de acceso emite un reto a la estación.
- Cuando la estación recibe el reto, responde con su identidad. El punto de acceso envía la identidad de la estación al servidor RADIUS para servicios de autenticación.
- El servidor RADIUS entonces requiere las identificaciones de la estación, especificando el tipo de identificaciones requeridas para confirmar la identidad de la estación. La estación envía sus identificaciones al servidor RADIUS (a través de un "puerto no controlado" del punto de acceso).
- El servidor RADIUS valida las identificaciones de la estación (asumiendo la validez) y transmite una clave autenticada al punto de acceso. La clave de autenticación se codifica de tal manera que sólo la puede interpretar el punto de acceso.
- El punto de acceso utiliza la clave de autenticación para transmitir de manera segura las claves apropiadas a la estación, incluyendo una clave de transmisión única de la sesión para esa estación y una clave global de sesión para transmisiones múltiples.
- Se puede solicitar a la estación que vuelva a realizar la autenticación periódicamente para mantener el nivel de seguridad.

Usar RADIUS facilita aún más la carga

Este enfoque 802.1x capitaliza el uso difundido y creciente de RADIUS para la autenticación. Un servidor RADIUS puede consultar una base de datos de autenticación local, si esto es lo apropiado para el ambiente. O, la solicitud se puede pasar a otro servidor para su validación. Cuando RADIUS decide que la máquina puede autorizarse en esta red, envía el mensaje de regreso al punto de acceso y luego el punto de acceso permite que fluya el tráfico de datos en la red. Un ejemplo de cómo esto funcionaría en un ambiente de negocios real, podría ser:

- Un usuario enciende su portátil, la cual contiene una tarjeta 802.11, en un aeropuerto.
- La máquina encuentra que existen redes inalámbricas disponibles, selecciona una red y se asocia con la misma.
- La máquina envía las identificaciones del usuario al punto de acceso para verificar que puede entrar en esta red.
- El usuario es ErikB@bigco.com. Bigco ha comprado acceso inalámbrico para todos sus usuarios en aeropuertos en todo el mundo.
- El servidor RADIUS, que recibe la solicitud del punto de acceso, observa el paquete y ve que es de un usuario BigCo.
- El servidor RADIUS pide luego a un servidor de BigCo definir si esta persona es un usuario real y si se permite el acceso.
- Si el servidor BigCo lo "afirma", entonces se le indica al punto de acceso que permita que fluya el tráfico.

Para proporcionar este nivel de seguridad, Microsoft ofrece con Windows XP una implementación de cliente 802.1X, a la vea que ha optimizado el servidor RADIUS de Windows - Servidor de autenticación de Internet (IAS) - para dar soporte a la autenticación de dispositivos inalámbricos.

Microsoft también ha trabajado con muchos proveedores de dispositivos 802.11 para soportar estos mecanismos en sus drivers de tarjetas de red y software de punto de acceso. Actualmente, muchos de los principales proveedores están próximos a comenzar a distribuir o ya distribuyeron en el mercado soporte 802.1x en sus dispositivos.

3.4.6 Rompiendo Candados

Cualquier usuario que disponga de una tarjeta de red Wireless, es decir, inalámbrica, puede conectarse a Internet utilizando el router o punto de acceso de otro usuario. Esto se debe a que la mayoría de las redes inalámbricas que se encuentran desprotegidas tienen activado un servidor DHCP (los router actuales suelen tener este servicio) que proporciona a las máquinas (ordenadores) conectados a esa red todo lo necesario: una dirección IP, la puerta de enlace, los servidores DNS… Por tanto con sólo configurar nuestra tarjeta para obtener estos parámetros de forma automática tendremos acceso a Internet.

El modo promiscuo (también llamado modo monitor).

El problema en estos casos radica en que una tarjeta de red sólo “hace caso” al trafico que está dirigido hacia ella. Si fuera posible acceder a todo el tráfico que circula por la red podríamos averiguar los parámetros necesarios para conectarnos a la red inalámbrica deseada. Esto es poner la tarjeta en modo promiscuo, hacer que reciba todo el tráfico aunque no vaya dirigido a ella.

Para ello debemos tener en cuenta que el tráfico al que estamos haciendo referencia está compuesto por paquetes, y cada paquete tendrá una estructura distinta según el protocolo que se esté usando.

Antes de seguir hay que decir que cada tarjeta de red inalámbrica puede tener un chipset distinto, aunque sea un modelo distinto del mismo fabricante. Así, los chipsets mas utilizados en este tipo de tarjetas son: Ralink, Altheros, Agere, Cisco y Realtek entre otros.

Investigando un poco en la página Web del fabricante de nuestra tarjeta inalámbrica podremos descubrir cuál es el chipset que utiliza.

Tráfico capturado

Con nuestra tarjeta de red inalámbrica en modo promiscuo y un buen “sniffer” (software que permite capturar el tráfico que circula por la red) se puede

empezar a capturar tráfico, analizar los paquetes que contiene y una vez hecho es posible determinar los parámetros a los que antes hacíamos referencia. El problema que ahora tenemos es la interpretación de los datos capturados.

En mi opinión, un software Opensource que realiza estas funciones y nos ayuda a interpretar los datos capturados es Ethereal.

Actualmente existen varios métodos para proteger una red inalámbrica. Los más habituales o conocidos son los siguientes: protección mediante MAC, protección WEP y protección WPA.

Las tarjetas de red cuentan con un identificador de 48 bits conocido como dirección MAC. Aunque es habitual la afirmación de que este identificador es único para cualquier dispositivo y que no se puede cambiar, he de decir que esto no es cierto. Sea como fuere, el método de protección mediante MAC se basa en que el router o el punto de acceso inalámbrico (AP) sólo permite la conexión a nuestra red a aquellos dispositivos cuya dirección MAC coincida con los que tiene almacenados.

Este método de protección es insuficiente, ya que si ponemos nuestra tarjeta de red inalámbrica en modo promiscuo y usamos un analizador de protocolos como Ethereal podemos descubrir la dirección MAC de algún dispositivo que se conecte a esta red y hacernos pasar por él.

Si se utiliza el método de protección WEP los datos viajan cifrados y por lo tanto este método es más seguro. Sin embargo he de decir que el uso de este método tampoco es suficiente, ya que el cifrado WEP se ha demostrado inseguro y es posible descifrar los datos que hayan sido cifrados con este protocolo y por consiguiente se puede averiguar la clave WEP y los parámetros necesarios para poder acceder a una red protegida con este método.

Rompiendo la clave WEP

WEP básicamente es la encriptación de nuestros datos o paquetes enviados por nuestra red, esto añade cierto grado de seguridad para evitar intrusos en nuestra red. Muchos usuarios son reacios al uso del WEP ya que se a demostrado que el cifrado puede ser ineficaz en algunas ocasiones, pero también puede ser un gran muro de seguridad si se realiza con ciertas reglas de uso.

En la red se encuentra disponible una gran variedad de software para analizar y “romper” la protección de los paquetes protegidos mediante WEP. Un ejemplo de este software puede ser aircrack. Se trata de un conjunto de utilidades que permiten monitorizar una red inalámbrica: captura paquetes, permite la inyección de tráfico en la red, y lo que es más, permite romper el cifrado de paquetes WEP.

El otro método que hemos mencionado es la protección basada en WPA. Al igual que ocurre con WEP se trata de un método que utiliza la criptografía para cifrar los paquetes que viajan por la red. Sin embargo este método es mas seguro, ya que se ha demostrado que es menos vulnerable. Existe una primera implementación de este método cuyos paquetes pueden ser descifrados con aircrack. La nueva implementación de WPA a la que estamos haciendo referencia es WPA2.

De forma generar podemos decir que WPA es mucho mas robusto y seguro que WEP; sin embargo WPA es más difícil de configurar y no todos los dispositivos inalámbricos permiten su uso, por lo que la mayoría de las redes protegidas usan WEP.

3.4.7 Autenticación

Están disponibles los siguientes tipos de autenticación para utilizarlos con las redes 802.11:

- Sistema abierto
- Clave compartida
- IEEE 802.1X
- WPA o WPA2 con clave previamente compartida

Sistema abierto

La autenticación de sistema abierto no es realmente una autenticación, porque todo lo que hace es identificar un nodo inalámbrico mediante su dirección de hardware de adaptador inalámbrico. Una dirección de hardware es una dirección asignada al adaptador de red durante su fabricación y se utiliza para identificar la dirección de origen y de destino de las tramas inalámbricas.

Para el modo de infraestructura, aunque algunos puntos de acceso inalámbricos permiten configurar una lista de direcciones de hardware permitidas para la autenticación de sistema abierto, resulta bastante sencillo para un usuario malintencionado capturar las tramas enviadas en la red inalámbrica para determinar la dirección de hardware de los nodos inalámbricos permitidos y, a continuación, utilizar la dirección de hardware para realizar la autenticación de sistema abierto y unirse a su red inalámbrica.

Para el modo ad hoc, no existe equivalencia para la configuración de la lista de direcciones de hardware permitidas en Windows XP. Por lo tanto, se puede utilizar cualquier dirección de hardware para realizar la autenticación de sistema abierto y unirse a su red inalámbrica basada en el modo ad hoc.

Clave compartida

La autenticación de clave compartida comprueba que el cliente inalámbrico que se va a unir a la red inalámbrica conoce una clave secreta. Durante el proceso de autenticación, el cliente inalámbrico demuestra que conoce la clave secreta sin realmente enviarla. Para el modo de infraestructura, todos los clientes inalámbricos y el punto de acceso inalámbrico utilizan la misma clave compartida. Para el modo ad hoc, todos los clientes inalámbricos de la red inalámbrica ad hoc utilizan la misma clave compartida.

IEEE 802.1X

El estándar IEEE 802.1X exige la autenticación de un nodo de red para que pueda comenzar a intercambiar datos con la red. Si se produce un error en el proceso de autenticación, se deniega el intercambio de tramas con la red. Aunque este estándar se diseñó para las redes Ethernet inalámbricas, se ha adaptado para su uso con 802.11. IEEE 802.1X utiliza EAP (Protocolo de autenticación extensible) y métodos de autenticación específicos denominados tipos EAP para autenticar el nodo de red.

IEEE 802.1X proporciona una autenticación mucho más segura que el sistema abierto o la clave compartida y la solución recomendada para la autenticación inalámbrica de Windows XP es el uso de EAP-TLS (Transport Layer Security) y certificados digitales para la autenticación. Para utilizar la autenticación EAP-TLS para las conexiones inalámbricas, debe crear una infraestructura de autenticación que conste de un dominio de Active Directory, servidores RADIUS (Servicio de usuario de acceso telefónico de autenticación remota) y entidades emisoras de certificados para emitir certificados a los servidores RADIUS y los clientes inalámbricos. Esta infraestructura de autenticación resulta más adecuada para grandes empresas y organizaciones empresariales, pero no es práctica para una oficina doméstica o de pequeña empresa.

La solución al uso de IEEE 802.1X y EAP-TLS para las pequeñas y medianas empresas es PEAP (EAP protegido) y el protocolo de autenticación por desafío mutuo de Microsoft, versión 2 (MS-CHAP v2) tipo EAP. Con PEAP-MS-CHAP v2, se puede lograr un acceso inalámbrico seguro mediante la instalación de un certificado adquirido en un servidor RADIUS y utilizando credenciales de nombre y contraseña para la autenticación. Windows XP con SP2, Windows XP con SP1, Windows Server 2003 y Windows 2000 con Service Pack 4 (SP4) admiten PEAP-MS-CHAP v2.

WPA o WPA2 con clave previamente compartida

Para una red doméstica o de pequeña empresa donde no se pueda realizar la autenticación 802.1X, WPA y WPA2 proporcionan un método de autenticación de clave previamente compartida para redes inalámbricas en modo de infraestructura. La clave previamente compartida se configura en el punto de

acceso inalámbrico y en cada cliente inalámbrico. La clave de cifrado WPA o WPA2 inicial se deriva del proceso de autenticación, que comprueba que tanto el cliente inalámbrico como el punto de acceso inalámbrico están configurados con la misma clave previamente compartida. Cada clave de cifrado WPA o WPA2 inicial es exclusiva.

La clave WPA o WPA2 previamente compartida debe ser una secuencia aleatoria de caracteres de teclado (letras mayúsculas y minúsculas, números y signos de puntuación) de una longitud mínima de 20 caracteres o dígitos hexadecimales (números del 0 al 9 y letras de la A a la F) de una longitud mínima de 24 dígitos hexadecimales. Cuanto más aleatoria sea la clave WPA o WPA2 previamente compartida, más seguro será su uso. A diferencia de la clave WEP, la clave WPA o WPA2 previamente compartida no está sujeta a la determinación mediante la recopilación de una gran cantidad de datos cifrados. Por lo tanto, no es necesario cambiar la clave WPA o WPA2 previamente compartida con tanta frecuencia.

Mientras no se protejan adecuadamente las redes inalámbricas (Wireless) cualquier usuario no experto podrá entrar en cualquier red y usar los servicios que en ella están disponibles, como Internet. Además si no se protege la red de forma adecuada algún usuario mal intencionado la tendrá más fácil para acceder a nuestros equipos y por lo tanto a nuestra información, que es tan valiosa para nosotros.

CAPÍTULO 4

IMPLEMENTACIÓN DE LA RED

4.1 PLANEACIÓN
4.2 DISEÑO
4.3 INSTALACIÓN
    4.3.1 PROBANDO LA CALIDAD DE LA CONEXIÓN
    4.3.2 MONTANDO LA RED
4.4 CONFIGURACIÓN
    4.4.1 TARJETA DE RED
    4.4.2 PUNTOS DE ACCESO
    4.4.2.1 CREAR INTERCONEXIÓN WDS
    4.4.3 HOTSPOT

4.1 Planeación

Hoy en día cualquier hotel que tenga entre sus principios el ofertar variedad de servicios con calidad debe ofrecer a sus huéspedes la posibilidad de conectarse a Internet y, si es posible, ofrecer múltiples opciones de conexión para así poder satisfacer toda la variedad de perfiles de clientes que llegan al establecimiento.

Especialmente, en hoteles orientados a los negocios, ofrecer acceso a Internet a cualquier hora del día y con total comodidad se ha convertido ya en algo normal en la mayoría de alojamientos.

Actualmente, la explosión de las redes inalámbricas (WIFI) ha hecho que pocos sean los hoteles de calidad que no ofrecen esta forma de conexión. Sin duda la más cómoda para el huésped que puede disponer de su portátil en cualquier lugar de su habitación y/o zonas comunes del hotel, salones, etc. Especialmente en salones para reuniones, charlas, congresos, etc. es bastante importante tener acceso inalámbrico para facilitar al máximo el montaje del evento al cliente y a todos los asistentes.

Otra opción que ofrecen muchos hoteles, ya sea como alternativa o bien como forma complementaria de conexión es disponer de puntos de conexión con cable LAN en habitaciones y/o zonas comunes. Si bien no es tan cómoda como el WIFI si que es interesante tenerla ya que no siempre el cliente puede tener WIFI en su portátil si bien esto cada vez es menos frecuente.

Y aunque parezca que hablemos de una opción totalmente en desuso, la conexión por módem tradicional vía RTC es algo que aún muchos huéspedes solicitan. El perfil de estos usuarios suelen ser clientes de empresas que acceden a la red interna de su compañía vía RAS (Remote Access Service). Todavía son muchas las empresas que tienen configurados su acceso interno desde el interior “a la antigua usanza” (marcando teléfono de contratación propia del cliente) en vez de considerar otras opciones más modernas por lo que para satisfacer esta demanda y dar un acceso completo a los clientes es necesario.

El servicio se puede considerar casi completo si la oferta se complementa con un business center o una zona común habilitada para aquellos clientes que no tienen su ordenador y quieren conectarse a Internet, imprimir, copiar sus datos a un CD, etc. Los dos puntos que completarían totalmente un excelente servicio es, por un lado la disposición de tarjetas WIFI (PCMCIA/USB) para aquellos clientes que no disponen de esta tecnología en sus equipos y, por otro lado, la existencia de un personal técnico de apoyo a los clientes para ayudar a configurar sus equipos para acceder a la red WIFI del hotel o resolver cualquier tipo de incidencia.

Mediante la solución de acceso a internet de forma inalámbrica, los clientes del hotel pueden conectar sus propios equipos portátiles a internet de una forma fácil y sencilla.

El sistema planea componerse de un punto central de gestión colocado normalmente en la recepción del hotel, varios puntos de acceso inalámbrico repartidos por diferentes puntos del hotel y una impresora de tickets pre-pago vinculada al ruteador o puerta de enlace que hace la función de hot spot y administra las sesiones.

Internet en todo el hotel gracias a la red WIFI

Como el acceso a internet es inalámbrico (se realiza mediante tecnología WIFI), el cliente tendrá una movilidad absoluta por todo el hotel. Es decir, puede conectarse a internet con su portátil en su habitación y luego bajar a la cafetería o a la piscina del hotel y seguir disfrutando de su conexión a internet.

Retorno de la inversión del sistema

El sistema de acceso a internet mediante WIFI, puede ofrecerse por parte del hotel de forma gratuita, o bien puede cobrarse por horas que el cliente haya estado conectado a internet para realizar un retorno de la inversión de la instalación del sistema de acceso inalámbrico a internet.

Para el acceso mediante pre-pago a la red inalámbrica del hotel y por consiguiente a internet, el cliente tendrá que solicitar en la recepción del hotel un ticket o bono con el número de horas que quiere poder disfrutar de la red WIFI de la que dispone el hotel para el acceso a internet.

Una vez haya transcurrido el tiempo del ticket o bono que solicitó el cliente del hotel, el sistema cerrará la conexión del cliente a internet y éste no podrá volver a conectarse a internet a través de la red inalámbrica a no ser que compre otro ticket en la recepción del hotel.

Seguridad del sistema de la red WI-FI en el hotel

Una vez el cliente ha solicitado y pagado un bono o ticket en la recepción del hotel, el recepcionista, le entregará un ticket con un nombre de usuario y una contraseña de acceso para poder conectarse a la red inalámbrica del hotel y por tanto a internet utilizando su ordenador portátil o su PDA.

Los usuarios y contraseña suministrados por el sistema al entregar un ticket bono de acceso a la red inalámbrica del hotel, son únicos y exclusivos para el cliente que solicitó el bono y sólo sirven para el tiempo de duración del ticket o bono que se le suministró en la recepción del hotel. Una vez transcurrido el tiempo disponible de conexión a internet en el hotel, el sistema elimina ese

nombre de usuario y contraseña y no vuelve a usarlo nunca más. Esto garantiza que nadie se conecte fraudulentamente a la conexión de internet del hotel mediante la red inalámbrica.

Otro nivel de seguridad que incorpora la solución de acceso a internet mediante WIFI en hoteles, es que incorpora un sistema de protección que imposibilita que los usuarios conectados a la red del hotel y que están disfrutando de la conexión a internet puedan verse entre ellos. De esta forma ningún usuario que esté conectando a la red WIFI del hotel podrá ver documentos o carpetas de ningún otro usuario.

Además el sistema incorpora varios elementos de seguridad en redes inalámbricas:

- WEP
- WPA
- RADIUS
- SSL

Simplicidad en la conexión a internet mediante WIFI

Otra de las ventajas que incorpora el sistema de conexión a internet a través de WIFI en hoteles, es que el cliente no tiene que cambiar ninguna configuración de su ordenador portátil o PDA.

Simplemente cuando su ordenador detecte la red inalámbrica de acceso a internet del hotel, el sistema redirigirá el navegador del ordenador del cliente a una página Web en la que se le solicitará al cliente un nombre de usuario y una contraseña. Ese nombre de usuario y contraseña son los que se le proporcionaron en la red del hotel cuando adquirió su ticket para el acceso a internet en el hotel.

Ventajas del sistema de acceso a internet inalámbrico para el hotel.

- Ofrecer un valor añadido a los servicios del hotel para sus clientes.
- Posibilidad de retorno de la inversión cobrando por el acceso a internet.
- Garantizar la seguridad del acceso a internet del cliente del hotel.
- Ventajas del acceso a internet inalámbrico en hoteles para el cliente.
- Posibilidad de revisar el correo electrónico e internet.
- Movilidad por todo el hotel sin perder la conexión a internet.

- Tener sus documentos seguros gracias a la seguridad incorporada en el sistema.

- Facilidad y simplicidad de la conexión a Internet.

4.2 Diseño

La calidad de señal que tenemos en una zona de cobertura Wireless viene determinada por la relación entre la potencia de la señal recibida y el nivel de ruido existente, incluyendo posibles señales interferentes. A dicha diferencia de potencias se le conoce como la relación señal-ruido, o SNR. Nosotros hemos considerado que por encima de 15db de SNR la calidad de la señal recibida es aceptable. Entonces el movernos alrededor de un punto de acceso nos determinará un área de cobertura determinada

Sin embargo dicha área de cobertura varia considerablemente según el entorno en que se encuentre ubicado dicho punto de acceso, por lo que no es posible extrapolar resultados obtenidos en un entorno abierto, hacia un entorno cerrado o semi-cerrado de oficinas. De este modo en un entorno de oficinas con paredes y muros de hormigón armado el área de cobertura se reduce considerablemente en comparación con un entorno de oficinas donde las separaciones entre despachos estén realizadas a base de ladrillos, madera o vidrio. Sin embargo dicha desventaja puede convertirse en un aliado cuando se desea limitar el área de cobertura a un determinado recinto por ejemplo por motivos de seguridad o bien para preservar el ancho de banda disponible.

En cuanto al emplazamiento de los puntos de acceso se trata hay un conjunto de recomendaciones que hay que tener en cuenta. Entre ellas que dicha banda de 2,4 Ghz es también utilizada por otras tecnologías sin hilos que pueden interferir con el servicio inalámbrico. Por ejemplo: Microondas y otros dispositivos comerciales con tecnología Bluetooth que trabajan utilizando la misma banda.

Así mismo el movimiento de personas también puede reducir el nivel de señal por lo que se recomienda no poner los puntos de acceso a alturas próximas al nivel de las personas sino algo más alto sobretodo en zonas de tránsito. También es bueno evitar las reflexiones de la señal por efecto de obstáculos ubicando dichos dispositivos a una cierta altura en un espacio abierto.

No olvidemos que “dicho punto de acceso inalámbrico debe conectarse a un punto de red alámbrica” así como a una toma de red eléctrica que en ocasiones dificulta las cosas pues en ocasiones el dispositivo destino es distante.

Es por todo ello que una vez determinadas las áreas a cubrir la opción más prudente consiste en analizar el sitio o “a pie”. El nivel de SNR detectado tras ubicar un punto de acceso en las proximidades e ir desplazando o reorientando este punto hasta conseguir cubrir el área deseada con los niveles deseados.

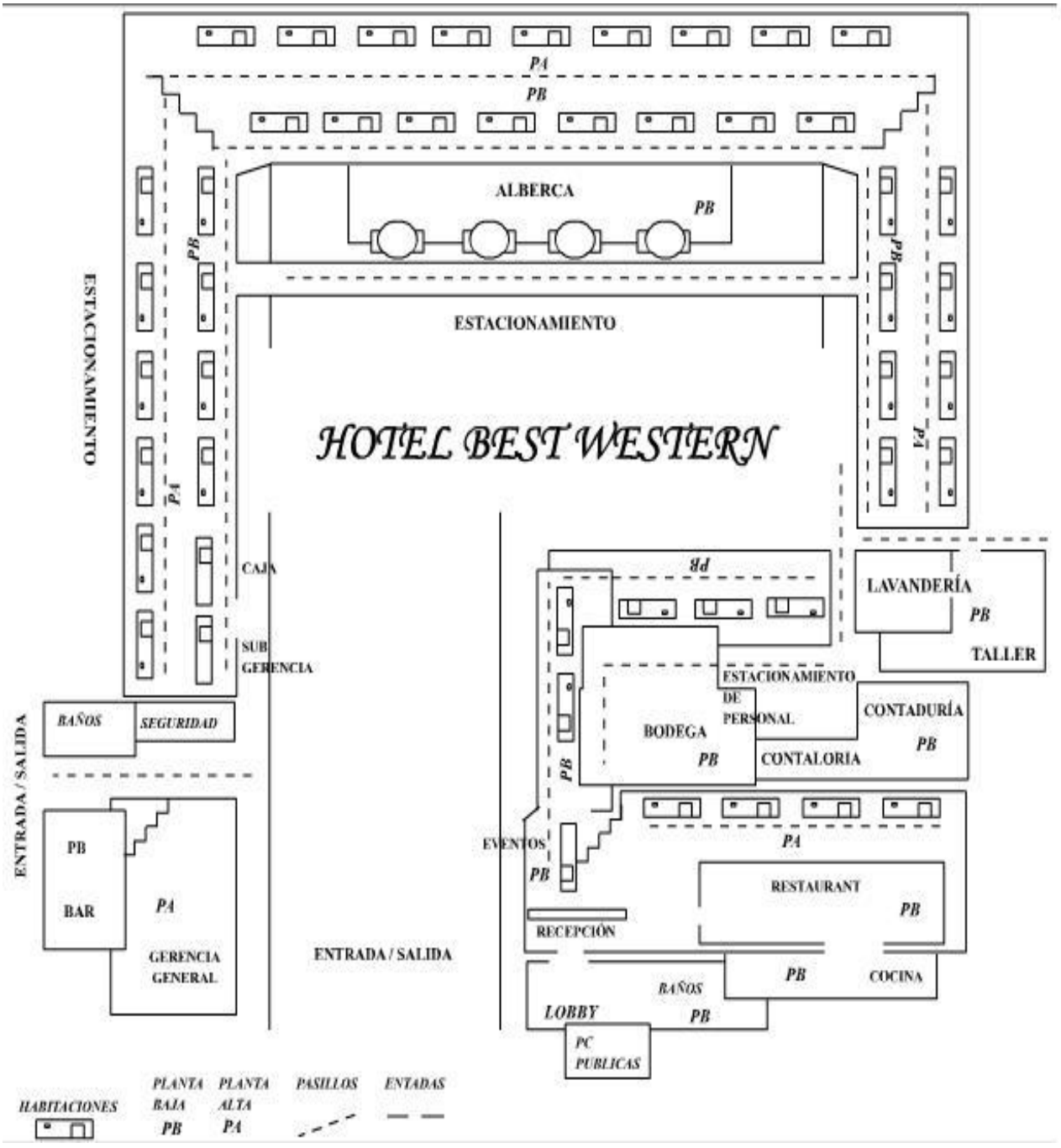
Por otro lado, aunque sería de gran ayuda el poder disponer del diagrama de radiación de las antenas de punto de acceso así como de las tarjetas PCMCIA en caso de que estas fueran diferentes, normalmente dicha información no se suministra y se reduce a simplemente indicar que son omnidirecionales, tras lo cual dicha metodología de campo resulta ser la más efectiva.

Los fabricantes de las principales marcas en el sector incluyen software cliente para poder tomar dichas medidas de relación SNR.

Si bien según el estándar 802.11b sólo se dispone de hasta 3 canales para trabajar simultáneamente sin solapamiento, es posible llegar a utilizar hasta 4 con un análisis de cobertura “en sitio” de forma que no haya interferencia entre ellos.

A continuación nos enfocaremos a nuestro caso en concreto, las instalaciones del hotel Best Western.

Figura 4.1



La arquitectura del hotel Best Western como vemos en la figura 4.1 nos detalla la ubicación de las habitaciones, donde se encuentran nuestros futuros usuarios. Nuestra finalidad antes de comenzar nuestra instalación es situar

estratégicamente los puntos de acceso así como las antenas de ampliación de señal a manera de que en cualquier parte que se encuentre el cliente cuente con una señal lo suficientemente fuerte para conectarse a Internet.

He iniciado este proyecto empezando a hacer pruebas con una antena omnidireccional estándar de 12 Dbi a 2.4 Ghz que incluye un punto de acceso (access point) como terminal. Una antena de este tipo orienta la señal en todas direcciones con un haz amplio pero de corto alcance. Sería como una bombilla emitiendo luz en todas direcciones pero con una intensidad menor que la de un foco, es decir, con menor alcance.

Las antenas Omnidireccionales "envían" la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

El alcance de una antena omnidireccional viene determinado por una combinación de los Dbi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. A mismos Dbi, una antena sectorial o direccional dará mejor cobertura que una omnidireccional.

Las antenas direccionales se suelen utilizar para unir dos puntos a largas distancias mientras que las antenas omnidireccionales se suelen utilizar para dar señal extensa en los alrededores. Las antenas sectoriales se suelen utilizar cuando se necesita un balance de las dos cosas, es decir, llegar a largas distancias y a la vez, a un área extensa.

En este caso que necesito dar cobertura de red inalámbrica en toda un área próxima (las diferentes secciones del edificio que forma el hotel) encuentro más adecuado utilizar una antena omnidireccional. Si tuviera que dar cobertura de red inalámbrica en un punto muy concreto (por ejemplo una portátil que esté bastante lejos) utilizaría una antena direccional, finalmente, si necesitara dar cobertura amplia y a la vez a larga distancia, utilizaría antenas sectoriales, pero éstas elevan mucho su precio y puedo reemplazar su utilidad con la combinación de otras de otro tipo.

Me he situado en puntos que por sentido común serían cómodos para el usuario o cliente del hotel. Empezando por las habitaciones debo decir que las paredes son bastante gruesas y lucen un tanto burdas, a pesar de que se han realizado pruebas para medir la fortaleza de la señal encuentro razonable la propuesta para la utilización de más de 1 antena y me inclino por proponer 3 de ellas.

He notado que en el área de corredores de las plantas altas, la señal (aún teniendo la antena de frente) no es muy buena y me parece buena idea fortalecerla con puntos de acceso independientes.

Recordando mi cita anterior: “Dicho punto de acceso inalámbrico debe conectarse a un punto de red alámbrica”. Encuentro la dificultad que tendrían un par de ellos para llegar a su destino, pues tendría que recorrer más de 40 metros en distancia directa y recta, sin contar obviamente con todos los obstáculos que representa una instalación o infraestructura tan compleja que lleva un hotel, así que situando la terminal de cada antena en formación delta es posible configurar el WDS entre éstas y olvidarnos de tanto cableado.

Con WDS, un punto de acceso puede funcionar no sólo como punto de acceso, bien como puente con otro punto de acceso, o ambas funciones.

De esta manera es posible crear una gran red inalámbrica dado que cada punto de acceso se conecta a cualquier otro punto de acceso disponible (que use WDS) y a cada punto de acceso se puede conectar (de forma cableada o inalámbrica) la cantidad máxima que soporte el aparato (típicamente 256 equipos).

Se requiere que todos los equipos usen el mismo canal de radio (frecuencia) y si usan cifrado WEP compartan las llaves de la clave.

Los SSID de los puntos de acceso pueden ser diferentes.

El SSID (Service Set IDentifier) es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Existen algunas variantes principales del SSID. Las redes *ad-hoc*, que consisten en máquinas cliente sin un punto de acceso, utilizan el BSSID (*Basic Service Set Identifier*); mientras que en las redes en infraestructura que incorporan un punto de acceso, se utiliza el ESSID (E de extendido). Nos podemos referir a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como nombre de la red.

Uno de los métodos más básicos de proteger una red inalámbrica es desactivar el *broadcast* del SSID, ya que para el usuario medio no aparecerá como una red en uso. Sin embargo no debería ser el único método de defensa para proteger una red inalámbrica. Se deben utilizar también otros sistemas de cifrado y autentificación que detallaremos más adelante.

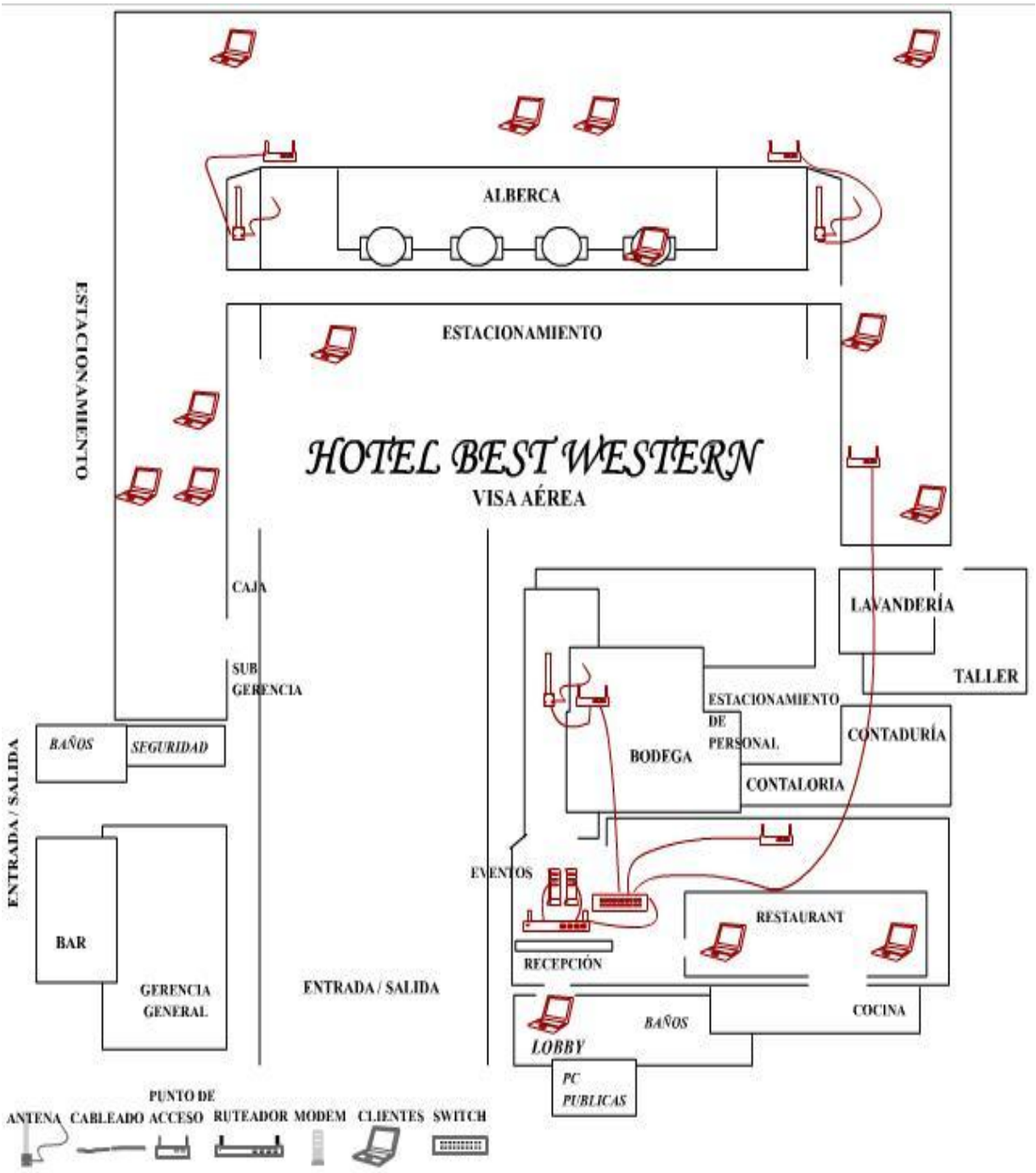
En cuanto a las zonas al aire libre; como el estacionamiento y la alberca del hotel la señal ha sido óptima con una sola antena que he colocado en el edificio central, en la instalación que ocupan como bodega o almacén, la he instalado provisionalmente en la azotea y he dado paseos a alrededores y no he encontrado ningún problema.

Dirigiéndome al área de recepción y restaurante la señal llega con debilidad pero este problema presumo resolverlo colocando el ruteador principal detrás del mobiliario que tienen las recepcionistas y un punto de acceso en el segundo piso, justo arriba del área de comida.

El hotel cuenta con un área llamada “Centro de Negocios” y ofrece Internet alámbrico y abierto a todos sus clientes, si es necesario podría restringirlo y dirigir las puntas destino de ese cableado al ruteador colocado detrás de recepción, pero no lo considero necesario por el momento.

Es así como he planeado y diseñado la instalación de dispositivos a lo largo del hotel y me ayudo de figura 4.2 para su mejor comprensión. Prosigamos con la instalación.

Figura 4.2


ALBERCA
ESTACIONAMIENTO
ESTACIONAMIENTO
HOTEL BEST WESTERN
VISA AÉREA
CAJA
SUB GERENCIA
BAÑOS
SEGURIDAD
ENTRADA / SALIDA
BAR
GERENCIA GENERAL
ENTRADA / SALIDA
LAVANDERÍA
TALLER
ESTACIONAMIENTO DE PERSONAL
BODEGA
CONTADURÍA
CONTALORIA
EVENTOS
RESTAURANT
RECEPCIÓN
COCINA
BAÑOS
LOBBY
PC PUBLICAS
PUNTO DE ACCESO
ANTENA
CABLEADO
RUTEADOR
MODEM
CLIENTES
SWITCH

4.3 Instalación

El punto de acceso se conecta a nuestra red física a través de un cable con terminal o conector RJ45, dado que un cable de este tipo puede tener una longitud de hasta 100 metros disponemos de una gran flexibilidad a la hora de elegir donde colocarlo. Ahora bien, el problema es que para nuestros propósitos necesitábamos añadirle al punto de acceso una antena amplificadora que debimos colocar en el exterior y ésta antena sólo tiene un cable de 1,5 metros, es por ellos que decidí hacer la montura de las mismas como muestro en la figura 4.2.

Una vez hecha la instalación el punto de acceso queda protegido en el interior de la oficina y la antena queda en el exterior sin necesitar ninguna protección ni recubrimiento, sin embargo puede hacerse con una manguera de PVC para exteriores y protegerle de las temperaturas extremas que se pueden alcanzar en la azotea de un edificio. Hay que decir que existen algunos puntos de acceso inalámbricos, mucho más económicos, pero a los que no se pueden añadir la antena amplificadora por lo que a nosotros no nos sería útil.

Elegir el emplazamiento de la antena amplificadora del punto de acceso es algo muy importante. De su buena colocación dependerá el éxito de la instalación, lo ideal es que el emisor y el receptor estén, lo más cercanos posible, a la misma altura y sin obstáculos entre uno y otro como se muestra en la figura haciendo o formando una alineación Delta y no encontrando ninguna interferencia o construcción que nos dificulte la señal.

4.3.1 Probando la calidad de la conexión

Las empresas líderes en hardware suministran un programa con el que además de poder configurar la conexión de los adaptadores podemos probar la calidad de la misma. Con las especificaciones IEEE 802.11b (2.4 GHz ISM spectrum), la de los equipos que he enumerado anteriormente, la velocidad máxima alcanzable es de 11Mbps, si la conexión no es muy buena pasará a las 5Mbps, luego a las 2Mbps y finalmente a 1Mbps.

Personalmente en su momento he pensado que incluso una conexión a 1Mbps sería suficiente, pero no lo es ya que es una conexión de muy baja calidad que no te permite trabajar ya que se corta, vuelve a conectarse... tal vez para utilizar el Internet bastaría pero para poco más.

Lo mínimo aceptable para trabajar es una conexión a 5Mbs, con ella puedes abrir una base de datos Access y trabajar relativamente rápido. Lógicamente lo mejor es conseguir 11Mbs de conexión.

Para encontrar la posición adecuada del adaptador lo mejor es conectarlo a un portátil e ir haciendo pruebas en distintas posiciones al mismo tiempo que

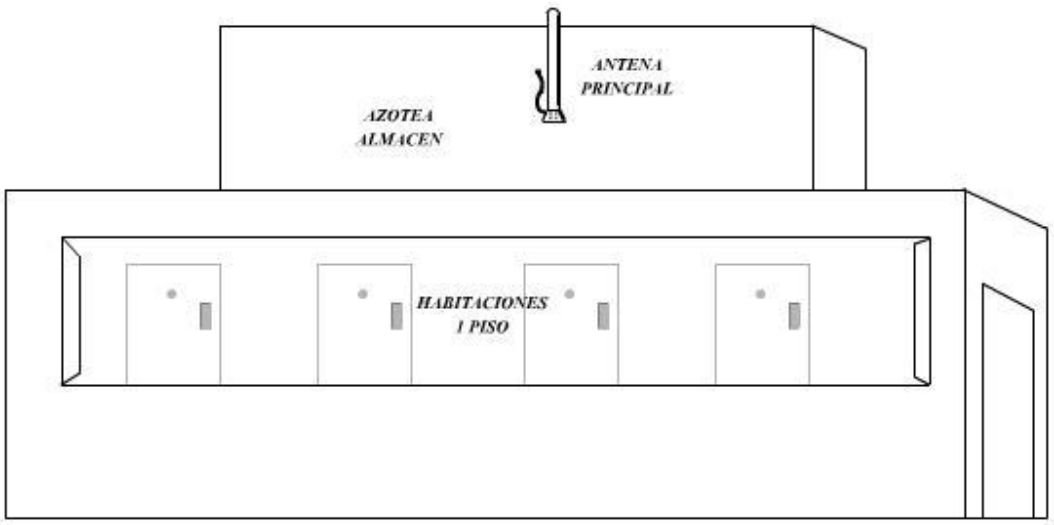
se hacen “test” con el programa que nuestro proveedor nos proporciona. La posición del dispositivo influye; incluso pudimos comprobar que por un lado recibe mejor que por otro.

4.3.2 Montando la Red

Ayudándonos de la figura 4.3 empecemos entonces con el montaje de la antena principal en la azotea del almacén, ésta estará conectada a un punto de acceso en la parte posterior del mismo edificio, al encontrarse en el interior estará a salvo de los cambios climatológicos que pueda haber y por protección he solicitado un regulador de corriente.

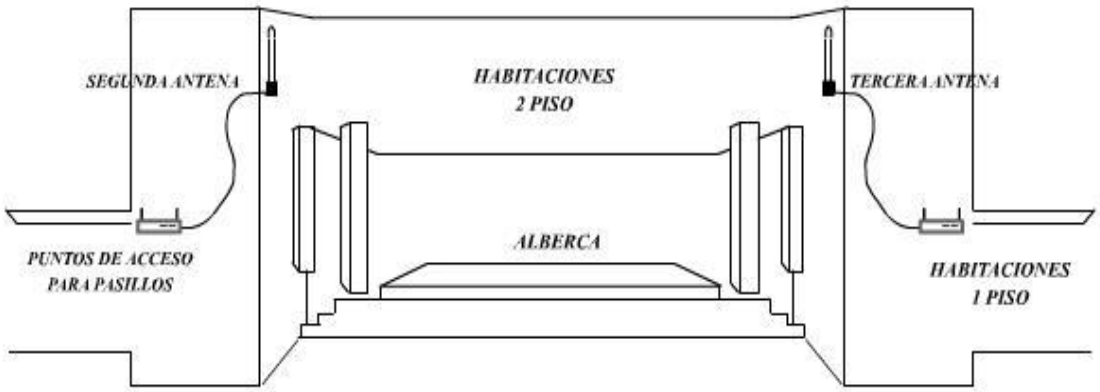
Es importante enfatizar la importancia de esta primera antena, pues se convierte en la líder al ser la única que tendrá conexión directa con el switch que a su vez conectará con el ruteador. Si algo llegara a pasarle se caerá igualmente el servicio de las restantes, al terminar el WDS que planeo configurar en ellas.

Figura 4.3



La segunda antena será instalada a un lado superior izquierdo de la alberca, acariciando la planta alta del edificio y se conectará a un punto de acceso que hay en la planta baja a no más de 2 metros de distancia y que se ubica estratégicamente en el pasillo que hace esquina en el edificio de mayor tamaño, repartiendo así la señal por el primer nivel y dejando que el amplificador se encarga de las habitaciones que se encuentran a una mayor altura como vemos en la figura 4.4.

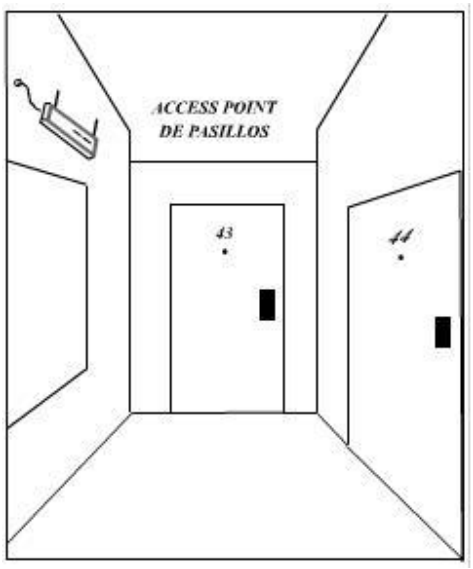
Figura 4.4



La tercera y última antena se colocará a un lado superior derecho de la alberca, exactamente a la misma altura de la segunda y cubriendo geográficamente las mismas habitaciones que su similar y cumpliendo sus mismas funciones, recordemos que la segunda y ésta tercera antena no tendrán conexión alámbrica alguna exceptuando el enlace de antena a access point por conexión coaxial y la señal que ambas apunten a la “líder” culminará con una interconexión WDS.

Los puntos de acceso que se sitúan en los pasillos cumplirán su función de ampliar o hacer llegar la señal a lugares donde ninguna de las antenas mayores reparten una posibilidad fuerte de conexión. Véase en la figura 4.5 que esos access point se encuentran ocultos tras múltiples paredes de gran grosor haciendo muy pobre la intensidad en el área de suites.

Figura 4.5

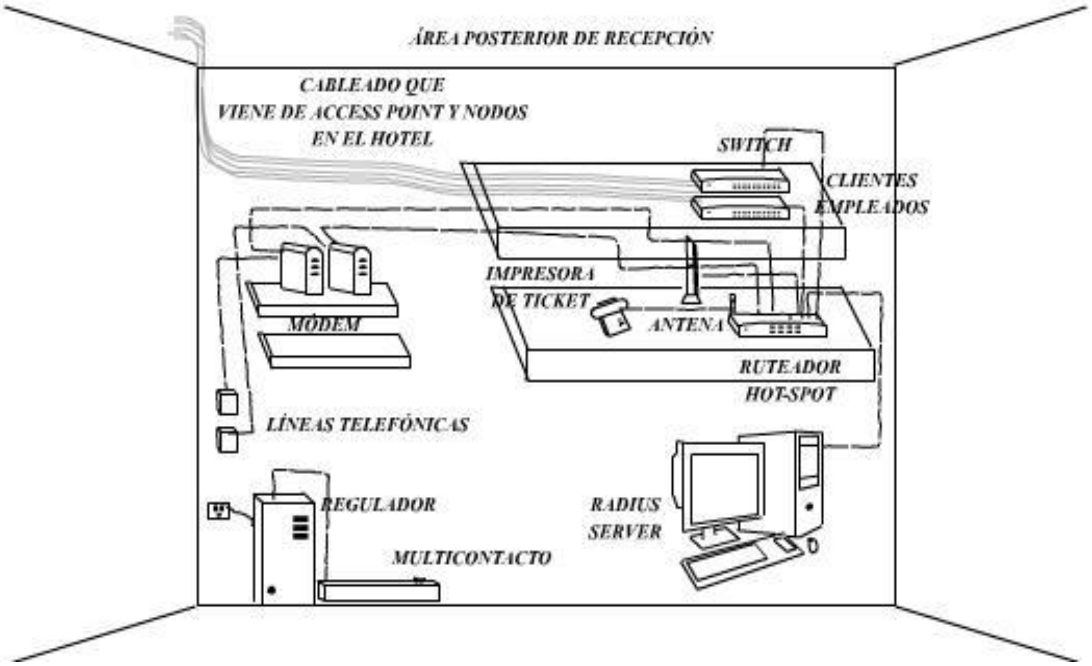


Todos y cada uno de los puntos de acceso (exceptuando los que se encuentran al costado de la alberca) conectan directamente por cable vía RJ45 al switch que a su vez conecta al ruteador, este también hace función de access point y reparte señal al área del lobby y restaurante.

Se conectarán dos módem en el ruteador, que por su modelo soporta hasta cuatro, teniendo así un ancho de banda superior que se pueda distribuir tanto al personal del hotel como a los clientes del mismo, cada uno de ellos con velocidad de transferencia de 1mb.

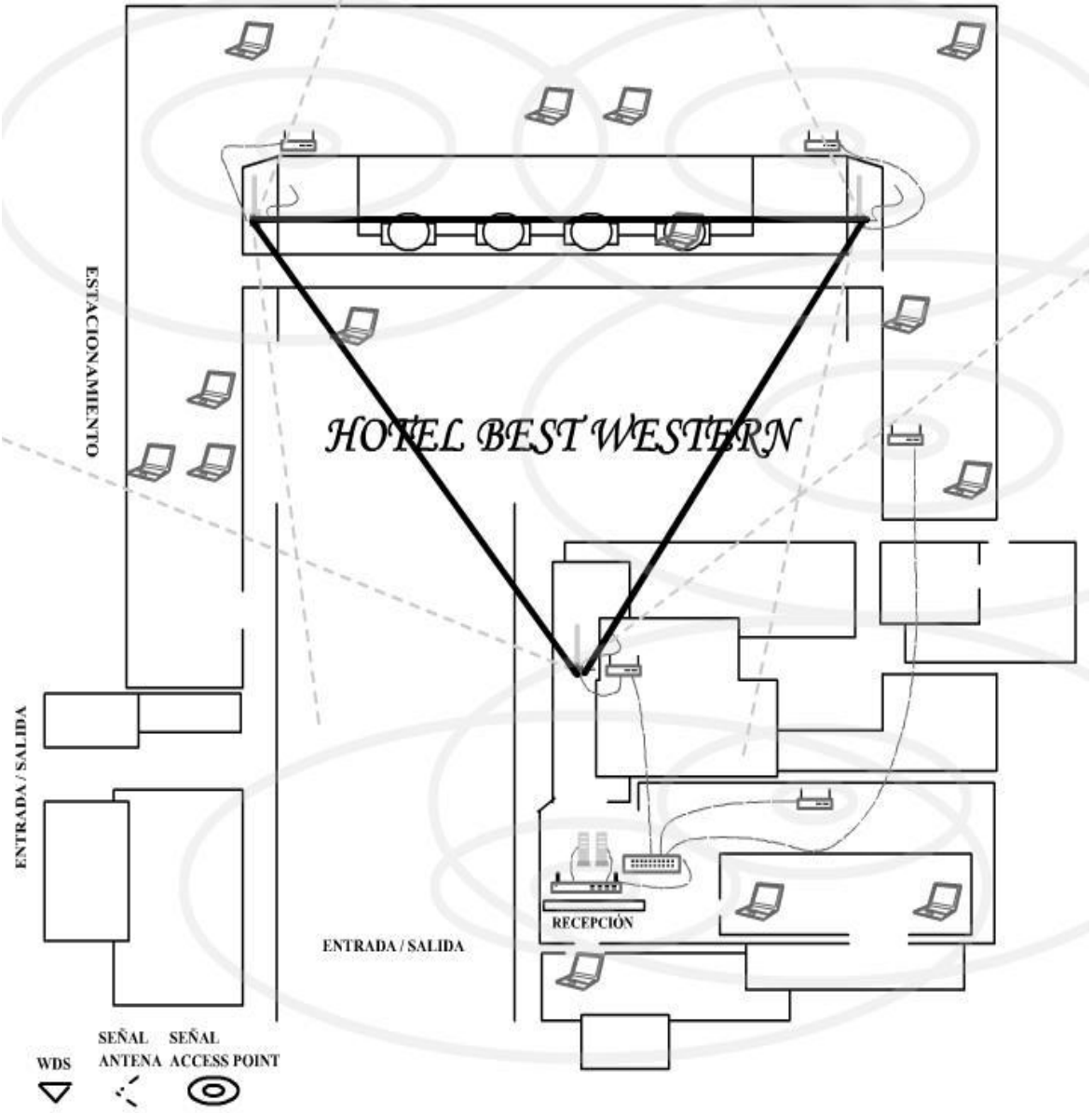
Finalmente también conectado al ruteador o puerta de enlace encontraremos una impresora de tickets que ya he redactado y explicado su funcionamiento en capítulos anteriores.

Figura 4.6



Así se realizará la implementación de dispositivos en las instalaciones del hotel Best Western, enfocando o situando cada uno de ellos a manera de que la señal WI-FI emitida sea lo suficientemente fuerte y constante para cualquier cliente en prácticamente cualquier punto o localidad del mismo como muestro en la figura 4.7.

Figura 4.7


HOTEL BEST WESTERN
ESTACIONAMIENTO
ENTRADA / SALIDA
RECEPCIÓN
ENTRADA / SALIDA
WDS
SEÑAL ANTENA
SEÑAL ACCESS POINT

4.4 Configuración

Ahora que tenemos una conexión inalámbrica a la red y la complejidad asociada, existen potencialmente muchos otros elementos que necesitan configurarse. Por ejemplo, es posible que necesitemos configurar el SSID de la red a la que nos estamos conectando. O, podemos necesitar configurar un conjunto de claves WEP de seguridad, posiblemente con varios conjuntos si tenemos varias redes a las cuales conectarnos. Es posible que necesitemos tener una configuración para trabajar en donde haya una red operando en modalidad de infraestructura y una configuración para el hogar cuando operamos en una modalidad ad-hoc. Por lo tanto, es posible que necesitemos seleccionar cuál de estas configuraciones se tiene que usar, con base en el lugar en que estemos en un momento dado.

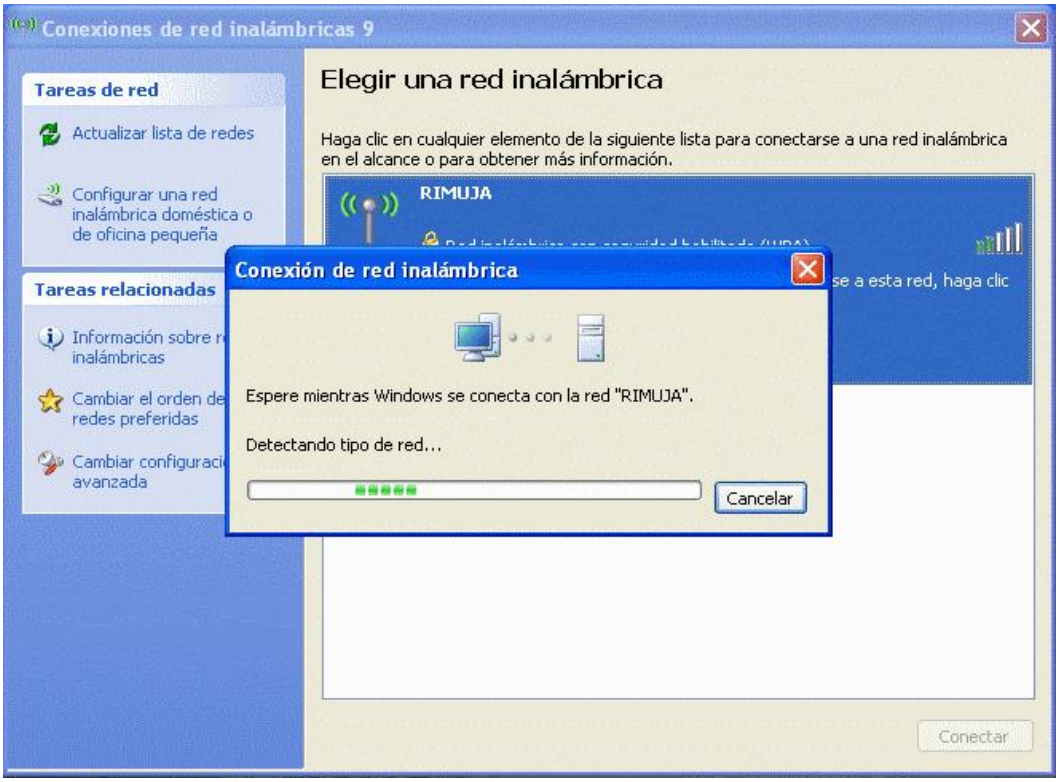
4.4.1 Tarjeta de red

Hablaré de la configuración en general que debería tener una tarjeta de red inalámbrica en un ordenador o equipo portátil con Windows XP, pues no se requerirá mayor asistencia técnica en cada cliente del hotel para ello, sólo detallaré los pasos para habilitar la encriptación WEP y decir que es importante que la NIC tenga habilitada el DHCP (IP automática) para poder conectarse a Internet.

Figura 4.8

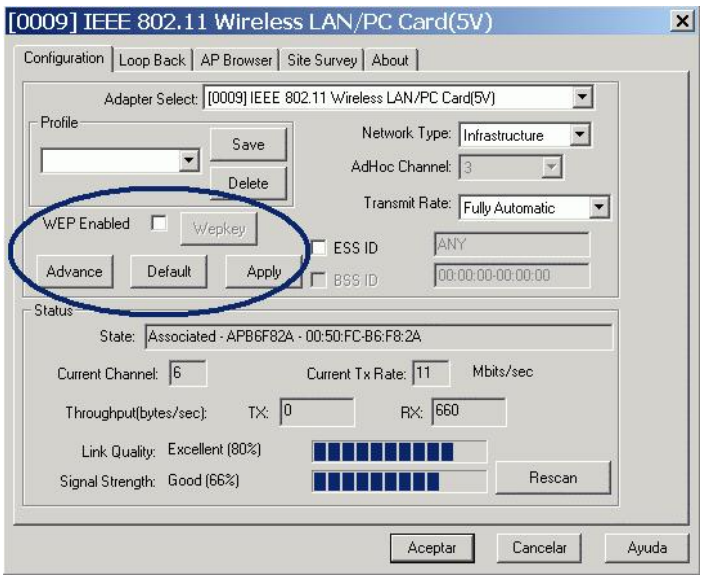
Desde el Icono de detección de red inalámbrica en la bandeja del sistema. Está disponible para todos los equipos con tarjeta WIFI integrada o PCMCIA (siempre que la tarjeta esté habilitada y activada la opción que la muestra en la bandeja del sistema). Se hace un clic con el botón derecho y se selecciona la opción Abrir conexiones de red. Esto visualiza la ventana de Conexiones de red disponibles en el equipo. Véase figura 4.9.

Figura 4.9



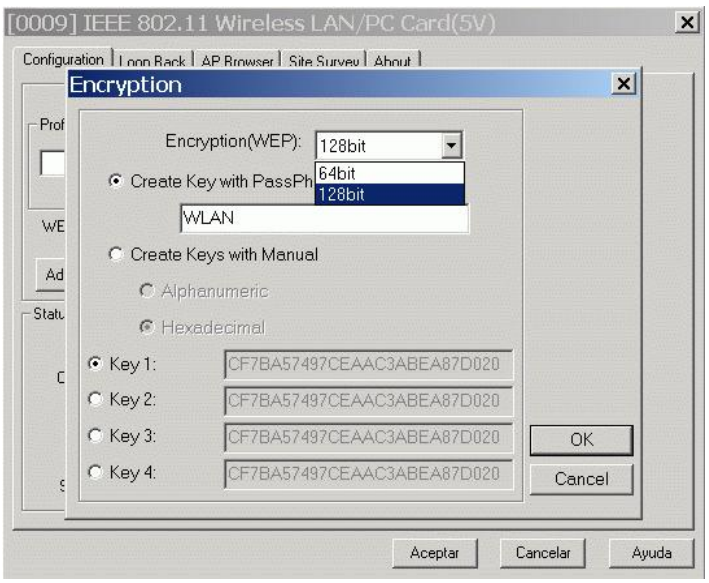
En cuanto a seguridad WEP básicamente es la encriptación de nuestros datos o paquetes enviados por nuestra red, esto añade cierto grado de seguridad para evitar intrusos en nuestra red. Muchos usuarios son reacios al uso del WEP ya que se ha demostrado que el cifrado puede ser ineficaz en algunas ocasiones, pero también puede ser un gran muro de seguridad si se realiza con ciertas reglas de uso.

Figura 4.10



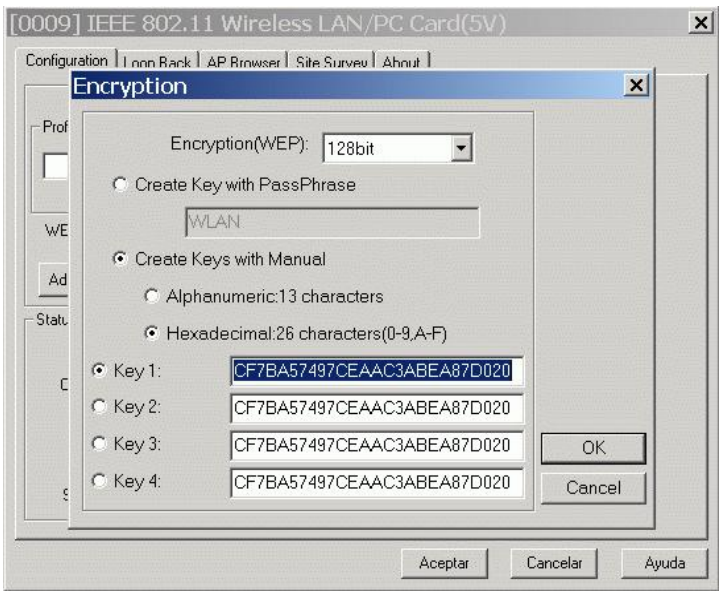
Activamos la opción WEP Enabled.

Figura 4.11



Seleccionamos el tipo de encriptación que queremos usar, la codificación puede ser mas o menos segura dependiendo del tamaño, 64 Bits o 128 Bits.

Figura 4.12



Marcamos la casilla de 128 Bits esto aportará mayor seguridad a nuestra red, también podemos escoger entre una clave alfanumérica (13 caracteres) o hexadecimal (26 caracteres 0-9/A-F), no todos los modelos de redes inalámbricas soportan estas opciones. Si queremos una buena seguridad se recomienda usar una llave (Key 1 - Key 2 - Key 3 - Key 4) por día o por semana, cambiando las claves cada mes, esto aporta un grado de seguridad mayor y hacemos que nuestro futuro intruso tenga que trabajar mas en el intento de sacar o descodificar nuestros paquetes que circulan por nuestra red inalámbrica.

Estos consejos son para hacer una red inalámbrica un poco mas segura y se aplica a la tarjeta de red personal en una instalación más hogareña que empresarial pero es importante hacer este aborde del tema para comprender referencias futuras.

4.4.2 Puntos de acceso

Antes de empezar a configurar el Access Point, debemos mirar si la versión del Firmware del Access Point es la última o la más adecuada para el dispositivo.

Una ves que tengas el Access Point, necesitas cambiar las opciones por defecto para ser compatibles con la red de Best Western Brisas. Las opciones que debes cambiar son las siguientes:

SSID: Cambiarlo por "Best Western Brisas"

WEP: Desactívalo. Lo hacemos por ampliar la compatibilidad del Hardware en la red. Una red con el WEP activado supone que todas las tarjetas deben funcionar al mismo nivel de cifrado. Esto es útil en una empresa donde todos los empleados usen el mismo Hardware, pero no en nuestra situación donde cada uno tendrá el Hardware que quiera. La encriptación correrá a cargo del ruteador Hostspot SMC que planeo instalar.

Nombre: Aquí pon el nombre de tu nodo. Los nombres de los Nodos en Best Western Brisa no son aleatorios, tienen relación con la situación física del mismo.

Situación: Pon tu dirección si lo deseas.

Canal: Observa los nodos mas cercanos a ti y escoge el canal menos usado. Date cuenta que solo hay 3 canales que no se solapan, debes escoger entre el 1, el 6 ó 11 para evitar el solapamiento.

Password: Muchos Access Point tienen passwords para cambiar las opciones de configuración. Escoge uno adecuado para que nadie pueda entrar en el Access Point y modificar las opciones.

DHCP: Tu Access Point o la red en la que este conectado debe correr un servidor DHCP para proporcionar direcciones IP adecuadas.

4.4.2.1 Crear la interconexión WDS

En la Web de configuración del PA, en Setup, Basic Setup.

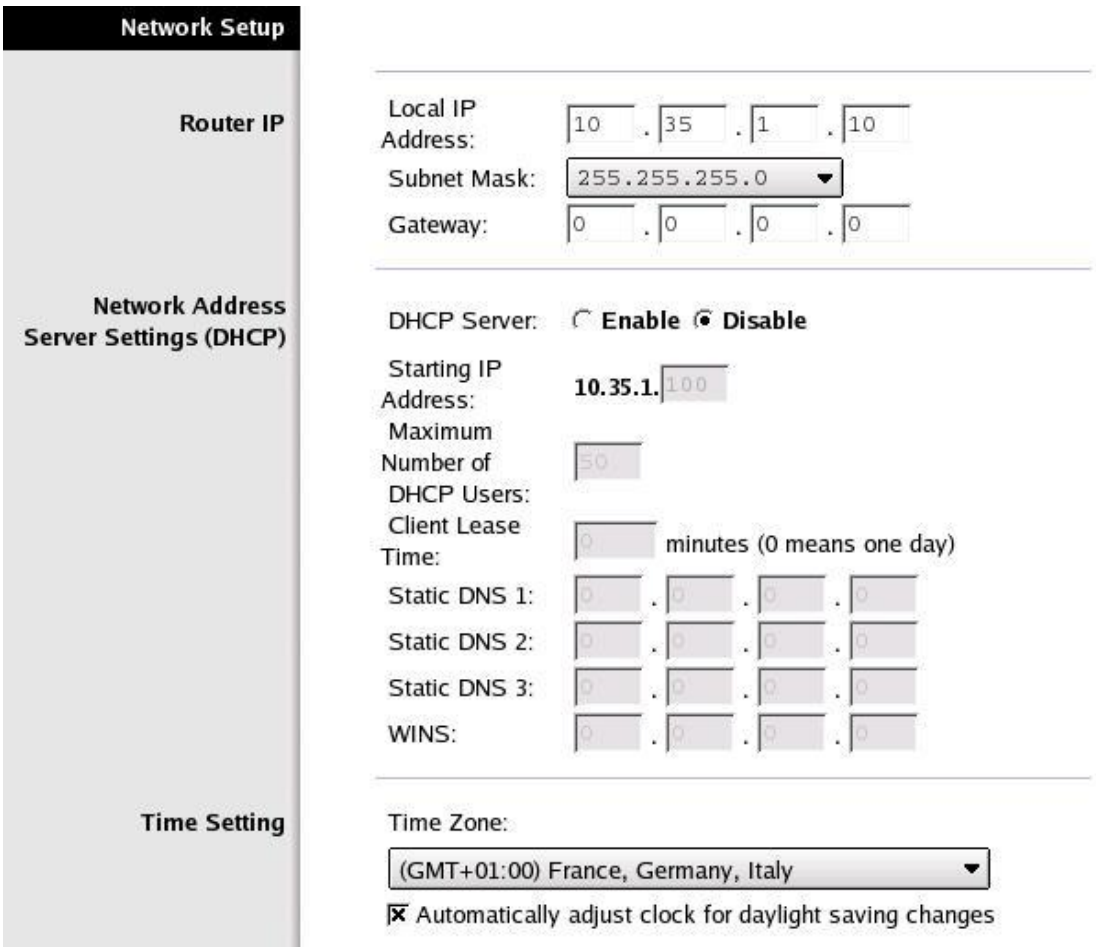
1 - En Router IP, pondremos la IP y máscara de red de nuestra red local (hay que recordar que hay que escoger una IP que esté libre dentro de nuestra red), la puerta de enlace (Gateway) no hace falta ponerla.

2 - Desactivaremos el servidor DHCP si es necesario. El servidor DHCP lo que hace es asignarnos una dirección IP automáticamente y por tanto como vamos a conectar varios PA con uno solo que lo tenga activado ya nos basta. Incluso si nuestro router ADSL ya tiene un servidor DHCP entonces podemos desactivarlo en todos los PA. En resumen: solo debemos tener un servidor DHCP.

3 - Time Setting, lo podremos en la zona horaria de nuestro país (GMT +6 México).

Pulsaremos en el botón de abajo donde dice: Save Settings.

Figura 4.13



Vamos al menú Wireless, Basic Settings:

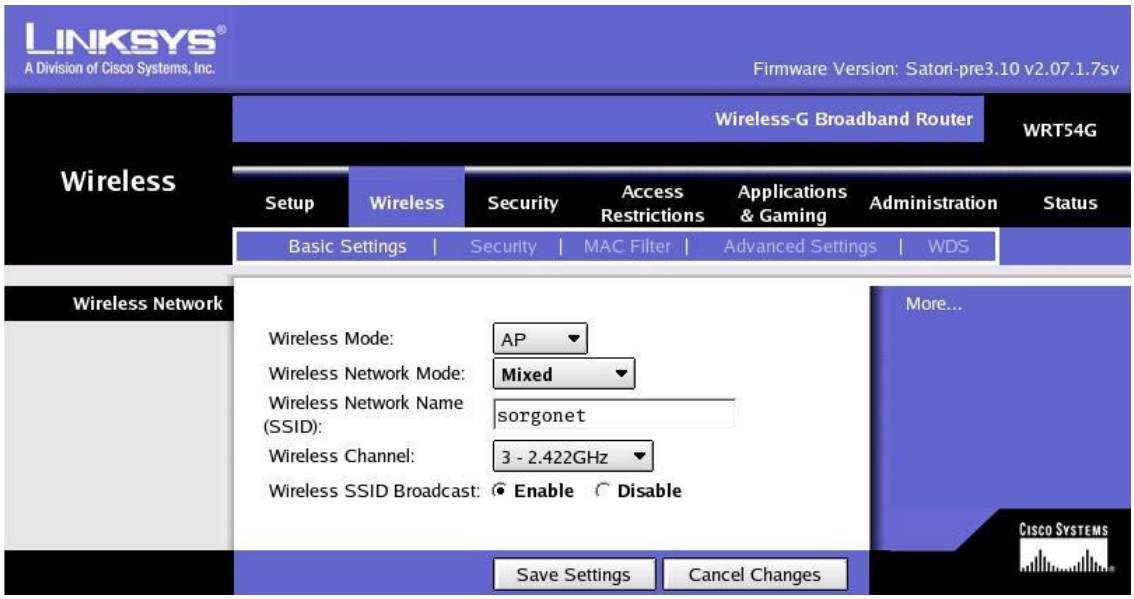
1.- En Wireless Mode seleccionaremos AP.

2.- Wireless Network Name (SSID) el nombre que queramos para nuestro nodo Wireless. (Es lo que verán los que quieran conectar)

3.- Wireless Channel, el número de canal para usar en la comunicación.

4.- Save Settings.

Figura 4.14



Es muy importante tener en cuenta que hay que poner el mismo número de canal (Wireless Channel) en todos los PA dónde queramos instalar WDS. El SSID puede ser diferente y yo lo aconsejo, ya que así siempre sabremos exactamente a que PA estamos conectados, sino tendríamos que guiarnos por las MAC.

En el menú Wireless, Advanced Settings:

1.- La última opción Xmit Power: (Potencia de Transmisión) por defecto viene a 28mW y como máximo se puede poner a 84mW, como la legislación actual permite hasta 100mW lo podemos poner por ejemplo a 75mW para llegar más lejos.

Algunos dicen que ponerlo a 84 Mw. es una locura porque se quema el chip, yo puedo decir que llevo varios meses teniéndolo al máximo 84mW y no se ha colgado nunca. Eso si, cuantos más Mw. más energía consume y más calor desprende. Por eso 75 Mw. me parece un buen valor para los más prudentes.

2.- Dejaremos la opción WDS para más adelante.

En el Menú Security, Firewall:

1 - Firewall Protection, marcaremos: Disable.

2 - Desactivar la casilla Block Anonymous Internet Requests.
Esto es importante para que el WDS funcione.

Figura 4.15

Volvamos ahora a la configuración WDS.

Menú Wireless, WDS.

1.- En Wireless WDS, activamos la primera de las 10 entradas seleccionando P2P y ponemos la dirección MAC del PA al cual queremos conectar (recuerda que esta dirección MAC la hemos buscado antes y es la del Wireless)

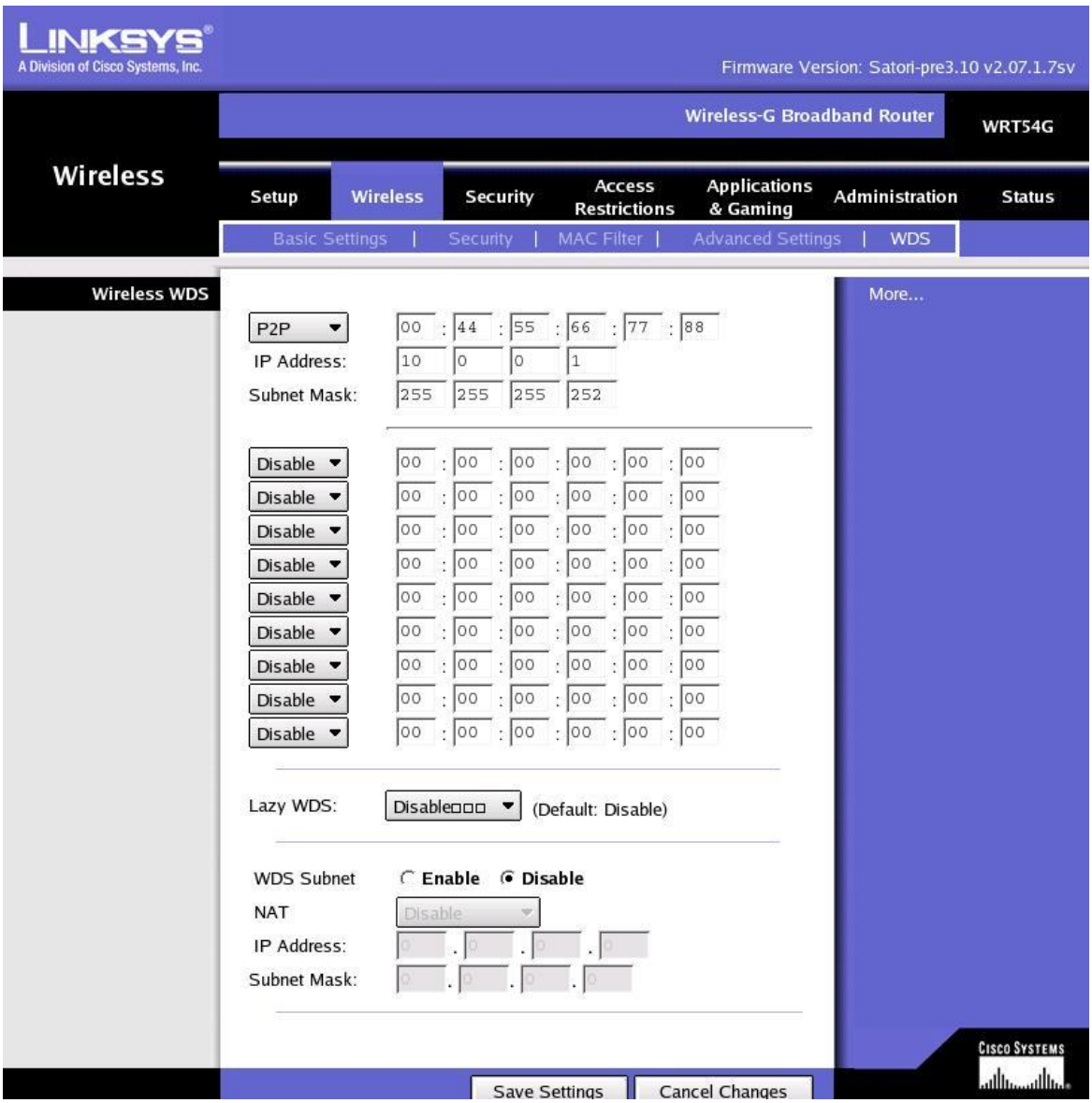
2.- En IP Address pondremos una dirección virtual (o sea inventada) que se le asignará al interfase WDS, podemos usar una dirección del tipo 10.0.0.x ya que seguro que no coincide con ninguna de Internet. Esta dirección será diferente en cada uno de los PA que queramos conectar. Por ejemplo 1er PA: 10.0.0.1, 2do: 10.0.0.2, 3er 10.0.0.3 y así sucesivamente.

3.- En Subnet Mask pondremos 255.255.255.252 hay que decir que es necesario usar ésta concretamente para que funcione.

4.- Lazy WDS lo pondremos en Disable.

5.- WDS subnet en Disable también.

Figura 4.16



La idea es encadenar los PA de manera que, como en la siguiente imagen, se conecten como si fueran vagones de un mismo tren, para eso en el primer PA solo habrá una interface WDS (10.0.0.1) en el segundo deberemos tener 2 ya que el (10.0.0.2) conectará con el primero y (10.0.0.3) con el tercero. He configurado hasta 6 WRT54G entre ellos sin ningún problema con esta técnica.

Figura 4.17

Una vez hecho todo esto no es suficiente para que funcione todavía, ahora hay que entrar vía telnet al aparato y ejecutar algunos comandos.

Para activar el telnet, iremos al menú Administration, Management, buscaremos Telnet y lo pondremos en Enable. Pulsaremos en Save Settings.

En Linux iremos a una consola o en Windows a inicio ejecutar, command y teclearemos:

Telnet 192.168.1.1, si es que esa es la IP actual del WRT54G.

Nombre de usuario es: *root* y password si no lo has cambiado será: *admin* sino será el mismo que hayas puesto en la Web de configuración.

Ahora hay que añadir al bridge la interface WDS, para comprobar que esa interface está configurada, podemos teclear ifconfig donde saldrán varios datos y beberían estar también el wds0.2 (si lo has configurado dos o más saldrían también: wds0.3, wds0.4 ...)

Nota: En mis pruebas en uno de los 6 PA con el que había jugado con varios firmwares diferentes no salía esa interface, tuve que ir a la Web oficial de Linksys, descargar el firmware de fábrica, poner los valores por defecto, volver a meter el Firmware Satori y configurarlo todo de nuevo.

Para añadir la interface wds0.2 en el bridge br0 el comando es:

~ # <>brctl addif br0 wds0.2

Esto lo haríamos en todos los PA, y en los que hayamos configurado dos interfaces WDS (o sea todos menos el primero y el último de la cadena) habrá que añadir también el wds0.3 con el comando:

~ # <>brctl addif br0 wds0.3

Ahora ya debería funcionar el enlace WDS entre todos los PA, podemos ir al menú Status, Wireless y allí ver la calidad de la señal en cada uno de los enlaces WDS.

Para comprobar que ha funcionado podemos ejecutar el comando:

~ # <>brctl showbr br0

Con lo que veremos los interfaces que están dentro del bridge y deberían aparecer los wds0.2 o wds0.3 según el caso.

Si algo no ha funcionado, pues habrá que repasarlo todo, sobretodo no nos equivoquemos en las direcciones MAC al meterlas en el apartado WDS de la configuración Web.

Ojo que todavía no hemos terminado.

Tal cual está ahora todo esto, al irse la corriente o reiniciar el WRT54G, deberemos volver a entrar vía telnet y ejecutar los comandos de nuevo. Para evitar esto y que estos comandos se ejecuten automáticamente al encender el router, deberemos volver a entrar por telnet y añadir los comandos al script que se ejecuta cada vez que arranca el PA.

Si solo tenemos una interface WDS, el comando es:

~ # nvram set rc_startup='/usr/sbin/brctl addif br0 wds0.2'

~ # nvram commit

Si tenemos dos interfaces WDS:

~ # nvram set rc_startup="/usr/sbin/brctl addif br0 wds0.2;/usr/sbin/brctl addif br0 wds0.3"

~ # nvram commit

Si tenemos más, hay que saber que el punto y coma separa los comandos y que nvram commit lo que hace es grabar las variables de sistema.

Atención porque hay que poner el /usr/sbin/brctl al escribir los comandos, ya que si ponemos tan solo brctl, como al iniciar el router y ejecutar ese comando todavía no tiene el path asignado, no funcionaría.

Para comprobar que está bien grabado:

~ # nvram show |grep startup

Ya podemos reiniciarlo con el comando reboot por ejemplo o desconectarlo de la corriente y volverlo a conectar.

Ahora si que ya tendríamos los WRT54G funcionando en WDS perfectamente.

4.4.3 Hotspot.

El Hotspot Gateway de 2.4GHz y de 802.11 es una solución multifuncional, "todo-en-uno" que ofrece:

1) Acceso seguro a Internet.

2) Acceso inalámbrico de alta velocidad dentro de una red de área local. (LAN).

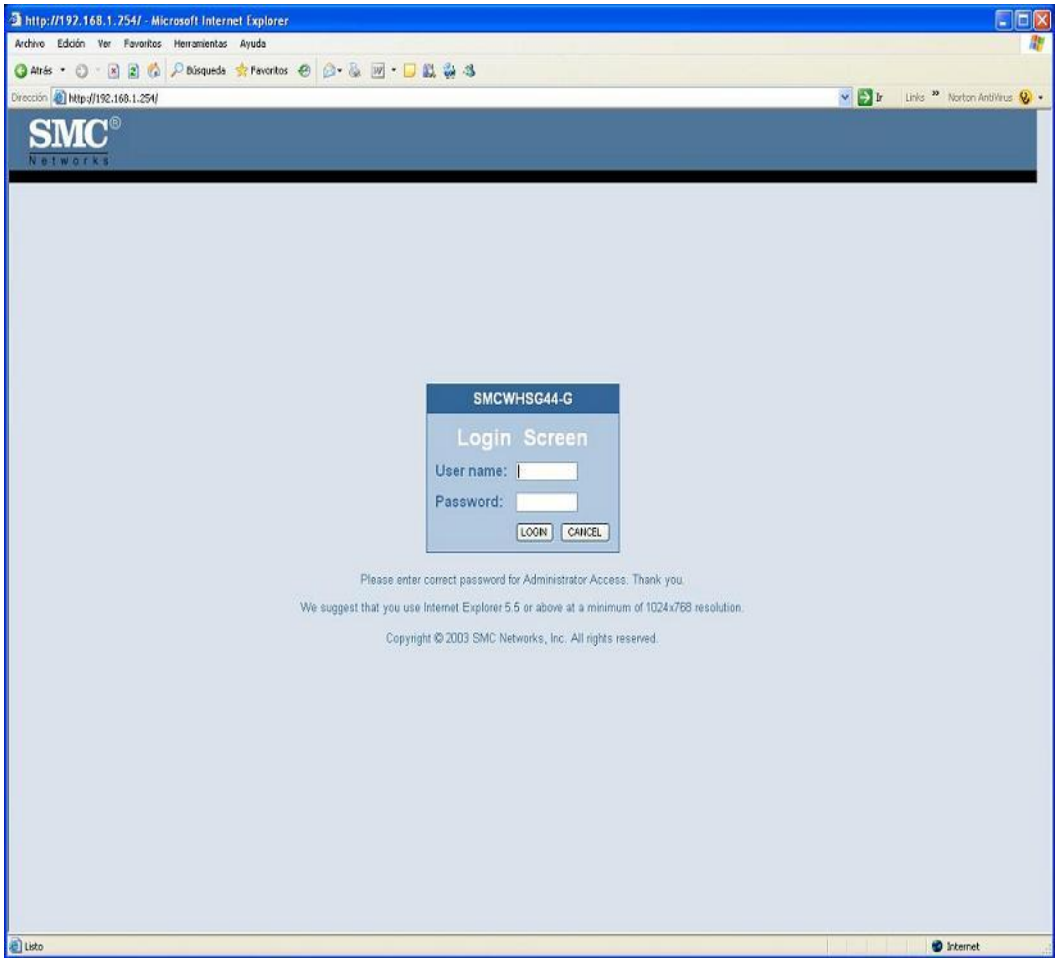
3) Servicios de autentificación, autorización y gestión de cuentas para clientes inalámbricos o cableados.

4) Soporte para la impresión de recibos/facturas de punto de venta. Como un módem/gateway de xDSL/cable el Hotspot, ofrece una combinación de hasta 4 puertos LAN o 4 puertos WAN. Además, un puerto LAN soporta POE (power-over-ethernet) compatible con 802.11af.

Los puertos WAN ofrecen hasta 4 conexiones xDSL/Cable módem o se pueden emplear para out-bound load-balancing y para añadir ancho de banda. También se pueden configurar los puertos WAN para ofrecer un enlace redundante para asegurar que la conexión se mantenga siempre online. El gateway soporta una amplia gama de prestaciones de seguridad como NAT, firewall SPI, y filtrado de direcciones MAC para garantizar un entorno seguro de Internet.

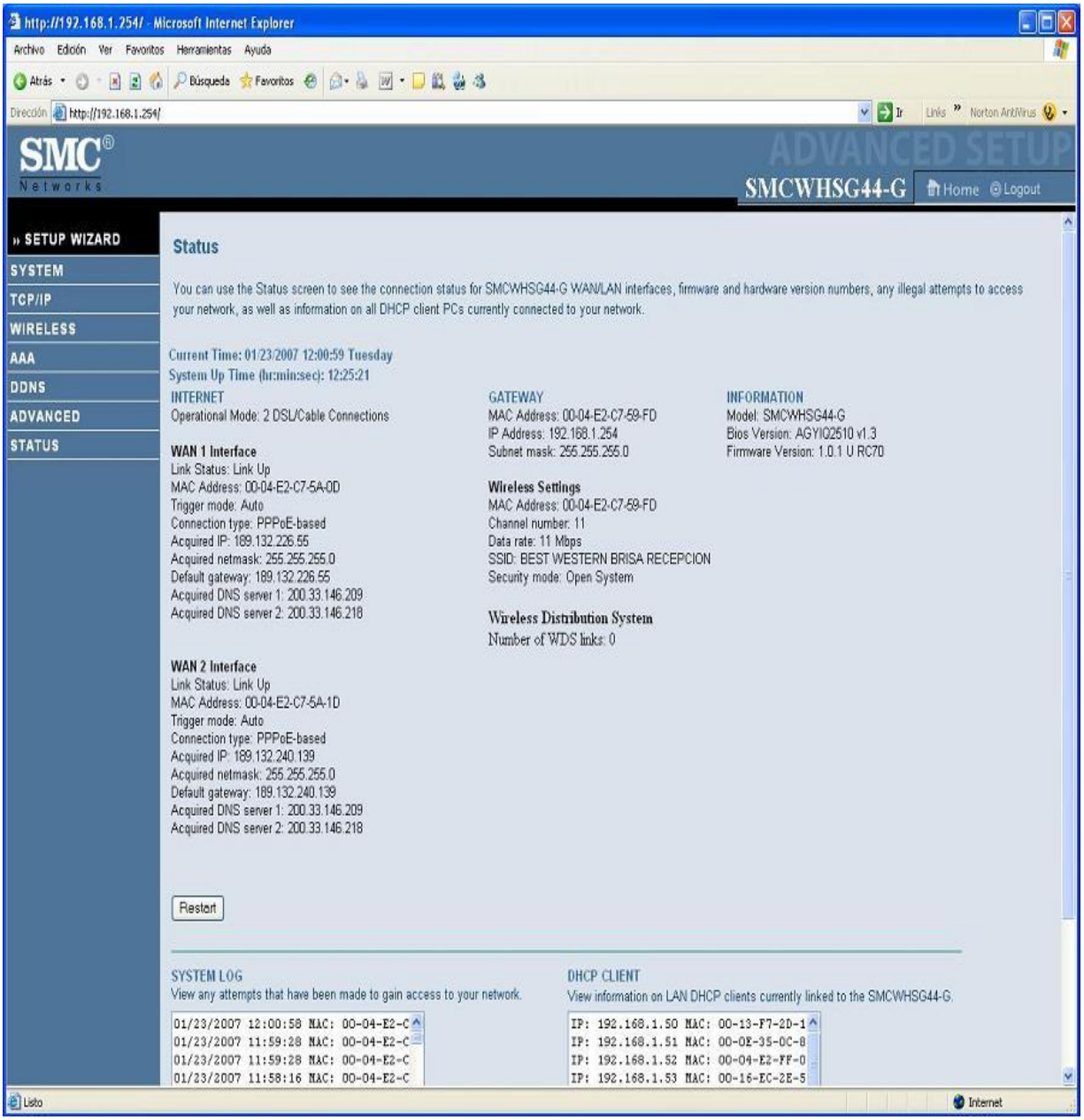
En cuanto a seguridad de nuestra red inalámbrica toda será administrada por este ruteador o puerta de en lace cubriendo los algoritmos de cifrado: WEP de 128 bits, encriptación de 64 bits WEP, TKIP, WPA y con su método de autentificación RADIUS.

Figura 4.18



En la pantalla de bienvenida pondremos nuestro usuario y contraseña de administradores para acceder a la configuración avanzada. La dirección por dafault en ésta que llamaremos nuestra puerta de enlace será 192.168.1.254 y podemos ingresar vía HTTP (desde nuestro explorador de Internet).

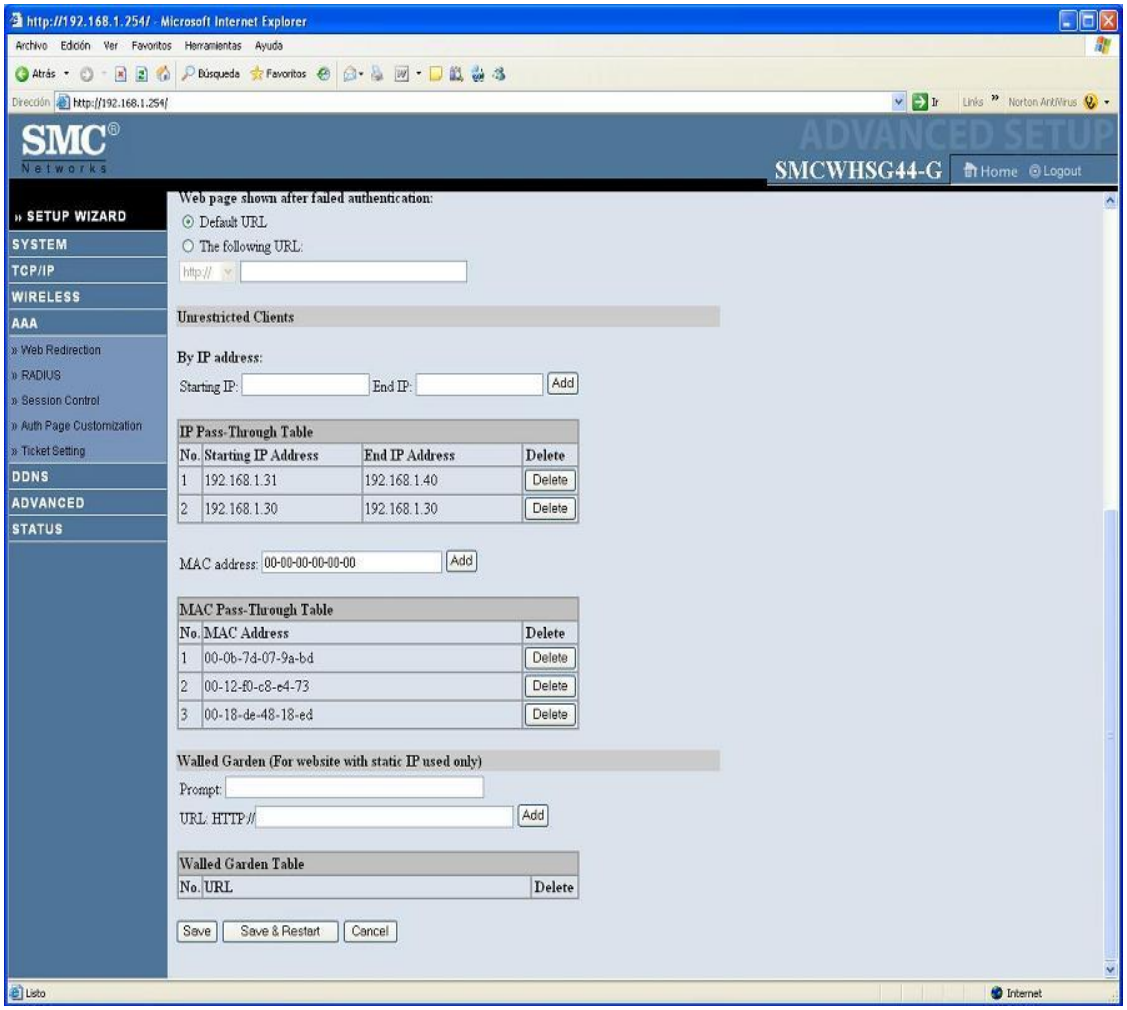
Figura 4.19



En la pantalla de status veremos las condiciones actuales o en tiempo real de nuestras conexiones a Internet (que en este caso con 2 de ellas a 1 MB cada una) que se han repartido a los huéspedes y a los empleados del hotel respectivamente.

Veremos aspectos generales como la IP de la puerta de enlace y dirección de hardware (MAC address) de cada dispositivo conectado físicamente y un Log o registro de entradas a nuestra red.

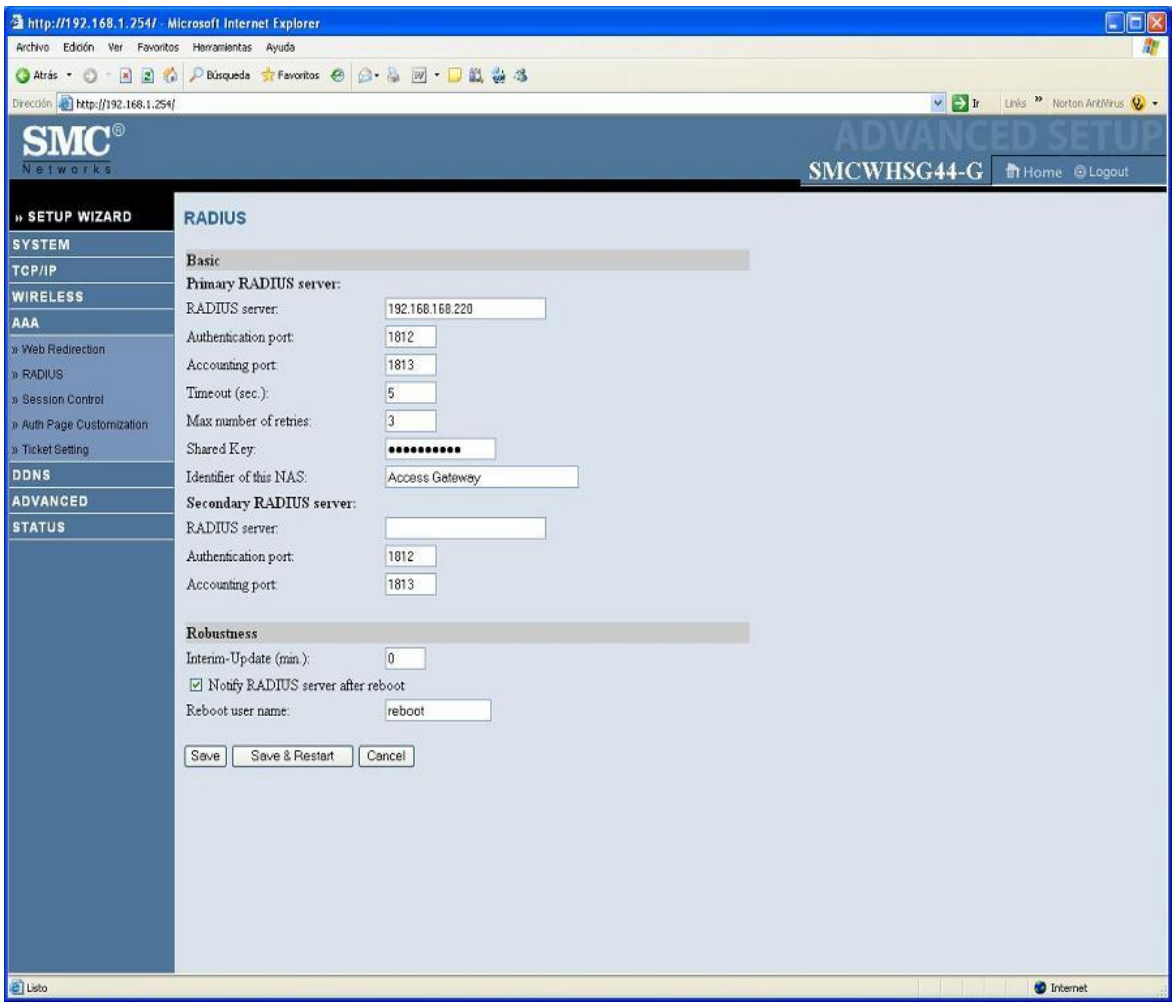
Figura 4.20



En la ventana de AAA (Administración Avanzada de Autenticidad) colocaremos las IP o las MAC address de los equipos que tendrán acceso directo y sin restricciones al Internet. Este apartado es para clientes especiales o constantes que ya no necesitarían un ticket temporal para conectarse y principalmente para los empleados del Best Western que tendrían una conexión fija.

Pueden identificarse con la base de datos del Hotspot por dirección IP o dirección de hardware.

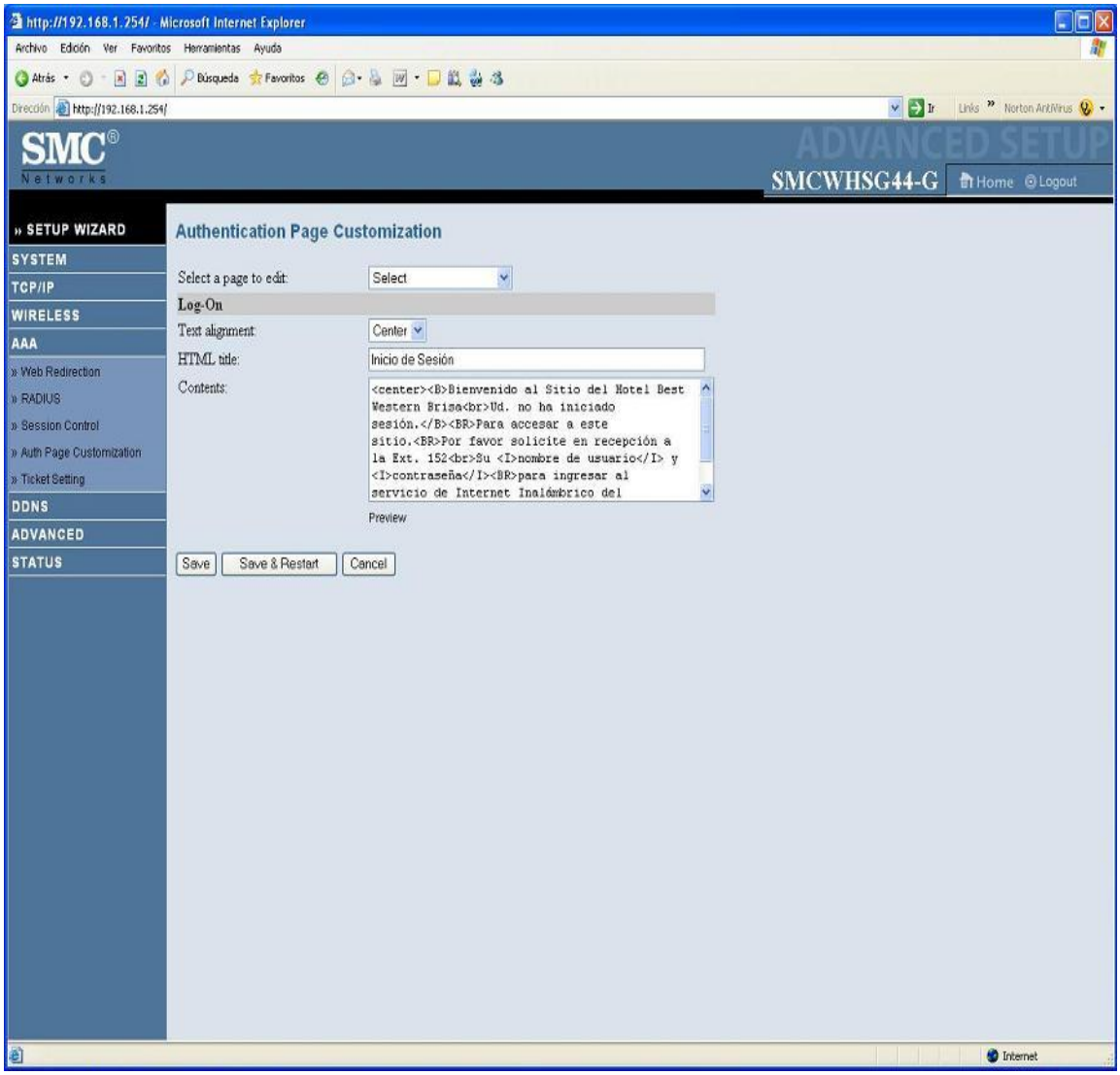
Figura 4.21



El Hotspot maneja su propio método de autentificación RADIUS que he detallado en segmentos anteriores, así mismo contiene la opción de vincular o mapear su base de datos con una máquina ajena o servidor del mismo tipo, es en esta pantalla donde se manda a llamar colocando la dirección IP y los puertos así como la contraseña de acceso e incluso manejar un secundario

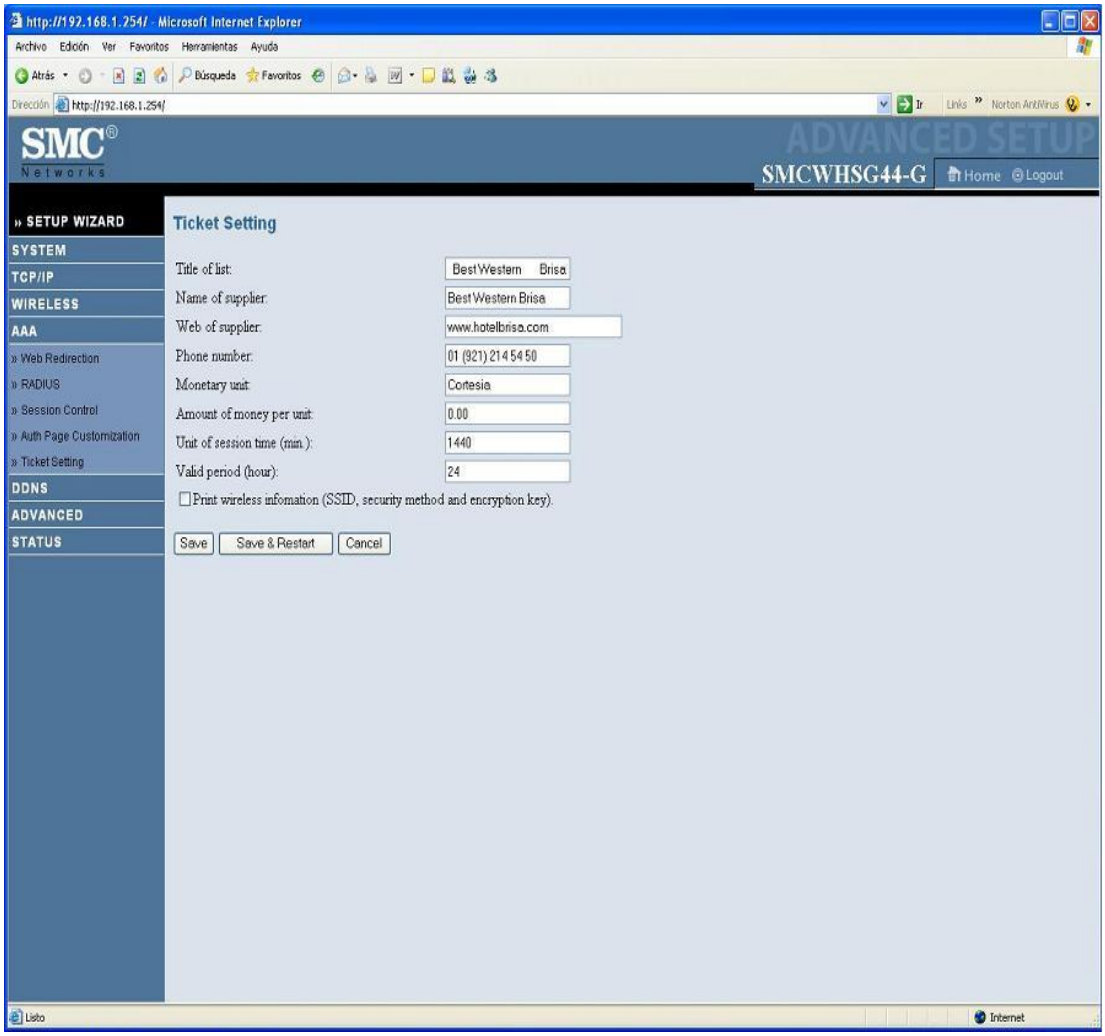
Esta opción es por demás interesante, sin embargo por los costos y configuraciones ajenas a nuestro proyecto no detallaré más.

Figura 4.22



En la ventana de *Authentication page customization* se usará lenguaje HTML para editar la pantalla de bienvenida en el explorador de Internet. El texto que se inserte aquí será mostrado al huésped una vez q trate de ingresar a una página de Internet.

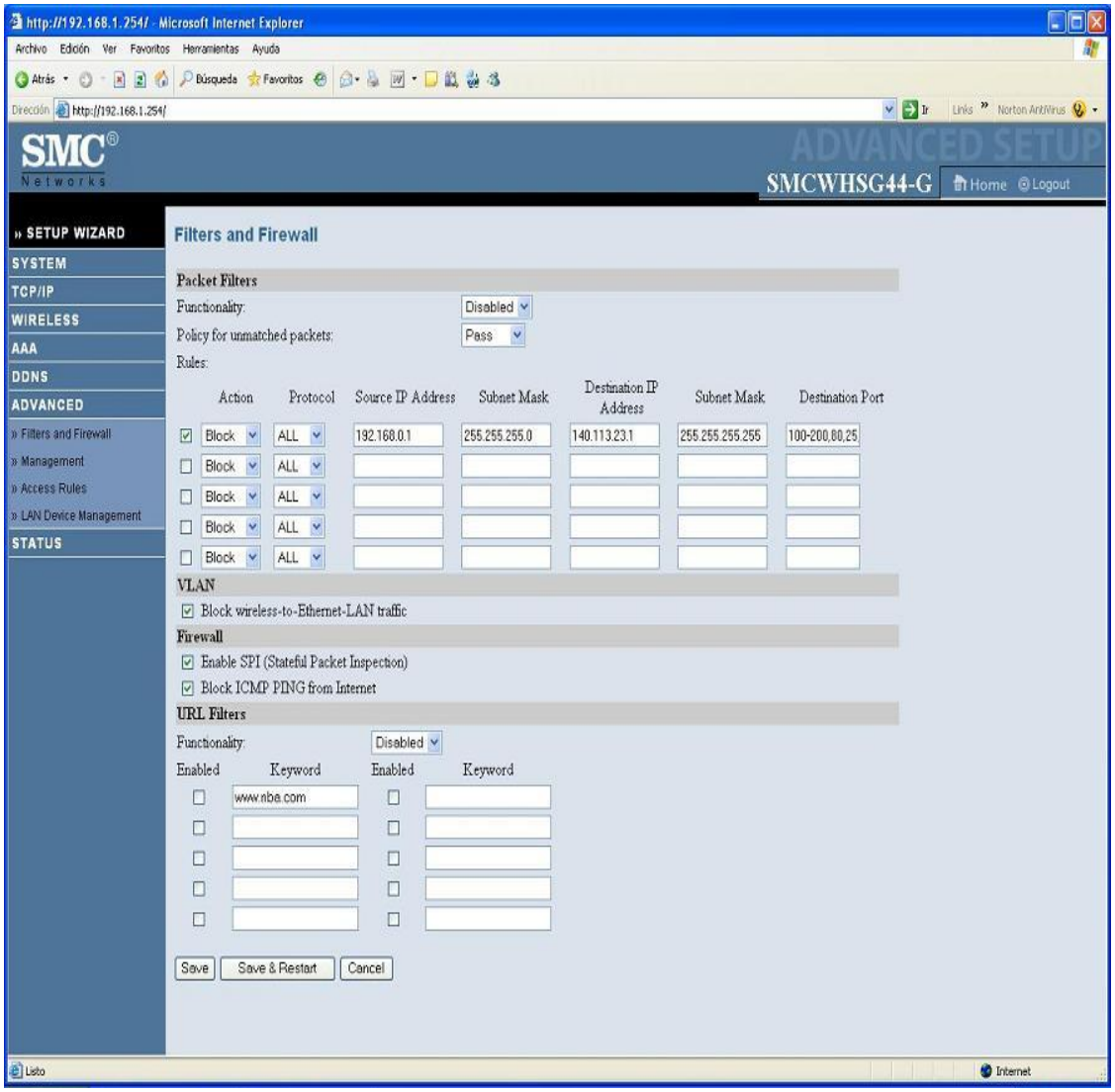
Figura 4.23



En Ticket Setting se personalizará el texto y presentación del ticket que entregará la impresora que se conecta a nuestro Hotspot. Con este ticket el cliente se conectará a Internet proveyendo el usuario y contraseña que aleatoriamente entrega el ruteador.

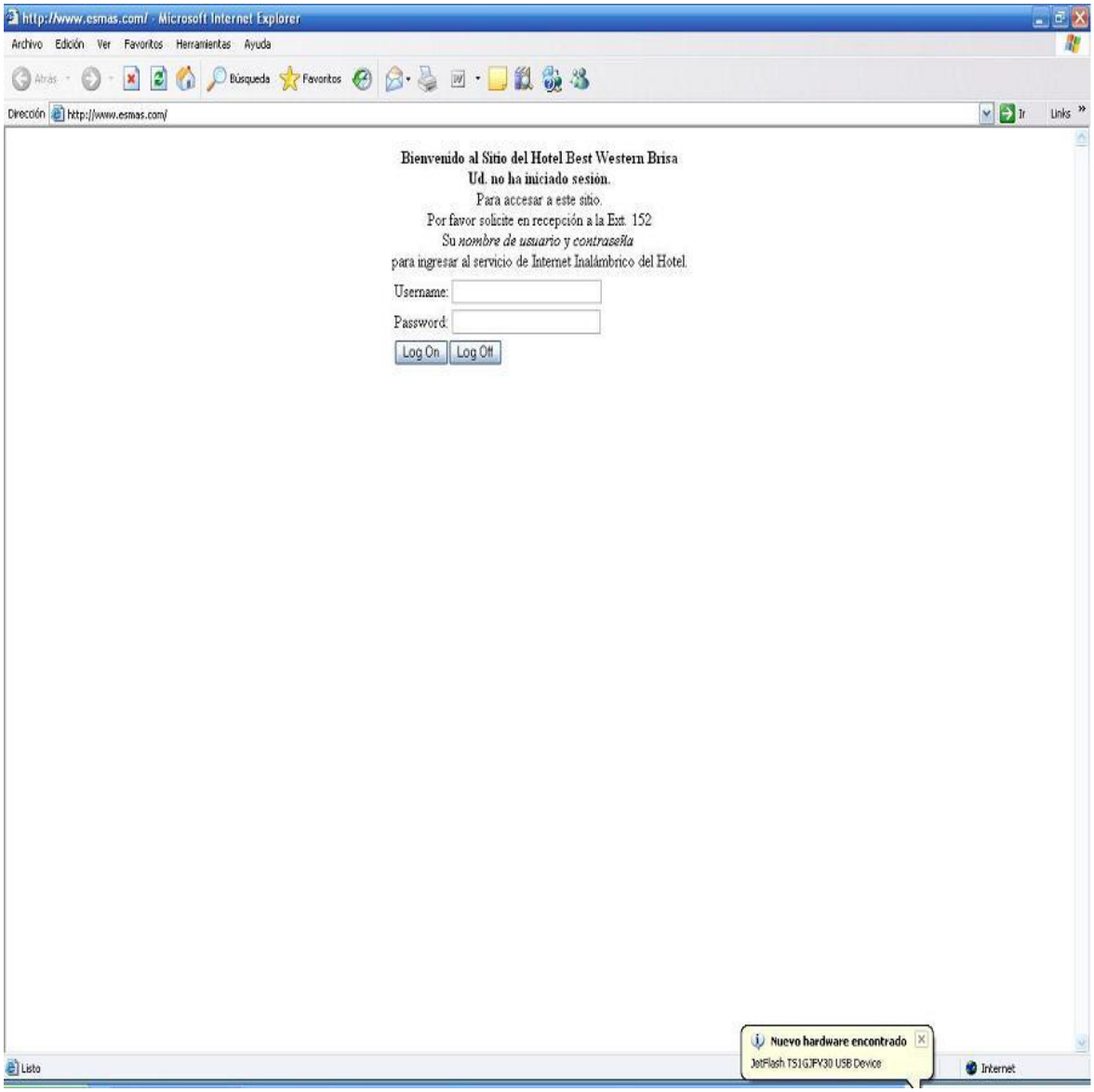
Entre más cifrado se agregue a la seguridad de la información mayor será la longitud de las cadenas de caracteres que entregará el ticket.

Figura 4.24



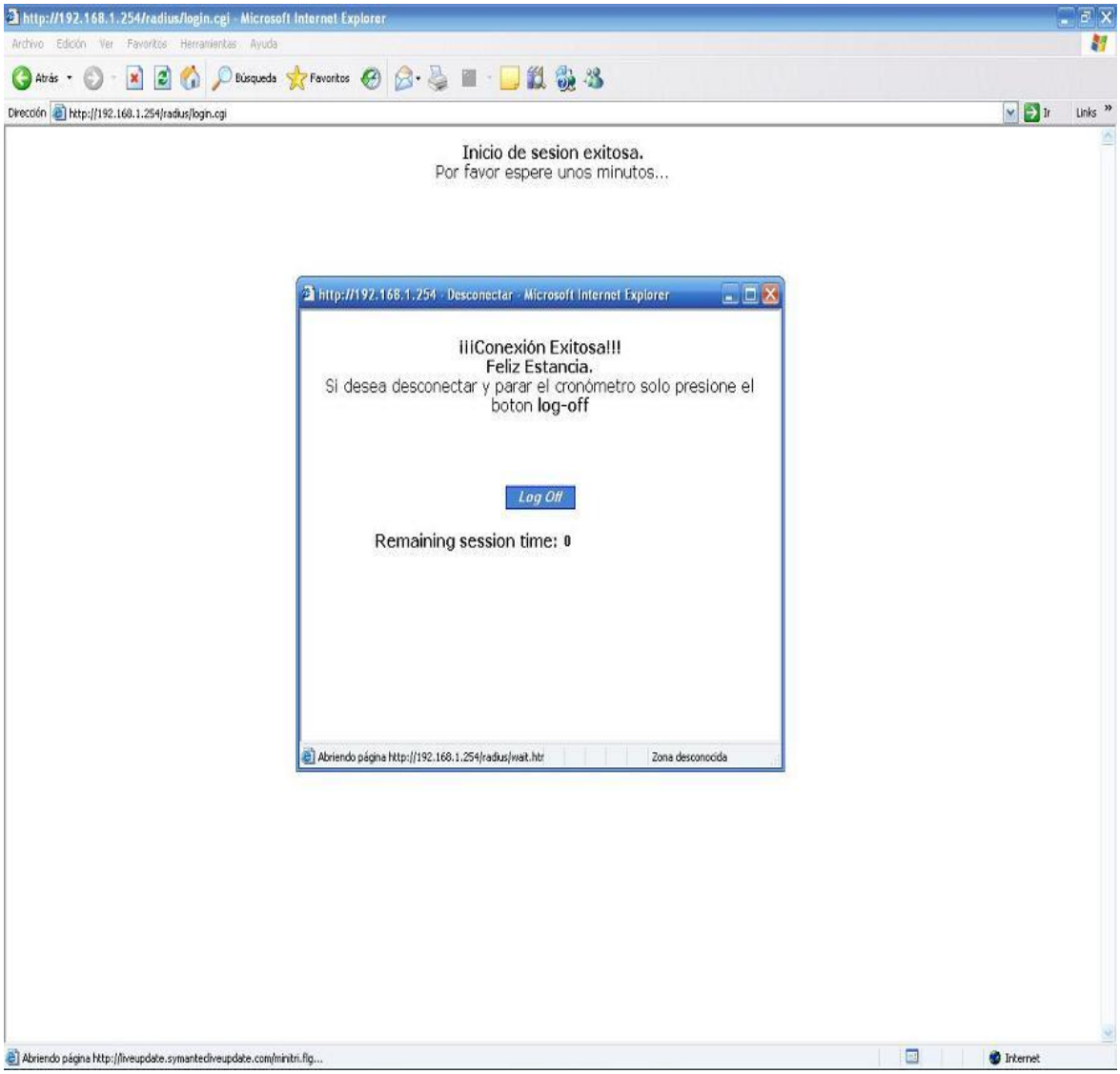
El firewall se usa para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es el que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

Figura 4.25



Finalmente después de hacer las configuraciones necesarias a nuestro Hotspot, ésta es la ventana con la que el huésped se encontrará y donde deberá escribir los datos del ticket que se le proporcionó en recepción.

Figura 4.26



Nuestra configuración y conexión ha sido exitosa, el Hotspot está proporcionando los servicios de seguridad y restricción que se planearon a lo largo de este trabajo. Los huéspedes ahora disponen de una conexión a Internet segura y exclusiva.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Recomendaciones

Consideraciones y consejos sobre alcance y cobertura

El alcance de la señal de nuestra red Wi-Fi dependerá de:

- La potencia del Punto de Acceso.
- La potencia del accesorio o dispositivo Wi-Fi por el que nos conectamos.
- Los obstáculos que la señal tenga que atravesar (muros o metal).

Cuanto más lejos (linealmente) quieras llegar, más alto deberás colocar el Punto de Acceso. Muchos de los actuales APs vienen preparados para poderlos colgar en la pared.

Si quieres llegar lejos, evita también interferencias como microondas o teléfonos inalámbricos.

Si la señal te llega debilitada, utiliza un *amplificador de señal* o si es posible, monta una nueva antena de más potencia al AP (los Puntos de Acceso de gama baja NO lo permiten) o una antena exterior al accesorio (normalmente sólo para formatos PCMCIA o PCI).

Mientras que en las redes cableadas es más complicado conectarse de forma ilegítima -habría que conectarse físicamente mediante un cable-, en las redes inalámbricas -donde la comunicación se realiza mediante ondas de radio-, esta tarea es más sencilla. Debido a esto hay que poner especial cuidado en *blindar* nuestra red Wi-Fi.

Conseguir una red Wi-Fi más segura

El protocolo 802.11 implementa encriptación WEP, pero no podemos mantener WEP como única estrategia de seguridad ya que no es del todo seguro. Existen aplicaciones para Linux y Windows (como AiroPeek, AirSnort, AirMagnet o WEPCrack) que, escaneando el suficiente número de paquetes de información de una red Wi-Fi, son capaces de obtener las claves WEP utilizadas y permitir el acceso de *intrusos* a nuestra red.

Más que hablar de la gran regla de la seguridad podemos hablar de una serie de estrategias que, aunque no definitivas de forma individual, en su conjunto pueden mantener nuestra red oculta o protegida de ojos ajenos.

Cómo asegurar el Punto de Acceso:

Nota 1: Antes de realizar los cambios recomendados a continuación, consulta el manual del Punto de Acceso y del accesorio o dispositivo Wi-Fi para información detallada sobre cómo hacerlo.

1. Cambia la contraseña por defecto.

Todos los fabricantes establecen un password por defecto de acceso a la administración del Punto de Acceso.

Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible que *el observador* la conozca.

Evita contraseñas como tu fecha de nacimiento, el nombre de tu pareja, etc. Intenta además intercalar letras con números.

Aumentar la seguridad de los datos transmitidos:

2. Usa encriptación WEP/WPA.

Activa en el Punto de Acceso la encriptación WEP. Mejor de 128 bits que de 64 bits… cuanto mayor sea el número de bits mejor.

Los Puntos de Acceso más recientes permiten escribir una frase a partir de la cual se generan automáticamente las claves. Es importante que en esta frase intercales mayúsculas con minúsculas y números, evites utilizar palabras incluidas en el diccionario y secuencias contiguas en el teclado (como "qwerty", "fghjk" o "12345").

También tendrás que establecer en la configuración WEP la clave que se utilizará de las cuatro generadas (*Key 1*, *Key 2*, *Key 3* o *Key 4*).

Después de configurar el AP tendrás que configurar los accesorios o dispositivos Wi-Fi de tu red. En éstos tendrás que marcar la misma clave WEP (posiblemente puedas utilizar la *frase* anterior) que has establecido para el AP y la misma clave a utilizar (*Key 1*, *Key 2*, *Key 3* o *Key 4*).

Ya hemos visto que con algunos programas y el suficiente tiempo pueden obtenerse estas claves. En cualquier caso si el observador encuentra una red sin encriptación y otra con encriptación, preferirá "investigar" la primera en vez de la segunda.

Algunos Puntos de Acceso más recientes soportan también encriptación WPA (Wi-Fi Protected Access), encriptación dinámica y más segura que WEP.

Si activas WPA en el Punto de Acceso, tanto los accesorios y dispositivos

WLAN de tu red como tu sistema operativo deben soportarlo (Palm OS por el momento no y para Windows XP es necesario instalar una actualización).

Ocultar tu red Wi-Fi:

3. Cambia el SSID por defecto.

Suele ser algo del estilo a "default", "wireless", "101", "linksys" o "SSID".

En vez de "MiAP", "APDaniel" o el nombre de la empresa es preferible escoger algo menos atractivo para el observador, como puede ser "Broken", "Down" o "Desconectado".

Si no llamamos la atención del *observador* hay menos posibilidades de que éste intente entrar en nuestra red.

4. Desactiva el broadcasting SSID.

El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual.

Al desactivarlo tendrás que introducir manualmente el SSID en la configuración de cada nuevo equipo que quieras conectar.

Si el observador conoce nuestro SSID (por ejemplo si está publicado en alguna web de acceso libre) no conseguiremos nada con este punto.

Evitar que se conecten:

5. Activa el filtrado de direcciones MAC.

Activa en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente tengas funcionando. Al activar el filtrado MAC dejarás que sólo los dispositivos con las direcciones MAC especificadas se conecten a tu red Wi-Fi.

Por un lado es posible conocer las direcciones MAC de los equipos que se conectan a la red con tan sólo "escuchar" con el programa adecuado, ya que las direcciones MAC se transmiten "en abierto", sin encriptar, entre el Punto de Acceso y el equipo.

Además, aunque en teoría las direcciones MAC son únicas a cada dispositivo de red y no pueden modificarse, hay comandos o programas que permiten simular temporalmente por software una nueva dirección MAC para una tarjeta de red.

6. Establece el número máximo de dispositivos que pueden conectarse.

Si el AP lo permite, establece el número máximo de dispositivos que pueden conectarse al mismo tiempo al Punto de Acceso.

7. Desactiva DHCP.

Desactiva DHCP en el router ADSL y en el AP.

En la configuración de los dispositivos/accesorios Wi-Fi tendrás que introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y el DNS primario y secundario.

Si el observador conoce "el formato" y el rango de IPs que usamos en nuestra red, no habremos conseguido nada con este punto.

8. Desconecta el AP cuando no lo uses.

Desconecta el Punto de Acceso de la alimentación cuando no lo estés usando o no vayas a hacerlo durante una temporada. El AP almacena la configuración y no necesitarás introducirla de nuevo cada vez que lo conectes.

9. Cambia las claves WEP regularmente.

Por ejemplo semanalmente o puede ser también cada 2 ó 3 semanas.

Antes decíamos que existen aplicaciones capaces de obtener la clave WEP de nuestra red Wi-Fi analizando los datos transmitidos por la misma. Pueden ser necesarios entre 1 y 4 Gb de datos para romper una clave WEP, dependiendo de la complejidad de las claves. Cuando lleguemos a este caudal de información transmitida es recomendable cambiar las claves.

Recuerda que tendrás que poner la misma clave WEP en el Punto de Acceso y en los dispositivos que se vayan a conectar a éste.

10. No dé por supuesto que los “Hotspots" públicos son seguros.

Muchos bares, hoteles, aeropuertos y otros establecimientos públicos ofrecen redes inalámbricas para sus clientes. Estos “Hotspots" o puntos de acceso a Internet son convenientes, pero no siempre son seguros. Consulte con el propietario del establecimiento para verificar cuáles son las medidas de seguridad implementadas.

11. Tenga cuidado con el tipo de información a la que accede o que envía desde una red inalámbrica pública.

Para evitar riesgos, debería tener en cuenta que otras personas pueden acceder a cualquier información que usted vea o envíe a través de una red inalámbrica pública. A menos que usted pueda verificar que un “Hotspot" haya implementado medidas de seguridad efectivas, lo mejor es evitar el envío o recepción de información delicada a través de la red.

5.2 Conclusión

Cada vez más son más los usuarios de computadoras que se interesan en la conveniencia y movilidad que brinda el acceso inalámbrico a Internet. Actualmente, las personas que viajan por negocios usan computadoras portátiles para mantenerse en contacto con sus oficinas; los turistas mandan fotos a sus amigos desde sus lugares de vacaciones y los compradores hacen sus pedidos cómodamente sentados en el sofá de sus casas. Una red inalámbrica (wireless network) puede conectar varias computadoras ubicadas en distintas partes de su casa o negocio sin enredos de cables y le permite trabajar en una computadora portátil desde cualquier lugar dentro del área de la red.

Generalmente, para acceder a Internet sin cables es necesario tener instalada una conexión de banda ancha, esto se llama "punto de acceso" (access point), como por ejemplo una línea de cable o DSL que funciona conectada a un módem. Para instalar la red inalámbrica, usted conecta el punto de acceso a un ruteador inalámbrico (wireless router) que emite una señal al aire que en algunas oportunidades tiene un radio de emisión de hasta varias decenas de metros. Cualquier computadora que esté equipada con una tarjeta de cliente inalámbrico (wireless client card) que se encuentre dentro del radio de emisión del ruteador puede captar la señal del aire y acceder a Internet.

El aspecto negativo de una red inalámbrica es que, a menos que usted tome ciertas precauciones, cualquier usuario que tenga una computadora preparada para acceder a Internet sin cable puede usar su red. Esto significa que sus vecinos, o en el peor de los casos los ciber-delincuentes o hackers que andan al acecho cerca de su computadora, podrían "colgarse" de su red, o hasta podrían lograr acceder a la información almacenada en su computadora. Si una persona no autorizada usa su red para cometer un delito o enviar mensajes electrónicos spam, la actividad puede ser rastreada hasta su cuenta de usuario.

La tecnología inalámbrica ha llegado, se ha instalado y empieza a enseñar coquetamente las posibilidades como inversión.

La tecnología inalámbrica se va instalando en nuestra sociedad. Parece que las pasadas navidades levantaron indefinidamente la barrera de las comunicaciones wireless, y vemos hoy cómo la carrera hacia el cliente, aun en los albores, se va aproximando a la que ya existe desde hace tiempo en otro tipo

de tecnologías más aceptadas como el ADSL, los portátiles o diversos dispositivos móviles (PDAs, Pocket PCs, etcétera)

Si bien entonces hablábamos de WIFI como ahorro para la empresa hoy nos acercaremos desde otra perspectiva, la de la inversión en WIFI como modelo de negocio. Todo esto parte del planteamiento de cuatro posibilidades, si bien una de ellas habla de las redes privadas y, por tanto, no refiere a un posible negocio directo. Se las resumimos:

Redes privadas. Tanto en empresas, como en entornos corporativos, en universidades, bibliotecas, usos domésticos, particulares o locales.

Hotspot. El verdadero mundo por descubrir y en el que baso este trabajo. Es el modelo más popular, consiste en colocación de puntos de conexión en zonas públicas como aeropuertos, hoteles, cafés, restaurantes, etcétera, dando la posibilidad al usuario que disponga de dispositivo con tarjeta de conexión WIFI cuya compatibilidad no cause problemas.

Servicios VIP. En ellos engloban los servicios que un agente no dedicado a dar servicios de telecomunicaciones ofrece de forma adicional este tipo de conexión.

Operadores WLAN. Esto es, los que directamente entienden como modelo de negocio la estructura, instalación además de dispositivos varios.

Apuntándonos a la clasificación nos centraremos de modo breve en el segundo de los casos. Los Hotspot permiten que WIFI sea una realidad mucho más compleja y extensible que el Internet que hoy conocemos. No se trata sólo de estar en un lugar físicamente y poder conectarte a la Red sin el cable, es mucho más. El concepto nos lleva a que Internet, mi oficina, mi secretaria, VAN con nosotros, por lo que podemos arriesgar a pensar en una penetración similar a la del móvil.

Si convertimos los Hotspots de los hoteles en un canal únicamente de venta y publicidad donde llenen un portátil con anuncios no solicitados sobre los mejores gimnasios de la ciudad (si yo no voy nunca al gimnasio) o en servicios donde, una vez más el usuario no se convenza de que lo que cuestan (algún inocente dudaba de que en Internet todo iba a ser gratuito) realmente merece la pena por lo que ofrecen, volvemos a la casilla de salida.

Por tanto y a modo de conclusión, el modelo de negocio del hot spot (siempre entendido como servicio y no como operador) necesita de:

Dispositivos cómodos y manejables que realicen (etimológicamente hablando: hagan real) el concepto de movilidad (hoy día sentarse en el autobús y sacar el portátil es imposible sin el permiso del codo ajeno)

Precios competitivos y sinceros, en tanto que lo que ofrezcan a través de esa conectividad sea realmente atractivo/productivo.

Velocidades y frecuencias acordes con las demandas que convenzan al usuario que es más rápido encender la computadora, hacer los *clicks* necesarios para encontrar lo que realmente buscan, antes que los métodos "de toda la vida"

Diferenciación de servicios. De una vez por todas, ya sea a través de un Hotspot o de cable, hemos de encontrar en la tecnología una mejora considerable frente al mismo servicio offline. ¿Por qué la gente prefiere aún leer un periódico con una foto estática escrito ayer antes que observar en un gráfico animado o un video los últimos sucesos que acontecen?

GLOSARIO

A

Ad-Hoc (Punto a Punto). Modo de conexión en una red wireless que define que nuestro equipo (PDA, ordenador portátil o de sobremesa) se conectará directamente a otro equipo, en vez de hacerlo a un Punto de Acceso.

ADSL. Línea de Suscripción Asimétrica Digital. Tecnología que mejora el ancho de banda de los hilos del cableado telefónico convencional que transporta hasta 16 Mbps (megabits por segundo) gracias a una serie de métodos de compresión.

Alias Apodo o Pseudónimo. Nombre usualmente corto y fácil de recordar que se utiliza en lugar de otro nombre usualmente largo y difícil de memorizar.

Ancho de Banda. Cantidad de bits que pueden viajar por un medio físico (cable coaxial, par trenzado, fibra óptica, etc.) de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información. Se mide en millones de bits por segundo (Mbps). Una buena analogía es una autopista. Mientras más carriles tenga la calle, mayor cantidad de tráfico podrá transitar a mayores velocidades. El ancho de banda es un concepto muy parecido. Es la cantidad de información que puede transmitirse en una conexión durante una unidad de tiempo elegida.

Aplicación. Cualquier programa que corra en un sistema operativo y que haga una función específica para un usuario. Por ejemplo, procesadores de palabras, bases de datos, agendas electrónicas, etc.

ARPANet. Advanced Research Projects Agency Network. Precursor del Internet desarrollado a finales de los 60's y principios de los 70's por el Departamento de Defensa de los Estados Unidos como un experimento de una red de área, no centralizada y amplia y que resista una guerra nuclear.

B

Browser. Aplicación para visualizar todo tipo de información y navegar por el WWW con funcionalidades plenamente multimedia. Como ejemplo de navegadores tenemos Internet Explorer, Firefox y Safari (Mac). Estos programas pueden también actualizarse a sus últimas versiones de forma gratuita.

C

Cableado. Columna vertebral de una red la cual utiliza un medio físico de cable, casi siempre del tipo de red de área local (LAN), de forma que la información se transmite de un nodo a otro. La reciente aparición de las redes inalámbricas ha roto el esquema tradicional al no utilizar ningún tipo de cableado.

Click. Cuando se oprime alguno de lo botones de un mouse el sonido es parecido a un "click". La palabra click escrita, se usa generalmente para indicarle al usuario que oprima el botón del mouse encima de un área de la pantalla. También es comúnmente

escrito así: clic. En español incluso se usa como un verbo, por ejemplo: al clickear en el enlace.

Cliente. Aplicación que permite a un usuario obtener un servicio de un servidor localizado en la red. Sistema o proceso el cual le solicita a otro sistema o proceso la prestación de un servicio.

Contraseña/Password. Código utilizado para acceder un sistema restringido. Pueden contener caracteres alfanuméricos e incluso algunos otros símbolos. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario.

Criptografía. Se dice que cualquier procedimiento es criptográfico si permite a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo, luego de haberlo descifrado.

D

DHCP. Tecnología utilizada en redes que permite que los equipos que se conecten a una red (con DHCP activado) auto-configuren los datos dirección IP, máscara de subred, puerta de enlace y servidores DNS, de forma que no haya que introducir estos datos manualmente. Por defecto la mayoría de los routers ADSL y los Puntos de Acceso tienen DHCP activado.

Dirección MAC. (MAC address - Media Access Control address) Es el código único de identificación que tienen todas las tarjetas de red. Nuestro accesorio Wi-Fi o nuestro PDA con Wi-Fi integrado, al ser un dispositivo de red, también tendrán una dirección MAC única.

DNS. Servidor de Nombres de Dominio. Servidor automatizado utilizado en el Internet cuya tares es convertir nombres fáciles de entender (como www.midominio.com) a direcciones numéricas de IP.

Dominio. Sistema de denominación de host en Internet el cual está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda. Comprenden una red de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado por un servidor de dominios. Los dominios se establecen de acuerdo al uso que se le da a la computadora y al lugar donde se encuentre. Los más comunes son .com, .edu, .net, .org y .gov; la mayoría de los países tienen su propio dominio, y en la actualidad se están ofreciendo muchos dominios nuevos debido a la saturación de los dominios .com (utilizados mucho por empresas).

E

Ethernet. Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus, tiene ancho de banda de 10 Mbps de forma que presenta una elevada velocidad de transmisión; y se ha convertido en un estándar de red corporativa.

F

Firewall. Combinación de hardware y software la cual separa una red de área local (LAN) en dos o más partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

FQDN. En inglés, Fully Qualified Domain Name. Nombre de Dominio Totalmente Calificado. Nombre completo de un sistema y no solo el nombre del sistema. Por ejemplo, "midominio" es un nombre de sistema y "midominio.com" es un FQDN.

FTP. File Transfer Protocol. Protocolo de transferencia de archivos. Se usan programas clientes para FTP (para Windows) como LeapFTP o Core FTP con soporte para SSL, por mencionar algunos. Se usan programas servidores de FTP como NcFTPd. Estos programas permiten la conexión entre dos computadoras, usando por lo general el puerto 21 para conectarse (aunque se puede usar otros puertos). Por medio del Protocolo de transferencia de archivos se pueden subir y bajar archivos entre el cliente y el host (servidor).

H

Hacker. Persona que tiene un conocimiento profundo acerca del funcionamiento de redes de forma que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

Host. Servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente a la que tenemos acceso de diversas formas (SSH, FTP, WWW, email, etc.). Al igual que cualquier computadora conectada a Internet, debe tener una dirección o número IP y un nombre.

Hosting. El servicio de Web Hosting consiste en el almacenamiento de datos, aplicaciones o información dentro de servidores diseñados para llevar a cabo esta tarea. Los servidores a su vez se deben colocar en edificios o estructuras denominadas data centers, con su debida planta eléctrica, seguridad y conectividad con los mayores proveedores de telecomunicaciones (backbones) del mundo, para poder ofrecer buen ancho de banda.

Hotspot. Áreas donde hay conexión Wi-Fi accesible.

Hub (Switch). El punto central de conexión para un grupo de nodos; útil para la administración centralizada, la capacidad de aislar nodos de problemas y ampliar la cobertura de una LAN.

I

Internet. Una red mundial, de redes de computadoras. Es una interconexión de redes grandes y chicas alrededor del mundo. El Internet empezó en 1962 como una red para los militares llamada ARPANet, para que en sus comunicaciones no existan “puntos de

falla". Con el tiempo fue creciendo hasta convertirse en lo que es hoy en día, una herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP. Sobre esta red se pueden utilizar múltiples servicios como por ejemplo e-mail, WWW, etc. que usen TCP/IP.

Intranet. Red privada dentro de una compañía u organización que utiliza el navegador favorito de cada usuario, en su computadora, para ver menús con opciones desde cumpleaños del personal, calendario de citas, mensajería instantánea privada, repositorio de archivos y las normativas de la empresa entre otras. Es como si fuera un sitio Web dentro de la empresa. Al usar los browser de Internet como Internet Explorer, Firefox o Safari el Intranet se convierte en multiplataforma. No importa la marca o sistema operativo de las computadoras dentro de la red, todos se pueden comunicar.

IP. Internet Protocol, Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. El IP es la dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos como por ejemplo, 132.248.53.10

ISDN. Integrated Services Digital Network. Red Digital de Servicios Integrados. Servicio mediante el cual las líneas telefónicas pueden transportar señales digitales en lugar de señales analógicas, aumentando considerablemente la velocidad de transferencia de datos a la computadora. ISDN combina servicios de voz y digitales a través de la red en un solo medio, haciendo posible ofrecer a los clientes servicios digitales de datos así como conexiones de voz a través de un solo "cable". Se requiere contar con el equipo y el software necesario así como la oferta del servicio por parte tanto de la central telefónica local ofrece como del proveedor de servicios de Internet. La velocidad de transferencia que puede alcanzar ISDN es de 128,000 bps, aunque en la práctica las velocidades comunes son de 56,000 o 64,000.

ISP. Internet Service Provider. Proveedor de Servicio Internet. Empresa que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas broadband o dial-up.

K

Kbps. Kilobits por segundo. Unidad de medida que comúnmente se usa para medir la velocidad de transmisión por una línea de telecomunicación, como la velocidad de un cable módem por ejemplo.

L

LAN. Local Area Network. Red de área local. Red de computadoras personales ubicadas dentro de un área geográfica limitada que se compone de servidores, estaciones de trabajo, sistemas operativos de redes y un enlace encargado de distribuir las comunicaciones. Por ejemplo, computadoras conectadas en una oficina, en un edificio o en varios. Se pueden optimizar los protocolos de señal de la red hasta alcanzar velocidades de transmisión de 100 Mbps .

Laptop. Computadora portátil que pesa aproximadamente dos o tres kilogramos. Existen distintos modelos, desde las notebooks comunes hasta las multimedia (dotadas

de parlantes, lectora de CD-ROMs, monitor color, etc.). Según su capacidad, tienen una autonomía de corriente eléctrica de dos a seis horas de duración. A raíz de que la tecnología compacta es bastante cara, estos equipos suelen costar prácticamente el doble que sus pares de escritorio, comparando sistemas de capacidades equivalentes.

Login. Clave de acceso que se le asigna a un usuario con el propósito de que pueda utilizar los recursos de una computadora. El login define al usuario y lo identifica dentro de Internet junto con la dirección electrónica de la computadora que utiliza.

M

Máscara de subred. Cifra de 32 bits que especifica los bits de una dirección IP que corresponde a una red y a una subred. Normalmente será del tipo 255.255.255.0

Módem. Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica o a una ISDN, mediante procesos denominados modulación (para transmitir información) y desmodulación (para recibir información). La velocidad máxima que puede alcanzar un módem para línea telefónica es de 33 Kbps, sin embargo los más comerciales actualmente son los de 28 Kbps. Un módem debe cumplir con los estándares de MNP5 y V42.bis para considerar su adquisición. Los módems pueden ser en internos (los que se colocan en una ranura de la computadora) y en externos (que se conectan a un puerto serial de la computadora).

N

Nodo. Cada una de las computadoras individuales u otros dispositivos de la red.

O

Ordenador. En Hispanoamérica se le conoce comúnmente como computadora, pero en Europa se le conoce de esta forma y se ha adoptado el nombre mundialmente en los últimos años.

OSI. Interconexión de Sistemas Abiertos (Open Systems Interconnect). Es el protocolo en el que se apoya Internet. Establece la manera como se realiza la comunicación entre dos computadoras a través de siete capas: Física, Datos, Red, Transporte, Sesión, Presentación y Aplicación.

P

Página Web. Resultado en hipertexto o hipermedia que proporciona un navegador del WWW después de obtener la información solicitada. Su contenido puede ir desde un texto corto a un voluminoso conjunto de textos, gráficos estáticos o en movimiento, sonido, etc. Algunas veces el citado término es utilizado incorrectamente en orden de designar el contenido global de un sitio Web, cuando en ese caso debería decirse "Web site".

PCMCIA. Tarjeta estandarizada de expansión, del tamaño de una tarjeta de crédito, utilizada en ordenadores personales. En telecomunicaciones, uno de sus principales usos es la transmisión de mensajes, datos y faxes a través de computadoras portátiles y teléfonos móviles.

PDA. Personal Digital Assistant (Asistente Digital Personal) - Ordenador de pequeño tamaño cuya principal función era, en principio, mantener una agenda electrónica. No obstante, cada vez más se va confundiendo con los ordenadores de mano y de palma.

Periféricos. Aparatos o equipos electrónicos, (como impresoras, teclados, escáner, etc.), adicionales a una computadora (formada por memoria principal y CPU); se usa habitualmente para definir a los elementos que se conectan externamente a un puerto de la computadora.

PING. Packet Internet Groper. Este comando se utiliza para comprobar si una determinada interfaz de red, de nuestra computadora o de otra, se encuentra activa. Lo que se está haciendo en realidad es mandar paquetes a donde se le indique y nos dice cuanto tiempo demoró el paquete en ir y regresar, entre otras informaciones. Entre sus usos más comunes: resolver el nombre de host para saber su IP o simplemente verificar si una máquina está prendida. Un "ping" sin respuesta no necesariamente significa que la computadora no existe o esta apagada. Si el host o ip al cual se le hace ping tiene un firewall que no permite las respuestas al protocolo ICMP, entonces el "ping" no puede proporcionarnos información.

Proxy. Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red. Al mismo tiempo contiene mecanismos de seguridad (firewall o cortafuegos) los cuales impiden accesos no autorizados desde el exterior hacia la red privada. También se le conoce como servidor caché.

Puente. Dispositivos que tienen usos definidos como interconectar segmentos de red a través de medios físicos diferentes (es usual ver puentes entre un cable coaxial y otro de fibra óptica). Además, pueden adaptar diferentes protocolos de bajo nivel (capa de enlace de datos y física de modelo OSI).

Puerto. Número que aparece tras un nombre de dominio en una URL. Dicho número va precedido del signo (dos puntos). Canal de entrada/salida de una computadora.

Punto de Acceso (AP). Es el dispositivo que hace de *puente* entre la red cableada y la red inalámbrica. Podemos pensar que es, de alguna manera, la *antena* a la que nos conectaremos.

R

RADIUS (acrónimo en inglés de *Remote Authentication Dial-In User Server*). Es un protocolo de autentificación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos

Red. Network en inglés. Sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en lugares más o menos próximos. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

RJ45. Es uno de los dos tipos de conectores usados en las computadoras, emplea un cable y un conector muy similares a los del teléfono, donde cada PC tiene su propio cable y todos ellos pueden unirse a un HUB. En caso de dañarse uno de los cables o conectores, este equipo quedará desconectado de los otros pero la red sigue funcionando con normalidad.

Router (Ruteador). Un dispositivo que conecta dos redes; opera como un bridge pero también puede seleccionar rutas a través de una red.

S

Servidor. Un servidor es una computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes). También puede referirse a un software específico, como lo es el servidor WWW. Una computadora puede tener distintos software de servidor, proporcionando muchos servidores a clientes en la red. Por ejemplo, las computadoras que contienen sitios Web se llaman servidores ya que “sirven” recursos de Web para aplicaciones cliente como los navegadores o browsers.

SSID. Nombre con el que se identifica a una red Wi-Fi. Este identificador viene establecido de fábrica pero puede modificarse a través del panel de administración del Punto de Acceso.

Sniffer. Programa que busca palabras claves que se le hayan impartido en los paquetes que atraviesan un nodo con el objetivo de conseguir información y normalmente se usa para fines ilegales. Por ejemplo, a un sniffer se le puede instruir que busque la palabra clave "password". No es tan sencillo en realidad. De todas formas, este tipo de problemas son fácilmente solucionables con algún tipo de política de seguridad electrónica, como un firewall.

T

TCP/IP. El nombre TCP/IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). En español es Protocolo de Control de Transmisión y Protocolo de Internet. Forma de comunicación básica que usa el Internet, la cual hace posible que cualquier tipo de información (mensajes, gráficos o audio) viaje en forma de paquetes sin que estos se pierdan y siguiendo cualquier ruta posible.

Telnet. Servicio de Internet con el cual un usuario se puede conectar de forma remota a otra computadora, como si se hiciera desde un terminal local, usualmente por el puerto 23. Es preferible usar otros programas más actualizados como ssh2, ya que telnet tiene vulnerabilidades.

W

WEP. Es el tipo de encriptación que soporta la tecnología Wi-Fi. Su codificación puede ir de 64 bits hasta 128 bits. WEP está deshabilitado por defecto.

WiFi (Wi-Fi). Abreviatura en inglés para "wireless fidelity". Un tipo de red inalámbrica (WLAN - wireless local area networks), que usa el protocolo inalámbrico de alcance limitado IEEE 802.11b, que transmite datos en banda ancha en el rango espectral de 2.4 GHz. Ha ganado aceptación en mucho ambientes como una alternativa viable a los LANs cableados. Muchos hoteles, restaurantes, aeropuertos, etc. ofrecen acceso público a Internet por medio de WiFi. A estos lugares se les conoce como “hotspots”. Se deben tomar las medidas mínimas de seguridad (firewall) en las computadoras con capacidad WiFi, y sobretodo en los routers inalámbricos para proteger el acceso a la red por personas ajenas a la misma. Sin los controles necesarios, cualquier persona cerca al radio de transmisión de su router inalámbrico puede conseguir conexión a Internet, navegar con su ancho de banda e incluso “hackear” su red privada.

WPA (*Wi-Fi Protected Access* - 1995 - Acceso Protegido Wi-Fi) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP

BIBLIOGRAFÍA

DOCUMENTO IEEE “Redes Híbridas" Pág. 21-26
1992 Universidad de Aveiro, Portugal
Ruiz T. Valadas, Adriano C. Moreira, A.M. de Oliveira Duarte.

DOCUMENTO IEEE "Ruteando con TCP/IP" Pág. 7-12
1992 IBM T.J. Watson Reserach Center
Charles E. Perkins.

DOCUMENTO IEEE "Características de una Radio LAN" Pág. 14-19
1992 LACE Inc.
Chandos A. Rypinski.

“Conexiones Inalámbricas“
McGraw-Hill 2003
Charlie Russel

Revista PC/Tips Byte Pág. 94-98
Artículo: “Redes Inalámbricas"
Abril 1992 Nicolas Baran.

Revista PC/Magazine Pág. 86-97
Artículo: "Sin Conexión"
Marzo 1995 Padriac Boyle.

“Redes y Computadoras”
Prentice Hall 1997
Andrew S. Tanenbaum

“Comunicaciones en Redes Inalámbricas”
McGraw-Hill 1994
Bates R.J.

“Redes de Área Local Inalámbricas””
NY, McGraw-Hill 1995
Davis P.T. y McGuffin, C.R.

http://lat.3com.com/lat/technology/technnical.papers/

http://www.wirelessethernet.com

http://www.pdaexpertos.com/tutoriales/comunicaciones/

http://www.mundotutoriales.com

http://www.emagister.com