UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

"DISEÑO E IMPLANTACIÓN DE UNA RED INALÁMBRICA PARA UNA CADENA DE RESTAURANTES"

T E S I S

Que para obtener el Título de:

INGENIERO EN COMPUTACIÓN

Presentan:

Marcos Moisés García Martín

Carlos David Cabrera Rosales

Directora de Tesis:

M en A. M. DEL CARMEN MALDONADO SUSANO

MEXICO, D.F., 2004.

ÍNDICE GENERAL

Capítulo I

ANÁLISIS INICIAL

1.1. INTRODUCCIÓN

1.1.1. Antecedentes Históricos

Los cuatro últimos siglos han estado dominados, cada uno de ellos, por una tecnología. El siglo XVIII fue la época de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la era de las máquinas de vapor. En el siglo XX, la tecnología clave ha sido la obtención, procesamiento y distribución de información. Entre otros avances, hemos visto la instalación de redes telefónicas mundiales, la invención de la radio y la televisión, el nacimiento y crecimiento sin precedentes de la industria de las computadoras y el lanzamiento de satélites de computación. Podría decirse que el primer conocimiento acerca de redes fue escrito por P. Baran, en 1960, por las Fuerzas Aéreas Americanas en respuesta al lanzamiento del Sputnik por los rusos.

Durante el período de 1962 a 1964, la agencia ARPA[1] del Departamento de Defensa Americano, bajo la dirección de J. C. Licklider, fomentó la investigación de sistemas de tiempo compartido y en 1967 se proponía la primera red experimental patrocinada por la ARPA que consistía en interconectar las computadoras de varios centros de investigación y universidades americanas. Esta red fue entonces diseñada por la firma Bolt, Beranck y Newman y comenzó a finales del año 1969, con cuatro nodos.

La red ARPANET[2] fue objeto de diversos experimentos y estudios ampliamente difundidos. De donde podemos destacar el trabajo de L. Kleinrock en la UCLA sobre teoría y aspectos prácticos del diseño de redes de computadoras.

En 1969 comenzó la instalación de la red TYMNET, realizada por la TYMSHARE para ofrecer acceso a sus sistemas interactivos.

La mayoría de las redes mencionadas tenían un carácter experimental en la investigación sobre tecnología de redes de computadoras. Con el abaratamiento del costo de proceso contra costo de transmisión, la tecnología de conmutación de paquetes para la transmisión de datos pasó a ser económicamente ventajosa, lo que atrajo el interés en ofrecer este tipo de servicio por parte de los órganos de correos y telégrafos de varios países. Las primeras redes públicas se extendieron por Europa en Inglaterra y Francia, entre otros; en América: Estados Unidos y Canadá, posteriormente se agregaron Japón, Australia y América Latina.
En el año de 1974 ARPA fue renombrada por DARPA[3], ARPANET estuvo constantemente utilizando como protocolo NCP[4] para transferir datos. Además de que se da pasó a un nuevo protocolo: TCP/IP[5], el cual fue desarrollado por un grupo encabezado por Vinton Cerf de Stanford y Bob Kahn de DARPA.

---

[1] ARPA (Advanced Research Projects Agency, Agencia de Proyectos de Investigación Avanzada)
[2] ARPANET (Agencia de Proyectos de Investigación Avanzada en la Red)
[3] DARPA (The Defense Advanced Research Projects Agency, Agencia de Proyectos de Investigación Avanzada para la Defensa)
[4] NCP (Network Control Protocol, Protocolo de Control de Red)
[5] TCP/IP (Protocolo de Control de Transmisión / Protocolo Internet) Sistema de protocolos, definidos en RFC 793, en los que se basa buena parte de Internet. El primero se encarga de dividir la información en paquetes

El Dr. Robert M. Metcalfe desarrolló Ethernet en 1976, la cual permitía con cable coaxial mover datos extremadamente rápido. Esto fue un componente crucial para el desarrollo de LANs (Local Area Networks).

El proyecto de satélite entró en el uso práctico: SATNET [6] se conectó a una red de computadoras, la cual unió a los Estados Unidos con Europa. Después, se crearon consorcios de países para utilizar los satélites, como fue el caso de INTELSAT.

El protocolo TCP/IP se propone como base de comunicación entre máquinas en el Departamento de Defensa de Estados Unidos para su utilización en ARPANET.

En enero de 1983, cada máquina conectada a ARPANET tenía que usar TCP/IP. TCP/IP se volvió completamente el protocolo de Internet y NCP fue reemplazado.

La Universidad de Wisconsin creó el Servidor de Nombres del Dominio (DNS). Esto permitió que los paquetes se dirigieran a un nombre de dominio que sería traducido por el servidor, en la base de datos con en el número de IP correspondiente.

En 1984 ARPANET era dividido en dos redes: MILNET cuya función principal era servir las necesidades del ejército y ARPANET para apoyar el avance en la investigación de componentes, la Sección de Defensa continuó apoyando ambas redes.

En 1985 se transmitía a 1.5 Mbps[7] en la red NSFNET, por mencionar alguna, este tipo de transmisión era 25 veces más rápida que las 56 líneas de Kbps[8].

En 1988, el tráfico aumentó tan rápidamente que se pensó en actualizar la red de nuevo, buscando nuevas alternativas. Una de las corporaciones interesadas en ello fue ANS[9] la cual inició investigaciones en redes de alta velocidad. En este momento, las alternativas de solución entran en una etapa de "construcción y prueba" y en 1991 comienza el auge de nuevas herramientas como es el caso de la programación en HTML y Mosaic, entre otros; además comienza la definición de dominios, de acuerdo con la función de las instituciones: .edu, .gov, .com, .org, etc.
La transmisión en NSFNET fue soportada por ATM[10] a 145 Mbps, mejorando considerablemente los problemas de tráfico en las líneas.
Actualmente la Sociedad de Internet, el grupo que controla el Internet, está intentando sacar un nuevo TCP/IP para poder tener billones de direcciones.

Debido al rápido progreso de la tecnología, estas áreas han convergido rápidamente, y las diferencias entre reunir, transportar, almacenar y procesar información desaparecen con

---

en origen, para luego recomponerla en destino, mientras que el segundo se responsabiliza de dirigirla adecuadamente a través de la red.
[6] SATNET (Satélite del Atlántico)
[7] Mbps (Mega bits por segundo)
[8] Kbps (Kilobits por segundo). Unidad de medida de la velocidad de transmisión por una línea de telecomunicación. Cada kilobit está formado por mil bits.
[9] ANS (Advanced Network Systems, Sistemas de Red Avanzados)
[10] ATM (Asynchronous Transmissión Mode, Transmisión Modo Asíncrono)

rapidez. Al crecer nuestra habilidad para obtener, procesar y distribuir información, también crece la demanda de técnicas de procesamiento de información más avanzadas.

Aunque la industria de la computación es joven comparada con otras industrias (por ejemplo, las de automóviles y transporte aéreo), las computadoras han logrado un progreso espectacular en un tiempo corto. Durante las dos primeras décadas de su existencia, los sistemas de cómputo eran altamente centralizados, por lo general, dentro de un cuarto grande. En muchos casos, este cuarto tenía paredes de vidrio a través de las cuales los visitantes podrían asombrarse de la gran maravilla electrónica que se encontraba dentro. Una compañía de tamaño mediano o una universidad tenía una o dos computadoras, mientras que una institución grande tenía cuando mucho unas cuantas docenas. La idea de que dentro de 20 años se pudieran producir en masa, por millones, computadoras de igual capacidad más pequeñas que las estampillas de correo, era pura ciencia ficción.

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, actualmente está siendo ampliamente investigada. 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. Éstas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Los sistemas de cable de fibra óptica logran velocidades aún mayores, y pensando futuristamente se espera que las redes inalámbricas alcancen velocidades de solo 10 Mbps.

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.

1.1.2. Metodología para el desarrollo del proyecto

Siempre que existe una necesidad humana de bienes o servicios habrá necesidad de invertir recursos, ya sean económicos o humanos; sacrificando beneficios actuales con la esperanza de obtener en un plazo dado beneficios superiores. La función del ingeniero es satisfacer esas necesidades humanas, encontrando una solución inteligente que minimice los recursos a invertir, maximizando los beneficios obtenidos. Un ingeniero debe hacer uso de metodologías que le permitan encontrar la mejor alternativa de solución a una necesidad; por lo que para desarrollar el proyecto motivo de esta tesis, se seleccionó la metodología para solución de problemas propuestas por Edward Krick en su libro “Fundamentos de

Ingeniería" la cual se presenta enseguida en forma esquemática con lo que cada punto durante el transcurso del proyecto verificaremos los criterios y las decisiones que se tomarán para un óptimo rendimiento llevando a cabo su implementación y puesta en marcha de la red inalámbrica:

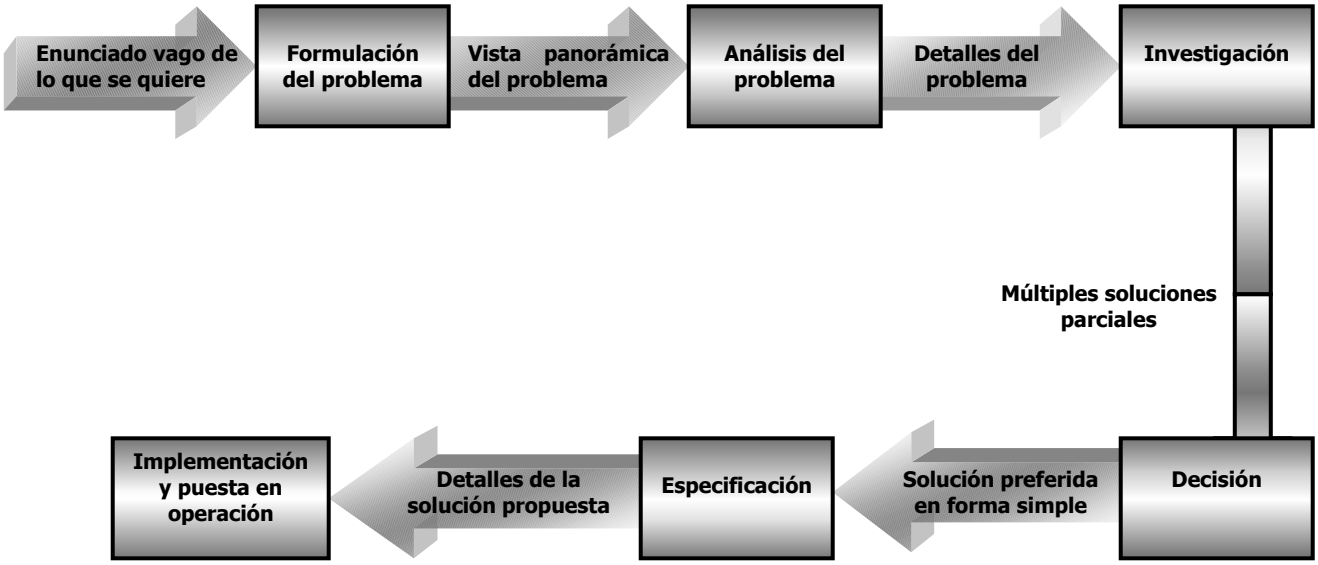


Figura 1.1. Metodología

Formulación del problema

La información es uno de los recursos más importantes para cualquier empresa, incluso la de restaurantes. El registro de datos de una entidad, así como su almacenamiento y la comunicación entre sus distintos componentes debe de realizarse de manera rápida, oportuna y segura. Mediante una red de computadoras intentamos proporcionar los medios necesarios para mantener un manejo óptimo de este recurso aprovechando la tecnología a nuestro alcance y manteniendo un sistema de vanguardia que dará como resultado una mejor administración de la empresa y por ello un mejor desarrollo de la misma.
Sin embargo existen limitaciones cuando se trabaja con redes extensas, especialmente si se trata de comunicar dos puntos distantes: a escasos metros, en edificios con problemas de instalación de cableado o distancias donde no llega el tendido de cables, un par de kilómetros uno del otro, etc. Éste es el caso de nuestro ambiente: una cadena de restaurantes.

Análisis del problema

La modernización para todo tipo de empresa requiere un alto grado de tecnología; la cadena de restaurantes actualmente tiene la desventaja de no contar con una red para la comunicación entre otras entidades que les permita manejar de manera eficiente la información correspondiente de cada producto así como de su precio y su actualización.

El equipo y los recursos que se desean utilizar se propondrán en capítulos posteriores. Esta red se pretende armar de acuerdo con los procesos de flujo de información que son lentos dado el volumen de datos que se manejan y porque la información se encuentra dispersa y muy heterogénea.

Por otro lado, es necesario modernizar los procesos empresariales, por lo que se requiere además proporcionar herramientas a los empleados para lograr esta modernización; una de las herramientas es la rapidez y seguridad apoyada con computadoras.

Parte importante de este análisis, es el no perder de vista nuestros objetivos, y visualizarlos como satisfechos en el mayor grado posible, teniendo como resultado que las actividades laborales y administrativas, sean más ágiles sin perder su eficiencia y confiabilidad, e inclusive éstas sean acrecentadas; que las funciones de capacitación y reclutamiento se vean enriquecidas con nuevas alternativas para su ejecución y que las herramientas de apoyo se encuentren al alcance del consorcio restaurantero encargado de dichas funciones o actividades, incluyendo a los empleados, gerentes y dueños; además de lograr una difusión amplia para las actividades e información que así lo requiera.

Investigación

La red se instalará en tres entidades que a su vez una de ellas será la cabeza principal de toda la información resguardando datos de cada una de las otras entidades a conectar; esto conlleva a:

- Investigar las características físicas del ambiente involucrado midiendo los parámetros que van a influir en la elección del equipo y diseño de la red.
- Realizar el diseño estructurado de la red considerando cada una de las cantidades involucradas en el proyecto.
- Analizar y comparar los diferentes tipos de equipo (hardware) que existen en el mercado para la implementación del proyecto y elegir aquel que resulte óptimo para nuestras necesidades.
- Establecer el sistema (software) que contenga las mejores características para el manejo y transmisión de la información a través de la red cubriendo los requerimientos de fiabilidad, seguridad, velocidad y otras características requeridas.

En los capítulos posteriores se presentarán los conceptos fundamentales sobre comunicaciones y redes, los cuales forman parte de la investigación que se realizó para

elegir la tecnología adecuada para implementar la solución, considerando que se deben cumplir ciertas especificaciones de acuerdo con los equipos y el sistema.

1.1.3. Descripción del ambiente a analizar

En este proyecto se pretende diseñar una red de datos inalámbrica para satisfacer las necesidades de comunicación de datos entre los diversos componentes de una cadena de restaurantes para mantener a la empresa a la vanguardia en cuanto al servicio que ofrece, además de proporcionar agilidad y versatilidad a sus operaciones manteniendo la seguridad que requiere una empresa con tales características. Esta comunicación se requiere para mantener el control de ventas, inventarios, precios de los productos, asistencia de personal, etc. Las características físicas del proyecto hacen necesaria implementar una red inalámbrica que, como se describirá en este trabajo, será la mejor opción en cuanto a costo y operabilidad. En principio se describirá lo más básico acerca de cómo se conformará esta cadena de restaurantes para tener idea más clara de lo que requerimos en el proyecto:

- La ubicación de nuestro primer edificio corresponderá a la CENTRAL A; llevando a cabo la función de servidor, que difundirá a cada una de las otras entidades conectadas toda la información para su funcionamiento y la actualización de cada dato requerido. Esta central será la encargada de corregir, enviar y recibir toda la información de los anexos conectados a la red y actualizará toda la base de datos así como el itinerario que llevará cada unidad. El equipo que se ocupará para esta parte, así como su descripción, se revisará con más detalle en el diseño de la red.

- El segundo edificio corresponderá al ANEXO B; el cual será una de las 2 entidades que se conectarán. La función de este recinto será la de informar a la central problemas técnicos, falta de personal, etc., que puedan surgir en el transcurso del servicio y sólo se podrá comunicar con otro anexo mediante la central para todos los casos. Al igual que para la central, el equipo implementado y su ubicación se describirán posteriormente.

- El tercer y último edificio será el ANEXO C; mantendrá la misma distribución que el anexo B (mismas funciones, equipos de cómputo y conexiones). De la misma manera, sólo se comunicará con la CENTRAL A.

1.2. MARCO TEÓRICO

1.2.1. Arquitectura de redes

Las primeras redes de cómputo tuvieron unos inicios muy similares a las primeras computadoras: las redes y los protocolos se diseñaban pensando en el hardware a utilizar en cada momento, sin tener en cuenta la evolución previsible, ni por supuesto la interconexión y compatibilidad con equipos de otros fabricantes. A medida que la tecnología avanzaba y

se mejoraba la red, los programas de comunicaciones que habían costado enormes esfuerzos de desarrollo, tenían que ser re-escritos para utilizarlos con el nuevo hardware, y debido a la poca modularidad, prácticamente nada del código era aprovechable.

El problema se resolvió de forma análoga a lo que se había hecho con las computadoras. Cada fabricante elaboró su propia *arquitectura de red,* que permitía independizar las funciones y el software del hardware concreto utilizado. De esta forma cuando se quería cambiar algún componente sólo la función o el módulo afectado tenía que ser sustituido. La primera arquitectura de redes fue anunciada por IBM en 1974, justo diez años después de anunciar la arquitectura S/360, y se denominó SNA[11]. La arquitectura SNA se basa en la definición de siete niveles o capas, cada una de las cuales ofrece una serie de servicios a la siguiente, la cual se apoya en ésta para implementar los suyos, y así sucesivamente. Cada capa puede implementarse en hardware, software o una combinación de ambos. El módulo (hardware y/o software) que implementa una capa en un determinado elemento de la red debe poder sustituirse sin afectar al resto de la misma, siempre y cuando el protocolo utilizado se mantenga inalterado. Dicho en otras palabras, SNA es una arquitectura altamente modular y estructurada.

El modelo de capas que utiliza SNA ha sido la base de todas las arquitecturas de redes actualmente en uso, incluidas las basadas en el modelo OSI[12] y el TCP/IP que veremos en detalle más adelante.

Las ideas básicas del modelo de capas son las siguientes:

- La capa *n* ofrece una serie de servicios a la capa *n+1*.
- La capa *n* solo 've' los servicios que le ofrece la capa *n-1*.
- La capa *n* en un determinado sistema sólo se comunica con su homóloga en el sistema remoto (comunicación de igual a igual o "peer-to-peer"). Esa "conversación" se efectúa de acuerdo con una serie de reglas conocidas como *protocolo de la capa n.*

La arquitectura de una red queda perfectamente especificada cuando se describen las capas que la componen, su funcionalidad, los servicios que implementan y los protocolos que utilizan para hablar con sus "iguales". El conjunto de protocolos que utiliza una determinada arquitectura en todas sus capas se denomina *pila de protocolos* ("protocol stack" en inglés); así es frecuente oír hablar de la pila de protocolos OSI, SNA, TCP/IP o DECNET, por ejemplo.

[11] SNA (Systems Network Architecture, Arquitectura Sistema de Redes)
[12] OSI (Open Systems Interconnection, Interconexión Sistema Abierto)

1.2.2. Modelos de Referencia

Las dos arquitecturas de redes más importantes en la actualidad son las correspondientes a los protocolos OSI y TCP/IP. Conviene destacar que la arquitectura es una entidad abstracta, más general que los protocolos o las implementaciones concretas en que luego se materializan éstos. Típicamente para cada capa de una arquitectura existirán uno o varios protocolos y para cada protocolo habrá múltiples implementaciones. Las implementaciones cambian continuamente; los protocolos ocasionalmente se modifican o aparecen otros nuevos que coexisten con los anteriores o los dejan anticuados; sin embargo una vez definida una arquitectura ésta permanece esencialmente intacta y muy raramente se modifica.

1.2.2.1 El Modelo de Referencia OSI

Entre 1977 y 1983 la ISO[13] definió la arquitectura de redes OSI con el fin de promover la creación de una serie de estándares que especificaran un conjunto de protocolos independientes de cualquier fabricante.

Seguramente la aportación más importante de la iniciativa OSI ha sido precisamente su arquitectura. Ésta ha servido como marco de referencia para describir multitud de redes correspondientes a diversas arquitecturas, ya que la arquitectura OSI es bien conocida en entornos de redes, y su generalidad y no dependencia de ningún fabricante en particular le hacen especialmente adecuada para estos fines. Por este motivo generalmente a la arquitectura OSI se la denomina *Modelo de Referencia OSI,* o también *OSIRM* (OSI Reference Model).

El modelo OSI define siete capas, curiosamente como en la arquitectura SNA si bien la funcionalidad es diferente. Las capas son las siguientes:

- *Física*
- *Enlace*
- *Red*
- *Transporte*
- *Sesión*
- *Presentación*
- *Aplicación*

La ISO ha especificado protocolos para todas las capas, aunque algunos son poco utilizados. En función del tipo de necesidades del usuario no siempre se utilizan todas ellas.

[13] ISO (International Organization for Standardization, Organización Internacional para la Estandarización)

- **La capa Física**

Esta capa transmite los bits entre dos entidades (nodos) directamente conectadas. La comunicación puede ser dúplex, semi-dúplex o simplex. Si la información se transmite por señales eléctricas se especifican los voltajes permitidos y su significado (1 ó 0) y análogamente para el caso de fibra óptica. Se especifican las características mecánicas del conector, la señalización básica, etc.

Como ejemplos de la capa física podemos mencionar las norma EIA RS-232-C, utilizada por las puertas COM de los ordenadores personales, la EIA-RS-449, CCITT X.21/X.21bis, CCITT V.35. Las normas de redes locales incluyen en sus especificaciones la capa física (IEEE[14] 802.3 o Ethernet, IEEE 802.5 o Token Ring, ISO 9314 o FDDI, etc.)

- **La capa de Enlace (data link)**

La principal función de la capa de enlace es ofrecer un servicio de comunicación fiable a partir de los servicios que recibe de la capa física, también entre dos entidades contiguas de la red. Esto supone que se realice detección y posiblemente corrección de errores. A diferencia de la capa física que transmitía los bits de manera continua, la capa de enlace transmite los bits en grupos denominados *tramas* (*frames* en inglés) cuyo tamaño es típicamente de unos pocos cientos a unos pocos miles de bytes. En caso de que una trama no haya sido transmitida correctamente se deberá enviar de nuevo; también debe haber mecanismos para reconocer cuando una trama se recibe duplicada. Generalmente se utiliza algún mecanismo de control de flujo, para evitar que un transmisor rápido pueda "abrumar" a un receptor lento.

Las redes "broadcast" utilizan funciones especiales de la capa de enlace para controlar el acceso al medio de transmisión, ya que éste es compartido por todos los nodos de la red. Esto añade una complejidad a la capa de enlace que no está presente en las redes basadas en líneas punto a punto, razón por la cual en las redes "broadcast" la capa de enlace se subdivide en dos subcapas: la inferior, denominada subcapa MAC[15] se ocupa de resolver el problema de acceso al medio, y la superior, subcapa LLC[16] cumple una función equivalente a la capa de enlace en las líneas punto a punto.

Ejemplos de protocolos de la capa de enlace son el ISO 7776, la capa de enlace de X.25 (de la ITU) o el ISO HDLC. Como ejemplos de protocolos de la subcapa MAC podemos citar los IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring[17]) o el ISO 9314 (FDDI). El protocolo de subcapa LLC de todas las redes locales "broadcast" es el IEEE 802.2.

[14] IEEE (Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos)
[15] MAC (Media Access Control , Control de Acceso al Medio)
[16] LLC (Logical Link Control, Control de Enlace Lógico)
[17] Token Ring (Red local desarrollada por IBM que utiliza el protocolo de acceso Token Passing y que utiliza un ancho de banda de 4 y 16 Mbps. Utiliza la topología de anillo)

- **La capa de Red**

La capa de red se ocupa del control de la subred. Ésta es la capa que tiene "conciencia" de la topología de la red y se ocupa de decidir por que ruta va a ser enviada la información; la decisión de la ruta a seguir puede hacerse de forma estática, o de forma dinámica con base en la información obtenida de otros nodos sobre el estado de la red. Además cabe destacar el control del tráfico para evitar situaciones de congestión o "atascos".

De forma análoga a la capa de enlace la capa de red maneja los bits en grupos discretos que aquí reciben el nombre de *paquetes*; motivo por el cual a veces se la llama la capa de paquete. Los paquetes tienen tamaños variables, pudiendo llegar a ser muy elevados, sobre todo en protocolos recientes, para poder aprovechar eficientemente la elevada velocidad de los nuevos medios de transmisión (fibra óptica, ATM, etc.). Por ejemplo en TCP/IP el tamaño máximo de paquete es de 64 KBytes, pero en el nuevo estándar, llamado IPv6, el tamaño máximo puede llegar a ser de 4 GBytes (4.294.967.296 Bytes).

La capa de red es la más importante en redes de conmutación de paquetes (tales como X.25 o TCP/IP). Algunos ejemplos de protocolos utilizados en la capa de red son los protocolos de nivel de paquete y nivel de pasarela CCITT X.25 y X.75, el IP (Internet Protocol), CCITT/ITU-T Q.931, Q.933, Q.2931, y el OSI CLNP (Connection Less Network Protocol).

- **La capa de Transporte**

La capa de transporte es la primera que se ocupa de comunicar directamente nodos terminales, utilizando la subred como un medio de transporte transparente gracias a los servicios obtenidos de la capa de red.

La principal función de la capa de transporte es fragmentar de forma adecuada los datos recibidos de la capa superior (sesión) para transferirlos a la capa de red, y asegurar que los fragmentos llegan y son recompuestos correctamente en su destino.

La capa de transporte establece el tipo de servicio que recibe la capa de sesión, y en último extremo los usuarios. El control de flujo que ha aparecido en capas anteriores, es necesario también en la capa de transporte para asegurar que un "host"[18] rápido no satura a uno lento. La capa de transporte realiza también su propio control de errores, que resulta ahora esencial pues algunos protocolos modernos como Frame Relay[19] o ATM han reducido o suprimido totalmente el control de errores de las capas inferiores, ya que con las mejoras en

[18] Host (Organizador) Computadora a la que tenemos acceso de diversas formas (telnet, ftp, world wide web, etc). Es el servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente.

[19] Frame Relay: En el contexto de una red Frame Relay son los datos que usan el ancho de banda solo esporádicamente, esto es, que la información no utiliza el ancho de banda el 100% del tiempo. El tráfico interactivo y entre LANs es de esta naturaleza debido a que los datos se envían intermitentemente.

la tecnología de transmisión de datos, éstos son menos frecuentes y se considera más adecuado realizar esta tarea en el nivel de transporte.

Ejemplos de protocolos de transporte incluyen el CCITT X.224, también llamado protocolo de transporte OSI TP4 (Transport Protocol 4). En Internet existen dos protocolos de transporte: TCP y UDP.

- **La capa de Sesión**

La capa de sesión es la primera que es accesible al usuario y es su interfaz más básica con la red. Por ejemplo, mediante los servicios de la capa de sesión un usuario podría establecer una conexión como terminal remoto de otra computadora.

- **La capa de Presentación**

La capa de presentación se ocupa de realizar las conversiones necesarias para asegurar que dichos bits se presentan al usuario de la forma esperada. Por ejemplo, si se envía información alfanumérica de una computadora ASCII[20] a uno EBCDIC será preciso efectuar una conversión, o de lo contrario los datos no serán interpretados correctamente. Lo mismo podríamos decir de la transferencia de datos enteros, flotantes, etc., cuando la representación de los datos difiere en las computadoras utilizadas.

- **La capa de Aplicación**

La capa de aplicación comprende los servicios que el usuario final está acostumbrado a utilizar en una red de cómputo, por lo que a menudo los protocolos de la capa de aplicación se denominan *servicios*. Dado que se crean continuamente nuevos servicios, existen muchos protocolos para la capa de aplicación, uno o más por cada tipo de servicio.

Ejemplos de protocolos estándar de la capa de aplicación son el X.400 o X.500 de la ITU, los protocolos SMTP, FTP[21] y HTTP de Internet, etc.

1.2.2.2 El Modelo de Referencia TCP/IP

En 1969 la agencia ARPA del Departamento de Defensa (DoD, Department of Defense) de los Estados Unidos inició un proyecto de interconexión de ordenadores mediante redes

[20] ASCII (American Standard Code for Information Interchange). Es el código numérico usado en computación para representar todos los caracteres del alfabeto, números, símbolos, etc. Está compuesto por 128 códigos estándares representados por un conjunto de 7 dígitos binarios.

[21] FTP (File Transfer Protocol, Protocolo de transferencia de archivos). Uno de los servicios más comunes de Internet el cual permite obtener o enviar archivos. Incluso existen muchos sitios en Internet que suministran información gratuita contenidas en archivos y que pueden ser accesadas usando el protocolo FTP, usando para tal efecto el nombre de cuenta anonymous.

telefónicas. Esto se consiguió en 1972 creando una red de conmutación de paquetes denominada ARPANET, la primera de este tipo que operó en el mundo.

La ARPANET fue creciendo paulatinamente y pronto se hicieron experimentos utilizando otros medios de transmisión de datos, en particular enlaces por radio y vía satélite; los protocolos existentes tuvieron problemas para ínter-operar con estas redes, por lo que se diseñó un nuevo conjunto o pila de protocolos y con ellos una arquitectura. Este nuevo conjunto se denominó TCP/IP (Transmission Control Protocol/Internet Protocol, Protocolo de Control de Transmisión / Protocolo Internet) nombre que provenía de los dos protocolos más importantes que componían la pila; la nueva arquitectura se llamó sencillamente *modelo TCP/IP*, los nuevos protocolos fueron especificados por vez primera por Cerf y Kahn en un artículo publicado en 1974. A la nueva red, que se creó como consecuencia de la fusión de ARPANET con las redes basadas en otras tecnologías de transmisión, se la denominó Internet.

En el modelo TCP/IP se pueden distinguir cuatro capas:

- La capa Host-Red
- La capa Internet
- La capa de Transporte
- La capa de Aplicación

- **La capa Host-Red**

Esta capa engloba realmente las funciones de la capa física y la capa de enlace del modelo OSI. El modelo TCP/IP no dice gran cosa respecto a ella, salvo que debe ser capaz de conectar el "host" a la red por medio de algún protocolo que permita enviar paquetes IP. Podríamos decir que para el modelo TCP/IP esta capa se comporta como una "caja negra". Cuando surge una nueva tecnología de red (por ejemplo ATM, Asynchronous Transmissión Mode, Transmisión Modo Asíncrono) una de las primeras cosas que aparece es un estándar que especifica de que forma se pueden enviar sobre ella paquetes IP; a partir de ahí la capa Internet ya puede utilizar esa tecnología de manera transparente.

- **La capa Internet**

Esta capa es el "corazón" de la red. Su papel equivale al desempeñado por la capa de red en el modelo OSI; es decir, se ocupa de encaminar los paquetes de la forma más conveniente para que lleguen a su destino y de evitar que se produzcan situaciones de congestión en los nodos intermedios. Debido a los requisitos de robustez impuestos en el diseño, la capa Internet da únicamente un servicio de conmutación de paquetes no orientado a conexión. Los paquetes pueden llegar desordenados a su destino, en cuyo caso es responsabilidad de las capas superiores en el nodo receptor la reordenación para que sean presentados al usuario de forma adecuada.

A diferencia de lo que ocurre en el modelo OSI, donde los protocolos para nada intervienen en la descripción del modelo, la capa Internet define aquí un formato de paquete y un protocolo, llamado IP (Protocolo Internet) que se considera el protocolo "oficial" de la arquitectura.

- **La capa de Transporte**

Esta capa recibe el mismo nombre y desarrolla la misma función que la cuarta capa del modelo OSI, consistente en permitir la comunicación extremo a extremo (host a host) en la red. Aquí se definen dos protocolos: el TCP ofrece un servicio confiable, con lo que los paquetes (llamados segmentos) llegan ordenados y sin errores. TCP se ocupa también del control de flujo extremo a extremo, para evitar que por ejemplo un "host" rápido sature a un receptor más lento. Ejemplos de protocolos de aplicación que utilizan TCP son el SMTP[22] y el FTP.

El otro protocolo de transporte es UDP[23] que da un servicio CLNS, no fiable. UDP no realiza control de errores ni de flujo. Una aplicación típica donde se utiliza UDP es la transmisión de voz y vídeo en tiempo real; aquí el retardo que introduciría el control de errores produciría más daño que beneficio: es preferible perder algún paquete que retransmitirlo fuera de tiempo. Otro ejemplo de aplicación que utiliza UDP es el NFS (Network File System); aquí el control de errores y de flujo se realiza en la capa de aplicación.

- **La capa de Aplicación**

Esta capa desarrolla las funciones de las capas de sesión, presentación y aplicación del modelo OSI. La experiencia ha demostrado que las capas de sesión y presentación son de poca utilidad, debido a su escaso contenido, por lo que la aproximación adoptada por el modelo TCP/IP parece más acertada.

La capa de aplicación contiene todos los protocolos de alto nivel que se utilizan para ofrecer servicios a los usuarios. Entre estos podemos mencionar tanto los "tradicionales", que existen desde que se creó el TCP/IP: terminal virtual (TelNet), transferencia de ficheros (FTP[24]), correo electrónico (SMTP) y servidor de nombres (DNS), como los más recientes, como el servicio de news (NNTP), el Web (HTTP[25]), el Gopher, etc.

En la Tabla 1.1 hacemos un resumen del modelo y los protocolos más comunes de cada capa.

[22] SMTP (Simple Mail Transfer Program, Programa Transferencia de Correo Simple, correo electrónico)
[23] UDP (User Datagram Protocol, Protocolo Datagrama Usuario)
[24] FTP (File Transfer Protocol, Protocolo Transferencia Archivo)
[25] HTTP (Protocolo de transmisión de Hipertexto). Protocolo usado para la transferencia de documentos WWW.

CAPA	PROTOCOLO
Aplicación	TCP/IP (DNS, SMTP, SNMP, NNTP, HTTP)
Transporte	TCP/IP (TCP, UDP) ATM (AAL1, AAL2, AAL3/4, AAL5)
Red	TCP/IP (IP, ICMP, ARP, RARP, OSPF, BGP, IPv6), ATM (Q2931)
Enlace	ISO(HDLC), TCP/IP (SLIP, PPP), ATM, LANs
Física	N-ISDN, B-ISDN (ATM), GSM, SONET/SDH, LANs Cable coaxial, cable UTP, fibra óptica, microondas, radio enlaces, satélite

Tabla 1.1. Ejemplos de protocolos en cada uno de los niveles del modelo de red OSI-TCP/IP

1.3. TECNOLOGÍA DE REDES

Aquí empezaremos a describir los medios de transmisión utilizados en la estructura e implementación del soporte físico de una red de cómputo, así como la comparación entre las diferentes características y ventajas de cada medio usado para el envío de datos por la red. La mayor parte de las redes existentes en la actualidad utilizan como medio de transmisión cable bifilar o par trenzado y el cable de fibra óptica; pero también se utiliza el medio inalámbrico que será el más detallado en esta parte.

Cualquier medio físico 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.

1.3.1. Par Trenzado

Describiremos las características generales de este medio así como las ventajas y desventajas del mismo:

- Es el tipo de cable más común y se originó como solución para conectar teléfonos, terminales y ordenadores sobre el mismo cableado, ya que está habilitado para comunicación de datos permitiendo frecuencias más altas de transmisión. Con anterioridad, en Europa, los sistemas de telefonía empleaban cables de pares no trenzados.

- Cada cable de este tipo está compuesto por una serie de pares de cables trenzados. Los pares se trenzan para reducir la interferencia entre pares adyacentes. Normalmente una serie de pares se agrupan en una única funda de color codificado para reducir el número de cables físicos que se introducen en un conducto. El número de pares por cable son 4, 25, 50, 100, 200 y 300. Cuando el número de pares es superior a 4 se habla de cables multipar.

Tipos de cables de par trenzado:

❖ **No blindado.** Es el cable de par trenzado normal y se le referencia por sus siglas en inglés UTP (*Unshield Twisted Pair*; Par Trenzado no Blindado). Las mayores ventajas de este tipo de cable son su bajo costo y su facilidad de manejo. Sus mayores desventajas son su mayor tasa de error respecto a otros tipos de cable, así como sus limitaciones para trabajar a distancias elevadas sin regeneración.

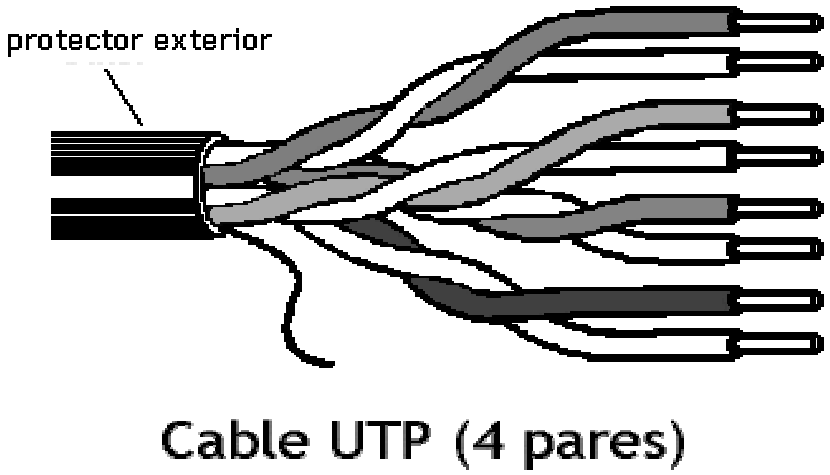


Figura 1.2. Par Trenzado

Para las distintas tecnologías de red local, el cable de pares de cobre no blindado se ha convertido en el sistema de cableado más ampliamente utilizado.

El estándar del E1 el EIA-568 en el adendum el TSB-36 diferencia tres categorías distintas para este tipo de los cables:

- Categoría 3: Admiten frecuencias de hasta 16 MHz
- Categoría 4: Admiten frecuencias de hasta 20 MHz
- Categoría 5: Admiten frecuencias de hasta 100 MHz

Las características generales del cable no blindado son:

- **Tamaño:** El menor diámetro de los cables de par trenzado no blindado permite aprovechar más eficientemente las canalizaciones y los armarios de distribución. El diámetro típico de estos cables es de 0.52 cm.
- **Peso:** El poco peso de este tipo de cable con respecto a los otros tipos de cable facilita el tendido.
- **Flexibilidad:** La facilidad para curvar y doblar este tipo de cables permite un tendido más rápido así como el conexionado de las rosetas y las regletas.
- **Instalación:** Debido a la amplia difusión de este tipo de cables, existen una gran variedad de suministradores, instaladores y herramientas que abaratan la instalación y puesta en marcha.
- **Integración:** Los servicios soportados por este tipo de cable incluyen:

  - Red de Área Local ISO 8802.3 (Ethernet) e ISO 8802.5 (Token Ring).
  - Telefonía analógica.
  - Telefonía digital.
  - Terminales síncronos.
  - Terminales asíncronos.
  - Líneas de control y alarmas.

❖ **Blindado.** Cada par se cubre con una malla metálica, de la misma forma que los cables coaxiales, y el conjunto de pares se recubre con una lámina blindada. Se referencia frecuentemente con sus siglas en inglés STP (*Shield Twisted Pair*, Par Trenzado blindado).

El empleo de una malla blindada reduce la tasa de error, pero incrementa el coste al requerirse un proceso de fabricación más costoso.

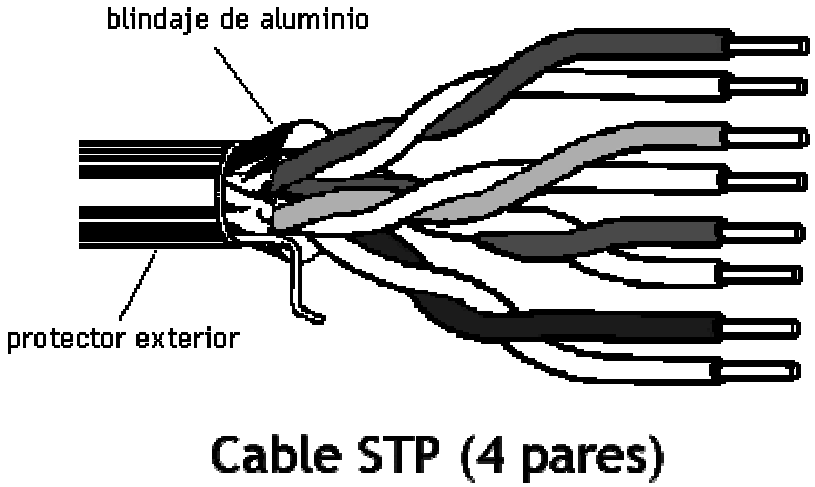


Figura 1.3. Par Trenzado Blindado

❖ **Uniforme**. Cada uno de los pares es trenzado uniformemente durante su creación. Esto elimina la mayoría de las interferencias entre cables y además protege al conjunto de los cables de interferencias exteriores. Se realiza un blindaje global de todos los pares mediante una lámina externa blindada. Esta técnica permite tener características similares al cable blindado con unos costes por metro ligeramente inferior.

Tipo	Uso
Categoría 1	Voz solamente (cable telefónico)
Categoría 2	Datos hasta 4 Mbps (Local Talk [Apple])
Categoría 3	Datos hasta 10 Mbps (Ethernet)
Categoría 4	Datos hasta 20 Mbps (16 Mbps Token Ring)
Categoría 5	Datos hasta 100 Mbps

Tabla 1.2. Categorías de Cables UTP

Especificación	Tipo de Cable	Long. Máxima
10BaseT	UTP	100 metros
10Base2	Thin Coaxial	185 metros
10Base5	Thick Coaxial	500 metros
10BaseF	Fibra Óptica	2000 metros
100BaseT	UTP	100 metros
100BaseTX	UTP	220 metros

Tabla 1.3. Sumario -Cable Ethernet

Ventajas y Desventajas:

El cable par trenzado está compuesto por conductores de cobre aislados por material plástico y trenzados en pares. Dicho trenzado, que en promedio abarca tres trenzas por pulgada, ayuda a disminuir la diafonía, el ruido e interferencia, para mejores resultados, el trenzado debe ser variado entre los diferentes pares.

Este tipo de cable tiene la ventaja de ser económico, flexible y fácil de conectar, entre otras propiedades que no presenta el coaxial en las aplicaciones de redes. No obstante, como medio de comunicación existe la desventaja de tener que usarse a distancias limitadas (menos de 100 metros), ya que la señal se va atenuando y pudiera llegar a ser imperceptible si se rebasa el límite mencionado.

Los cables de par trenzado más comúnmente usados como interfaces de capa física son los siguientes:

Especificación	Interfaz de capa física
10BaseT	Ethernet
100BaseTX	Fast Ethernet
100BaseT4	Fast Ethernet con 4 pares
1000BaseT	Gigabit Ethernet

Tabla 1.4. Cables según la interfaz de capa física

1.3.2. Fibra Óptica

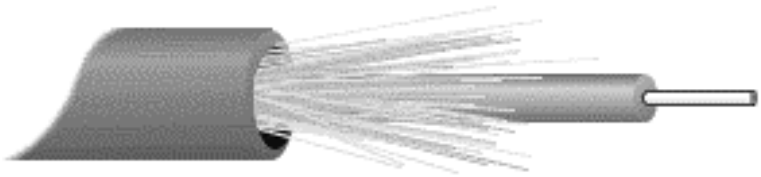


Figura 1.4. Fibra Óptica

Los circuitos de fibra óptica son filamentos de vidrio flexibles, del espesor de un cabello, llevan mensajes en forma de haces de luz que realmente pasan a través de ellos de un extremo a otro, donde quiera que el filamento vaya (incluyendo curvas y esquinas) sin interrupción.

Las fibras ópticas pueden ahora usarse como los alambres de cobre convencionales, tanto en pequeños ambientes autónomos (tales como sistemas de procesamiento de datos de aviones), como en grandes redes geográficas (como los sistemas de largas líneas urbanas mantenidos por compañías telefónicas).

Este cable está constituido por uno o más hilos de fibra de vidrio. Cada fibra de vidrio consta de:

- Un núcleo central de fibra con un alto índice de refracción.
- Una cubierta que rodea al núcleo, de material similar, con un índice de refracción ligeramente menor.
- Una envoltura que aísla las fibras y evita que se produzcan interferencias entre fibras adyacentes, a la vez que proporciona protección al núcleo. Cada una de ellas está rodeada por un revestimiento y reforzada para proteger a la fibra.

La luz producida por diodos o por láser, viaja a través del núcleo debido a la reflexión que se produce en la cubierta y es convertida en señal eléctrica en el extremo receptor.

La fibra óptica es un medio excelente para la transmisión de información debido a sus excelentes características: gran ancho de banda, baja atenuación de la señal, integridad, inmunidad a interferencias electromagnéticas, alta seguridad y larga duración. Su mayor desventaja es su coste de producción superior al resto de los tipos de cable, debido a necesitarse el empleo de vidrio de alta calidad y la fragilidad de su manejo en producción. La terminación de los cables de fibra óptica requiere un tratamiento especial que ocasiona un aumento de los costes de instalación.

Uno de los parámetros más característicos de las fibras es su relación entre los índices de refracción del núcleo y de la cubierta que depende también del radio del núcleo y que se denomina frecuencia fundamental o normalizada; también se conoce como apertura numérica y es adimensional. Según el *valor de este parámetro* se pueden clasificar los cables de fibra óptica en dos clases:

❖ **Modo Simple (o Unimodal).** Cuando el valor de la apertura numérica es inferior a 2'405 (frecuencia fundamental), un único modo electromagnético viaja a través de la línea; es decir, una sola vía y por tanto ésta se denomina Modo Simple. Este tipo de fibra necesita el empleo de emisores láser para la inyección de la luz, lo que proporciona un gran ancho de banda y una baja atenuación con la distancia, por lo que son utilizadas en redes metropolitanas y redes de área extensa. Resultan más caras de producir y el equipamiento es más sofisticado.

❖ **Multimodo**. Cuando el valor de la apertura numérica es superior a 2'405 (frecuencia fundamental), se transmiten varios modos electromagnéticos por la fibra, denominándose por este motivo fibra multimodo. Las fibras multimodo son las más utilizadas en las redes locales por su bajo coste. Los diámetros más frecuentes 62.5/125 y 100/140 micras. Las distancias de transmisión de este tipo de fibras están alrededor de los 2.4 Km. y se utilizan a diferentes velocidades: 10 Mbps, 16 Mbps y 100 Mbps.

Las características generales de la fibra óptica son:

- **Ancho de banda.** La fibra óptica proporciona un ancho de banda significativamente mayor que los cables de pares (blindado/no blindado) y el Coaxial. Aunque en la actualidad se están utilizando velocidades de 1.7 Gbps en las redes públicas, la utilización de frecuencias más altas (luz visible) permitirá alcanzar los 39 Gbps. El ancho de banda de la fibra óptica permite transmitir datos, voz, vídeo, etc.
- **Distancia.** La baja atenuación de la señal óptica permite realizar tendidos de fibra óptica sin necesidad de repetidores.
- **Integridad de datos.** En condiciones normales, una transmisión de datos por fibra óptica tiene una frecuencia de errores o BER (*Bit Error Rate*) menor de $10E^{-11}$. Esta característica permite que los protocolos de comunicaciones de alto nivel, no necesiten implantar procedimientos de corrección de errores por lo que se acelera la velocidad de transferencia.
- **Duración.** La fibra óptica es resistente a la corrosión y a las altas temperaturas. Gracias a la protección de la envoltura es capaz de soportar esfuerzos elevados de tensión en la instalación.
- **Seguridad.** Debido a que la fibra óptica no produce radiación electromagnética, es resistente a las acciones intrusivas de escucha. Para acceder a la señal que circula en la fibra es necesario partirla, con lo cual no hay transmisión durante este proceso, y puede por tanto detectarse.

Ventajas:

- Insensibilidad a la interferencia electromagnética, como ocurre cuando un alambre telefónico pierde parte de su señal a otro.
- Las fibras no pierden luz, por lo que la transmisión es también segura y no puede ser perturbada.
- Carencia de señales eléctricas en la fibra, por lo que no pueden dar sacudidas ni otros peligros. Son convenientes por lo tanto para trabajar en ambientes explosivos.
- Liviandad y reducido tamaño del cable capaz de llevar un gran número de señales.
- Sin puesta a tierra de señales, como ocurre con alambres de cobre que quedan en contacto con ambientes metálicos.
- Compatibilidad con la tecnología digital.
- Fácil de instalar.

Desventajas:

- El costo.
- Fragilidad de las fibras.
- Disponibilidad limitada de conectores.
- Dificultad de reparar un cable de fibras roto en el campo.

Aplicaciones Comerciales:

a) Portadores comunes telefónicos y no telefónicos.
b) Televisión por cable.
c) Enlaces y bucles locales de estaciones terrestres.
d) Automatización industrial.
e) Controles de procesos.
f) Aplicaciones de computadora.
g) Aplicaciones militares.

1.3.3. Redes Inalámbricas

Figura 1.5. Punto de Acceso Inalámbrico

¿Qué es una red inalámbrica? Es una red que provee la funcionalidad y los beneficios que ofrecen las redes como Ethernet, pero sin la limitante de los cables. La infraestructura inalámbrica se puede mover a la velocidad de la organización.

Esta tecnología tiene aplicaciones inmediatas como:

- Cuando se desea movilidad dentro de la organización, tal vez en adición a la red de cableado.
- Cuando se necesita flexibilidad para realizar cambios y movimientos dentro de la organización, o en algunas áreas específicas.
- Cuando el edificio no permite la instalación de cables.
- Cualquier organización que requiera flexibilidad y obtener ahorros eliminando rentas de enlaces probados.

En nuestros días las redes de computadoras están presentes en todas las empresas. Desde la más pequeña, de solo un par de máquinas, hasta las más sofisticadas que cubren bastas áreas geográficas. Pero existen limitaciones cuando se trabaja con redes extensas, especialmente si se trata de comunicar dos puntos distantes: a escasos metros, en edificios

con problemas de instalación de cableado o distancias donde no llega el tendido de cables, un par de kilómetros uno del otro, etc.

La solución más común a este inconveniente es la utilización de líneas telefónicas o de fibra óptica para lograr la transmisión de datos. Lamentablemente éstas suelen transportar información a poca velocidad o se transforman en muy costosas. Sin embargo, gracias a los avances tecnológicos en telecomunicaciones, se ha conseguido transmitir datos a grandes distancias, con velocidades de hasta 11 ó incluso 54 Mbps, a un muy bajo costo.

Básicamente, ellos son radio módems que permiten comunicar computadoras punto a punto o como punto a multipunto con Access Points (Puntos de Acceso). Una conveniente prestación de estos dispositivos reside en el acceso a Internet, ya que es posible proveer conexión a la red mundial, a través de este sistema inalámbrico, llegando a lugares ajenos a las últimas tecnologías (ADSL[26], fibra óptica, etc.)

Otro punto a favor para la implementación de esta tecnología es la frecuencia de trabajo que es de 2.4 Ghz, una frecuencia libre (ISM Band[27]) y no requiere licencia para la transmisión de datos ante la CNC (Comisión Nacional de Comunicaciones) lo cual disminuye notablemente el costo final de su implementación.

Contrariamente a lo que se piensa, una de sus grandes ventajas radica en su empleo como red fija, pues son múltiples los beneficios que ofrecen frente a la instalación de cableado estructurado convencional. Es ésta una faceta todavía relativamente desconocida pero que puede reportar un fuerte impulso a su introducción en el ambiente empresarial y residencial. Se puede aplicar tanto a redes de área local (LANs) dentro de la empresa como en la interconexión de redes de edificios próximos que anteriormente mencionamos, en la que la solución cableada requiere complejas tramitaciones o es obligado la contratación de la línea de datos a un operador de red con licencia para operar públicamente.

1.3.3.1 Configuraciones en Redes Inalámbricas

A continuación se enumerarán las posibles configuraciones disponibles para equipos en red inalámbrica.

Red peer-to-peer (igual a igual).

La más básica se da entre dos computadoras equipadas con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que

[26] ADSL (Línea suscriptor digital de abonado) es una técnica de transmisión que, aplicada sobre los abonados de la red telefónica, permite la transmisión de voz y datos a altas velocidades.
[27] ISM Band (Industrial, Scientific and Medical; Industrial, Científica y Medica) es un conjunto de anchos de banda para uso no regulado, en la llamada Banda ISM el espectro de operación se encuentra cerca de los 2.4GHz. En particular, está comenzando a ser disponible en todo el mundo; esto representa una oportunidad verdaderamente revolucionaria para ubicar convenientes capacidades de redes inalámbricas a altas velocidades en las manos de los usuarios alrededor del globo.

estén dentro del área que cubre cada uno. Esto es llamado red de igual a igual (a veces llamado modo Ad-Hoc). Cada cliente tendría únicamente acceso a los recursos de otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o preconfiguración.

Figura 1.6. Red peer-to-peer (Red punto a punto)

Red con único punto de acceso.

Instalando un Punto de Acceso (AP – Access Point) se puede doblar el rango al cual los dispositivos pueden comunicarse, pues actúan como repetidores. Desde que el punto de acceso se conecta a la red cableada, cualquier cliente tiene acceso a los recursos del servidor y además actúan como mediadores en el tráfico de la red en la vecindad más inmediata. Cada punto de acceso puede servir a varios clientes, según la naturaleza y número de transmisiones que tienen lugar. Existen muchas aplicaciones en el mundo real utilizando entre 15 y 50 dispositivos cliente en un solo punto de acceso.

Figura 1.7. Cliente y Punto de Acceso

Red con varios puntos de acceso.

Los puntos de acceso tienen un rango finito, del orden de 100m en lugares cerrados y alrededor de 20 km en zonas abiertas (dependiendo de las antenas). En zonas grandes como por ejemplo un campus universitario o un edificio es probablemente necesario más de un punto de acceso. La meta es cubrir el área con células que solapen sus áreas de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso. Esto es llamado "roaming" (vagando).

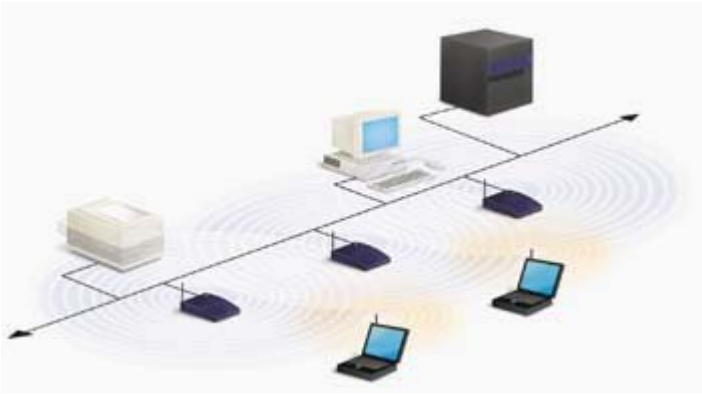


Figura 1.8. Múltiples Puntos de Acceso y "roaming"

Red con puntos de extensión.

Para resolver problemas particulares de topología, el diseñador de la red puede elegir usar un Punto de Extensión (EP – Extension Points) para aumentar el número de puntos de acceso a la red, de modo que funcionan como tales pero no están enganchados a la red cableada como los puntos de acceso. Los puntos de extensión funcionan como su nombre indica: extienden el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión. Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos.

Figura 1.9. Uso de un punto de extensión

1.3.3.2 Redes Locales Inalámbricas (WLAN)

En los últimos años, las redes inalámbricas (WLAN: Wireless Local Area Network) han ganado muchos adeptos y popularidad en mercados verticales, tales como hospitales, fábricas, bodegas, tiendas de autoservicio, tiendas departamentales, pequeños negocios y áreas académicas. Las Redes Inalámbricas WLAN proporcionan todas las características y ventajas de las tecnologías tradicionales LAN, como Ethernet y Fast Ethernet sin las limitaciones que imponen los cables, a través de la tecnología de Radiofrecuencia o Láser.

Al igual que las habituales redes LAN Ethernet 802.3 donde el medio físico es un cable de par trenzado o fibra óptica compartido, en las redes WLAN el medio de transmisión es el espacio abierto, empleando para ello ondas de radiofrecuencia (RF) o infrarrojos (IR). Las redes locales inalámbricas están enfocadas para solucionar los requerimientos de conectividad y desplazamiento de usuarios y dispositivos en corporaciones, instituciones educativas, naves industriales, centros de distribución, hoteles, museos, bibliotecas, etc.

Las redes inalámbricas permiten a los usuarios acceder a información y recursos, en tiempo real, sin necesidad de estar físicamente en un solo lugar. Con WLANs, la red por sí misma es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante, incrementa la productividad y eficiencia en las actividades diarias de la empresa. Un usuario dentro de una red inalámbrica, puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de hasta 11 Mbps. Muchos de los fabricantes de computadoras y equipos de comunicaciones como módems, microprocesadores inalámbricos, lectores de punto de venta y otros dispositivos, están introduciendo aplicaciones en soporte a las comunicaciones inalámbricas. Las nuevas posibilidades que ofrecen las WLANs, son permitir una fácil incorporación de nuevos usuarios a la red, ofrecen una alternativa de bajo costo a los sistemas cableados, además de la posibilidad ubicua para entrar a cualquier base de datos o cualquier aplicación localizada dentro de la red. A continuación se resumen algunas de estas ventajas de las WLANs, concernientes a productividad, conveniencia y costo, en comparación con las redes cableadas.

Características Principales de Instalación de una WLANs

- *Movilidad.* Las redes inalámbricas pueden proveer a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red cableada.

- *Simplicidad en la instalación.* La instalación de una red inalámbrica puede ser tan fácil y además puede eliminar la posibilidad de tirar cable a través de paredes y techos.

- *Flexibilidad en la instalación.* La tecnología inalámbrica permite a la red ir donde la cableada no puede ir.

- *Costo de propiedad reducido.* Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN alámbrica, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los beneficios y costos a largo plazo, son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.
- *Escalabilidad.* Los sistemas de WLANs pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

Ventajas de Implementación de una Red Local Inalámbrica (WLANs):

- **Economía.** El costo de despliegue de una WLAN puede variar comparado en cuestión de un cableado de edificio a edificio ya que con un "Access Point" se supliría todo el cable, dependiendo notablemente de los requerimientos (seguridad, calidad, bitrate[28]) y de las características del lugar de implantación. En el caso de una red cableada, el coste se dispararía notablemente, donde la gran dispersión en el presupuesto se atribuye fundamentalmente a la problemática asociada despliegue físico del cableado. Algunos especialistas han publicado un estudio que va todavía más lejos, llegando a afirmar que la reducción del costo por la implantación de una red inalámbrica puede suponer ahorros de hasta un 95% frente a un despliegue tradicional.

- **Rapidez de implantación.** Por lo general, la tarea que suele consumir mayor tiempo en la instalación de una red inalámbrica es paradójicamente la parte cableada que se emplea para enlazar los puntos de acceso con la red local de la empresa. Aún así se mide en días la duración de un proyecto, siempre dependiendo de su envergadura. En el caso de redes fijas, no son días sino habitualmente semanas. Esto es, en muchos casos un factor decisivo para ciertos proyectos. También cada vez se ven más casos de despliegues primeros o ampliaciones de infraestructura que por necesidades urgentes se inician por la construcción de una red inalámbrica para posteriormente consolidarse con una cableada, aunque manteniendo la primera para temas de movilidad y atender los requerimientos de ciertos usuarios.

- **Estética.** Las instalaciones de redes locales se caracterizan por la existencia de infinidad de rosetas (cajas de conexiones) próximas a cada puesto de trabajo, canalizaciones generalmente visibles y cables desde las PCs (computadoras personales) hasta el punto de conexión más próximo. Todo ello y debido a la cada vez mayor densidad de equipos, impacta de forma muy negativa en la estética del entorno de trabajo. Como contrapartida, en una instalación inalámbrica desaparecen los cables de las PCs y las rosetas, así como se reducen al mínimo las canalizaciones visibles. Este factor, siempre bien valorado, en ocasiones se convierte en fundamental, decidiendo la tecnología de la red a implantar.

- **Provisionalidad.** Las WLANs tienen una gran utilidad en instalaciones que tienen carácter de provisionalidad. Ejemplos de ello son infraestructuras itinerantes (ferias, congresos, demostradores) despliegues cortos o limitados en el tiempo (oficinas temporales) para absorber fuertes picos de utilización ocasional (las WLAN pueden soportar un número elevado de usuarios transitorios, mientras que las fijas están limitadas a las conexiones ya cableadas exclusivamente) y para permitir crecimientos urgentes en una red ya establecida hasta adoptar otras alternativas. Las razones que soportan esta característica frente a la solución cableada son múltiples: economía, escalabilidad, rapidez de implantación, movilidad, etc.

[28] Bitrate: Tasa de transferencia de bits por segundo.

- **Robustez.** Las redes basadas en cableado estructurado son por lo general más robustas frente a interferencias y condiciones adversas que las inalámbricas. Sin embargo en ciertos entornos en fábricas con elevada humedad, agentes químicos agresivos, calor, etc., las instalaciones cableadas pueden sufrir una rápida degradación o ser inviables. Una instalación inalámbrica adecuadamente ubicada para resguardarse de dichas inclemencias puede ser la alternativa idónea.

Desventajas de las Redes locales Inalámbricas (WLANs):

Obviamente no todas son ventajas de las redes inalámbricas frente a las cableadas:

Hay una serie de parámetros en lo que las últimas ofrecen mayores prestaciones. La velocidad binaria es mucho mayor, obteniéndose en general límites máximos de 100 Mbps por puesto (Fast Ethernet) frente a 54 Mbps en una WLAN (802.11g) compartidos entre varios usuarios. Son asimismo más inmunes a interferencias, más seguras y requieren de un menor mantenimiento. Estas desventajas pueden ser realmente importantes o casi insignificantes dependiendo de la calidad de la implantación.

WLAN en la Industria:

- **Corporaciones.** Con WLAN los empleados pueden beneficiarse de una red móvil para el correo electrónico, compartir archivos y visualización de WEB´s, independientemente de dónde se ubiquen en la oficina.

- **Educación.** Las instituciones académicas que soportan este tipo de conexión móvil permiten a los usuarios con computadoras conectarse a la red de la universidad para intercambio de opiniones en las clases, para acceso a internet, etc.

- **Finanzas.** Mediante una PC portátil y un adaptador a la red WLAN, los representantes pueden recibir información desde una base de datos en tiempo real y mejorar la velocidad y calidad de los negocios. Los grupos de auditorias contables incrementan su productividad con una rápida puesta a punto de una red.

- **Cuidado de la salud.** WLAN permite obtener información en tiempo real, por lo que proporciona un incremento de la productividad y calidad del cuidado del paciente eliminando el retardo en el tratamiento del paciente, los papeles redundantes, los posibles errores de trascripción, etc.

- **Restaurantes y venta al por menor.** Los servicios de restaurantes pueden utilizar WLAN para directamente entrar y enviar los pedidos de comida a la mesa. En los almacenes de ventas al por menor un WLAN se puede usar para actualizar temporalmente registros para eventos especiales.

- **Manufacturación.** WLAN ayuda al enlace entre las estaciones de trabajo de los pisos de la fábrica con los dispositivos de adquisición de datos de la red de la compañía.

- **Almacenes.** En los almacenes, terminales de datos con lectores de código de barras y enlaces con redes WLAN, son usados para introducir datos y mantener la posición de las paletas y cajas. WLAN mejora el seguimiento del inventario y reduce los costos del escrutinio de un inventario físico.

1.3.3.3 Tecnologías Inalámbricas

Existen varias tecnologías utilizadas en redes inalámbricas. El empleo de cada una de ellas depende mucho de la aplicación. Cada tecnología tiene sus ventajas y desventajas.

A continuación se explican las más importantes en este género:

- **Infrarrojo (Infrared)**
- **Banda Angosta (Narrowband)**
- **Espectro Extendido (Spread Spectrum)**

Infrarrojo:

Los sistemas de comunicación por infrarrojo utilizan muy altas frecuencias, justo abajo del espectro de la luz visible para transportar datos. Como la luz, el infrarrojo no puede penetrar objetos opacos, ya sea directamente (línea de vista) o indirectamente (tecnología difundida/reflectiva). El alto desempeño del infrarrojo directo es impráctico para usuarios móviles pero su uso es prácticamente para conectar dos redes fijas. La tecnología reflectiva no requiere línea de vista, pero está limitada a cuartos individuales en zonas relativamente cercanas.

Banda Angosta:

Un sistema de radio de banda angosta transmite y recibe información en una radio frecuencia específica. La banda amplia mantiene la frecuencia de la señal de radio, tan angostamente posible para pasar la información. El cruzamiento no deseado entre canales, es evitado al coordinar cuidadosamente diferentes usuarios en diferente canal de frecuencia. En un sistema de radio la privacidad y la no interferencia se incrementan por el uso de frecuencias separadas de radio. El radio receptor, filtra todas aquellas frecuencias que no son de su competencia. La desventaja de esta tecnología es el uso amplio de frecuencias, uno para cada usuario, lo cual es impráctico si se tienen muchos.

Espectro extendido

La gran mayoría de los sistemas inalámbricos, emplean la tecnología de Espectro Extendido (Spread Spectrum), una tecnología de banda amplia desarrollada por los militares estadounidenses, que provee comunicaciones seguras, confiables y de misión crítica. La tecnología de Espectro Extendido está diseñada para intercambiar eficiencia en ancho de banda por confiabilidad, integridad y seguridad. Es decir, más ancho de banda es consumida con respecto al caso de la transmisión en banda angosta, pero el 'trueque' [ancho de banda/potencia] produce una señal que es en efecto más fuerte y así más fácil de detectar por el receptor que conoce los parámetros de la señal de espectro extendido que está siendo difundida. Si el receptor no está sintonizado a la frecuencia correcta, una señal de espectro extendido se miraría como ruido en el fondo. Otra característica del espectro disperso, es la reducción de interferencia entre la señal procesada y otras señales no esenciales o ajenas al sistema de comunicación.

Espectro extendido con salto en frecuencia (FHSS[29])

FHSS utiliza una portadora de banda angosta que cambia la frecuencia en un patrón conocido tanto por el transmisor como por el receptor. Tanto transmisor como receptor están debidamente sincronizados, comunicándose por un canal que está cambiando a cada momento de frecuencia. FHSS es utilizado para distancias cortas, en aplicaciones por lo general punto a multipunto, donde se tienen una cantidad de receptores diseminados en un área relativamente cercana al punto de acceso.

Espectro extendido en secuencia directa (DSSS[30])

DSSS genera un patrón de bits redundante para cada bit que sea transmitido. Este patrón de bit es llamado código chip. Entre más grande sea este chip, es más grande la probabilidad de que los datos originales puedan ser recuperados (pero, por supuesto se requerirá más ancho de banda). Más sin embargo, si uno o más bits son dañados durante la transmisión, técnicas estadísticas embebidas dentro del radio transmisor, podrán recuperar la señal original sin necesidad de retransmisión. DSSS se utilizará comúnmente en aplicaciones punto a punto.

[29] FHSS (Espectro extendido con salto en frecuencia) Es utilizado para distancias cortas, en aplicaciones por lo general punto a multipunto.

[30] DSSS (Direct Sequence Spread Spectrum) Método de transmisión de espectro extendido que también usan equipos compatibles con IEEE 802.11b. Con este método se transmite un bit de la señal útil, lo cual implica una multiplicación de la velocidad de transmisión (extensión de la velocidad de transmisión).

1.3.3.4 Distintas Especificaciones de WLANs

IEEE 802.11:	Utilizado por la mayoría de fabricantes de WLANs. Máxima tasa de bits: 2 Mbps Frecuencia de Operación: 2.4 Ghz
IEEE 802.11b:	Especificación reciente. Máxima tasa de bits: 11 Mbps (22 Mbps con D-Link AirPlus) Frecuencia de Operación: 2.4 Ghz
IEEE 802.11a:	Especificación reciente Máxima tasa de bits: 24 – 54 Mbps (74 Mbps con D-Link AirPro) Frecuencia de Operación: 50 Ghz
IEEE 802.11g:	Especificación reciente Máxima tasa de bits: 54 Mbps (74 Mbps con D-Link AirPro) Frecuencia de Operación: 2.4 Ghz
HiperLAN:	Desarrollado por ETSI Máxima tasa de bits: 24 Mbps Frecuencia de Operación: 50 Ghz
Bluetooth:	Promo-video por 3Com, Ericson, IBM, Intel, Microsoft, Motorola, Nokia y Toshiba. Máxima tasa de bits: 1 Mbps Frecuencia de Operación: 2.4 Ghz

IEEE: Institute of Electrical and Electronic Engineers (Instituto de Ingenieros Eléctricos y Electrónicos). ETSI: European Telecomunications Standards Institute (Instituto de Estándares de Telecomunicaciones Europeas).

Son varios los factores a considerar a la hora de comprar un sistema inalámbrico para la instalación de una red LAN. Algunos de los aspectos a tener en cuenta son los siguientes:

Cobertura

La distancia que pueden alcanzar las ondas de Radiofrecuencia (RF) o de infrarrojos (IR) es función del diseño del producto y del camino de propagación, especialmente en lugares cerrados. Las interacciones con objetos, paredes, metales, e incluso la gente, afectan a la propagación de la energía. Los objetos sólidos bloquean las señales de infrarrojos, esto impone límites adicionales. La mayor parte de los sistemas de redes inalámbricas usan RF porque pueden penetrar la mayor parte de lugares cerrados y obstáculos. El rango de cobertura de una LAN inalámbrica típica va de 30 m. a 100 m. y con antena externa puede llegar a cubrir hasta 2 a 2.5 km. Puede extenderse y tener posibilidad de alto grado de libertad y movilidad utilizando puntos de acceso (Access Point) que permiten "navegar" por la LAN.

Rendimiento

Depende de la puesta a punto de los productos así como del número de usuarios, de los factores de propagación (cobertura, diversos caminos de propagación) y del tipo de sistema inalámbrico utilizado. Igualmente depende del retardo y de los cuellos de botella de la parte cableada de la red. Para la más comercial de las redes inalámbricas los datos que se tienen hablan de un rango de 1.6 Mbps. Los usuarios de "Ethernet" o "Token Ring" no experimentan generalmente gran diferencia en el funcionamiento cuando utilizan una red inalámbrica. Éstas proporcionan suficiente rendimiento para las aplicaciones más comunes de una LAN en un puesto de trabajo, incluyendo correo electrónico, acceso a periféricos compartidos, acceso a Internet, acceso a bases de datos y aplicaciones multiusuario. Como punto de comparación una LAN inalámbrica operando a 1.6 Mbps es al menos 30 veces más rápida que una LAN cableada.

Integridad y fiabilidad

Estas tecnologías para redes inalámbricas se han probado durante más de 50 años en sistemas comerciales y militares. Aunque las interferencias de radio pueden degradar el rendimiento éstas son raras en el lugar de trabajo. Los robustos diseños de las testeadas (probadas) tecnologías para LAN inalámbricas y la limitada distancia que recorren las señales, proporciona conexiones que son mucho más robustas que las conexiones de teléfonos móviles y proporcionan integridad de datos de igual manera o mejor que una red cableada.

Compatibilidad con redes existentes

La mayor parte de LANs inalámbricas proporcionan un estándar de interconexión con redes cableadas como Ethernet o Token Ring. Los nodos de la red inalámbrica son soportados por el sistema de la red de la misma manera que cualquier otro nodo de una red LAN, aunque con los discos apropiados. Una vez instalado, la red trata los nodos inalámbricos igual que cualquier otro componente de la red.

Interoperatividad de los dispositivos inalámbricos dentro de la red

Los consumidores deben ser conscientes de que los sistemas inalámbricos de redes LAN de distintos vendedores pueden no ser compatibles para operar juntos. Tres razones de estos son:

- Diferentes tecnologías no interoperarán. Un sistema basado en la tecnología de Frecuencia Esperada (FHSS), no se comunicará con otro basado en la Tecnología de Secuencia Directa (DSSS).
- Sistemas que utilizan distinta banda de frecuencias no podrán comunicarse aunque utilicen la misma tecnología.
- Aún utilizando igual tecnología y banda de frecuencias ambos vendedores, los sistemas de cada uno no se comunicarán debido a diferencias de implementación de cada fabricante.

Interferencia y Coexistencia

La naturaleza en que se basan las redes inalámbricas implica que cualquier otro producto que transmita energía a la misma frecuencia puede potencialmente dar cierto grado de interferencia en un sistema LAN inalámbrico; por ejemplo, los hornos de microondas. Pero la mayor parte de fabricantes diseñan sus productos teniendo en cuenta las interferencias por microondas. Otro problema es la colocación de varias redes inalámbricas en lugares próximos. Mientras unas redes inalámbricas de unos fabricantes interfieren con otras redes inalámbricas, hay otras redes que coexisten sin interferencia. Este asunto debe tratarse directamente con los vendedores del producto.

Simplicidad y Facilidad de Uso

Los usuarios necesitan muy poca información a añadir a la que ya tienen sobre redes LAN en general, para utilizar una LAN inalámbrica. Esto es así porque la naturaleza inalámbrica de la red es transparente al usuario, las aplicaciones trabajan de igual manera que lo hacían en una red cableada, Los productos de una LAN inalámbrica incorporan herramientas de diagnóstico para dirigir los problemas asociados a los elementos inalámbricos del sistema. Sin embargo, los productos están diseñados para que los usuarios rara vez tengan que utilizarlos.

Las LAN inalámbricas simplifican muchos de los problemas de instalación y configuración que atormentan a los que dirigen la red. Ya que únicamente los puntos de acceso ("Access Point") de las redes inalámbricas necesitan cable, ya no es necesario llevar cable hasta el usuario final. La falta de cable hace también que los cambios, extensiones y desplazamientos sean operaciones triviales en una red inalámbrica. Finalmente, la naturaleza potable de las redes inalámbricas permite a los encargados de la red preconfigurar ésta y resolver problemas antes de su instalación en un lugar remoto. Una vez configurada la red puede llevarse de un lugar a otro con muy poca o ninguna modificación.

Seguridad en la comunicación

Puesto que la tecnología inalámbrica se ha desarrollado en aplicaciones militares, la seguridad ha sido uno de los criterios de diseño para los dispositivos inalámbricos. Normalmente se suministran elementos de seguridad dentro de la LAN inalámbrica, haciendo que éstas sean más seguras que la mayor parte de redes cableadas. Es muy complicado que los receptores no sintonizados escuchar el tráfico que se da en la LAN.
Complejas técnicas de encriptado hacen imposible para todos, incluso los más sofisticados, acceder de forma no autorizada al tráfico de la red. En general los nodos individuales deben tener habilitada la seguridad antes de poder participar en el tráfico de la red.

Costos

La instalación de una LAN inalámbrica incluye los costos de infraestructura para los puntos de acceso y los costos de usuario para los adaptadores de la red inalámbrica. Los costos de infraestructura dependen fundamentalmente del número de puntos de acceso desplegados. El valor de los puntos de acceso ("Access Point") oscila entre 1000 y 2000 dólares. El

número de puntos de acceso depende de la cobertura requerida y del número y tipo de usuarios. El área de cobertura es proporcional al cuadrado del rango de productos adquirido. Los adaptadores son requeridos para las plataformas estándar de computadoras y su precio oscila entre 300 y 1000 dólares.

El costo de instalación y mantenimiento de una WLAN generalmente es más bajo que el costo de instalación y mantenimiento de una red cableada tradicional, por dos razones:

- En primer lugar una red WLAN elimina directamente los costos de cableado y el trabajo asociado con la instalación y reparación.

- En segundo lugar una red WLAN simplifica los cambios, desplazamientos y extensiones, por lo que se reducen los costos indirectos de los usuarios sin todo su equipo de trabajo y de administración.

Escalabilidad

Las redes WLAN pueden ser diseñadas para ser extremadamente simples o bastante complejas. WLANs pueden soportar un amplio número de nodos y/o extensas áreas físicas añadiendo puntos de acceso para dar energía a la señal o para extender la cobertura.

Alimentación en las plataformas móviles

Los productos WLAN de los usuarios finales están diseñados para funcionar sin corriente alterna o batería de alimentación proveniente de sus portátiles, puesto que no tienen conexión propia cableada. Los fabricantes emplean técnicas especiales para maximizar el uso de la energía del computador y el tiempo de vida de su batería.

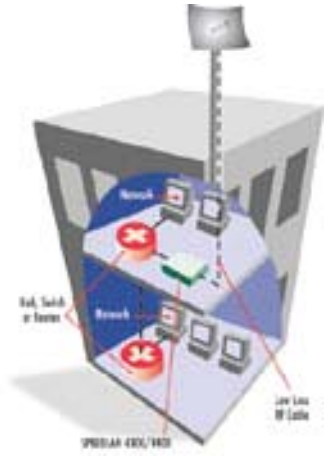


Figura 1.10. Estructura Inalámbrica

1.3.4. Protocolos y Estándares de las Redes de Comunicación

1.3.4.1 Protocolos

Una red es una configuración de computadora que intercambia información. Pueden proceder de una variedad de fabricantes y es probable que tenga diferencias tanto en hardware como en software, para posibilitar la comunicación entre éstas es necesario un conjunto de reglas formales para su interacción. A estas reglas se les denominan protocolos. Un protocolo es un conjunto de reglas establecidas entre dos dispositivos para permitir la comunicación entre ambos.

A continuación se describirán algunos de los protocolos más importantes en el uso de redes y en especial, algunos distintivos de redes inalámbricas.

Protocolo TCP/IP

Se han desarrollado diferentes familias de protocolos para comunicación por red de datos. El más ampliamente utilizado es el Internet Protocol Suite, comúnmente conocido como TCP/IP. El nombre TCP/IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto.

En líneas generales, el conjunto de protocolos TCP/IP se corresponde con el modelo de comunicaciones de red definido por la International Organization for Standardization (ISO). La siguiente figura muestra las siete capas del modelo de referencia OSI y su correspondencia general con las capas del conjunto de protocolos TCP/IP.

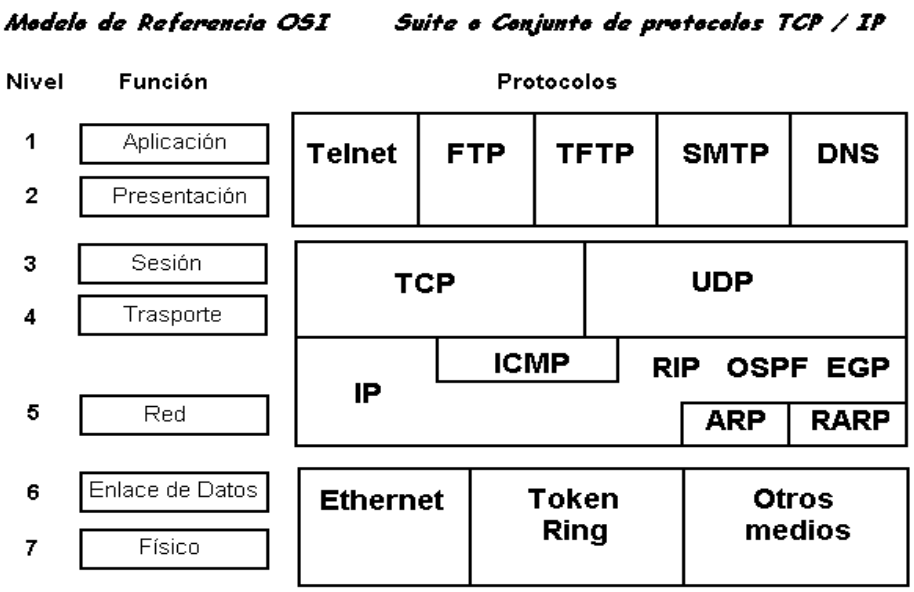


Figura 1.11. Conjunto de Protocolos TCP/IP

El sistema de división de capas permite a los programadores concentrar sus esfuerzos en las funciones de una capa determinada. No es necesario que creen todo los mecanismos para enviar información a lo largo de la red. Sólo tienen que saber los servicios que el software debe proporcionar a la capa superior, los servicios que las capas inferiores pueden proporcionar al software y qué protocolos del conjunto proporcionan estos servicios.

A continuación se enumeran los protocolos más comunes del conjunto de protocolos TCP/IP, los servicios que proporcionan:

Protocolos TCP/IP	**Servicio**
Protocolo Internet (IP)	Proporciona servicios para la entrega de paquetes (encaminamiento) entre nodos.
Protocolo de control de mensaje Internet (ICMP)	Regula la transmisión de mensajes de error y control entre los "host" y las "gateways".
Protocolo de resolución de direcciones (ARP)	Asigna direcciones Internet a direcciones físicas.
Protocolo de resolución de direcciones invertidas (RARP)	Asigna direcciones físicas a direcciones Internet.
Protocolo de control de transmisión (TCP)	Proporciona servicios de envío de flujos fiables entre los clientes.
Protocolo de datagrama de usuario (UDP)	Proporciona servicio de entrega de datagramas no fiable entre clientes.
Protocolo de transferencia de archivos (FTP)	Proporciona servicios de nivel de aplicación para la transferencia de archivos.
TELNET	Proporciona un método de emulación de terminal.
Protocolo de información de encaminamiento (RIP)	Permite el intercambio de información de encaminamiento de vectores de distancia entre "routers".
Protocolo Abrir la vía más corta primero (OPSF)	Permite el intercambio de información de encaminamiento de estado del enlace entre "routers".
Protocolo Gateway externo (EGP)	Permite el intercambio de información de encaminamiento entre "routers" externos.

Tabla 1.5. Protocolos TCP/IP

Descripción general del uso de TCP/IP

Las aplicaciones que se desarrollan con TCP/IP, normalmente, usan varios protocolos del conjunto. La suma de las capas del conjunto de protocolos se conoce también como el stack de protocolo. Las aplicaciones definidas por el usuario se comunican con la capa superior del conjunto de protocolos. La capa de nivel superior del protocolo del computador de origen traspasa la información a las capas inferiores del stack, que a su vez la pasan a la red física. La red física traspasa la información al ordenador de destino. Las capas inferiores del stack de protocolo del ordenador de destino pasan la información a las capas superiores, que a su vez la pasan a la aplicación de destino.

Cada capa del conjunto de protocolos TCP/IP tiene varias funciones; estas funciones son independientes de las otras capas. No obstante, cada capa espera recibir determinados servicios de la capa inferior y cada capa proporciona ciertos servicios a la capa superior.

La Figura 1.12 muestra las diferentes capas del conjunto TCP/IP. Cada capa del stack de protocolo del ordenador de origen se comunica con la misma capa del ordenador de destino. Las capas que se encuentran al mismo nivel en el ordenador de origen y de destino son pares. Así mismo, la aplicación del ordenador de origen y la del de destino también son pares. Desde el punto de vista del usuario o programador, la transferencia de paquetes se efectúa directamente de una capa a otra.

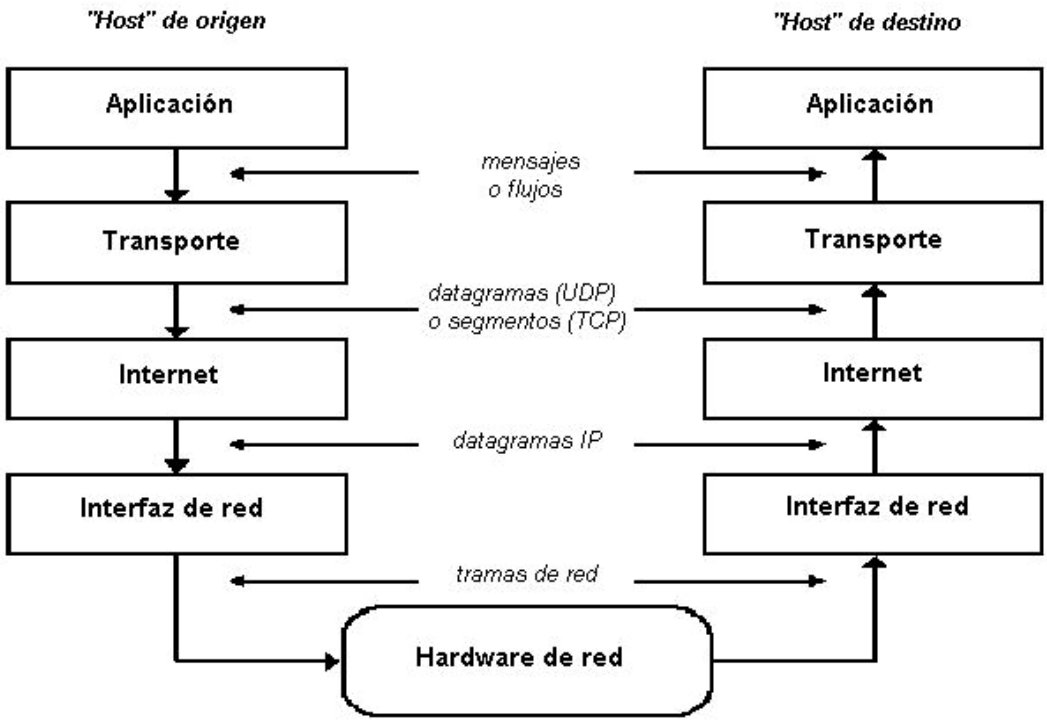


Figura 1.12. Capas de los protocolos TCP/IP

El proceso que utiliza una aplicación para transferir el contenido de un archivo es el siguiente:

1. La capa de la aplicación envía un flujo de bytes a la capa de transporte del ordenador de origen.

2. La capa de transporte divide el flujo en segmentos TCP, asigna un encabezado con un número de secuencia al segmento en cuestión y transmite este segmento a la capa de Internet (IP). Se calcula la suma de comprobación.

3. La capa de IP crea un paquete con parte de los datos que contiene el segmento TCP. La capa de IP añade al paquete un encabezado que indica las direcciones IP de origen y de destino. Esta capa también determina la dirección física del ordenador de destino o los ordenadores que actúan como intermediarios hasta el "host" de destino. Entonces, envía el paquete y la dirección física a la capa de enlace de datos. Se vuelve a calcular la suma de comprobación.

4. La capa de enlace de datos transmite el paquete IP en la sección de datos de una trama de enlace de datos al ordenador de destino. Si el ordenador de destino actúa como intermediario, el paso 3 volverá a repetirse hasta que se alcance el destino final.

5. Cuando se alcanza el ordenador de destino, la capa de enlace de datos descarta el encabezado del enlace y envía el paquete IP a la capa de IP.

6. La capa de IP verifica el encabezado del paquete. Si la suma de comprobación del encabezado no coincide con la calculada por dicha capa, el paquete se ignora.

7. Si las sumas coinciden, la capa IP descarta el encabezado y envía el segmento TCP a la capa TCP correspondiente. Esta capa comprueba el número de secuencia para determinar si el segmento, es el segmento correcto de la secuencia.

8. La capa TCP calcula una suma de comprobación para los datos y el encabezado TCP. Si la suma no coincide con la suma transmitida con el encabezado, la capa TCP descarta el segmento. Si la suma coincide y el segmento está en la secuencia correcta, la capa TCP envía un reconocimiento al ordenador de destino.

9. La capa TCP descarta el encabezado TCP y transfiere los bytes del segmento que acaba de recibir a la aplicación.

La capacidad de TCP/IP para mover información en una red, por grande que sea, sin perder datos, su sistema de nombres y direcciones, y su facilidad para saltar de una red a otra, lo convierten en el candidato ideal para cualquier red de computadoras. No obstante, pueden tener algunos inconvenientes tales como la dificultad de configuración para el usuario y la necesidad de un mantenimiento constante por parte del administrador de la red.

El primer inconveniente se debe a la necesidad que tiene el usuario de conocer algunos datos imprescindibles antes de que el sistema empiece a funcionar en red: dirección IP, máscara de red, dirección del servidor de nombres y dirección del encaminador, afortunadamente este problema puede resolverse utilizando el *Servicio de Configuración Dinámica de Equipos (DHCP)* que viene incluido en Windows NT Server, este servicio asigna los datos mencionados arriba a cada equipo en el momento en que éste se conecta en red de manera transparente para el usuario.

El trabajo de mantenimiento por parte del administrador también implica más trabajo: asignación de direcciones IP a los nuevos equipos, mantenimiento de la tabla de nombres en el servidor de nombres si este existe o, peor aún, en cada equipo si no existe y vigilar que no haya direcciones duplicadas por citar sólo algunos. De nuevo NT Server nos da una mano si combinamos la potencia de DHCP con el *Servicio de Nombres para Windows (WINS) y el Servicio de Nombres de Dominio (DNS).*

Otro inconveniente es la falta de seguridad de TCP/IP frente a los intrusos que tengan acceso físico a la red, ya que las tramas TCP/IP no van codificadas y con un software adecuado podría capturarse parte de la información que estamos enviando. Para este problema comienzan a surgir soluciones como el *Protocolo Punto a Punto Apantallado (PPTP[31])*, que encripta las tramas TCP/IP que enviamos, estableciendo de esta forma un canal seguro incluso a través de Internet.

Ventajas	***Desventajas***
✓ Es el protocolo más aceptado en redes locales. ✓ Ofrece conectividad a través de distintas plataformas de Hardware y sistemas operativos. ✓ Permite conectarse a Internet. ✓ Admite encaminamiento. ✓ Admite Windows Sockets. ✓ Admite SNMP.	• No es tan rápido como NetBEUI. • Configuración más compleja. • Mantenimiento constante.

Tabla 1.6. Protocolo TCP/IP

Protocolo NetBEUI

NetBEUI (interfaz extendida de usuario de NetBIOS) fue presentado por primera vez por IBM en 1985 y es un protocolo compacto, eficiente y rápido.

NetBEUI está optimizado para obtener un rendimiento muy elevado cuando se utiliza en redes locales o segmentos de redes locales departamentales. En cuanto al tráfico cursado

[31] PPTP (Point-to-Point Tunnelling Protocol, Protocolo Punto a Punto Apantallado)

dentro de un segmento de red local, NetBEUI es el más rápido de los protocolos suministrados con Windows NT.

En sentido estricto, NetBEUI 3.0 no es realmente NetBEUI, sino más bien un protocolo con formato de trama de NetBIOS (NBF).

Es el protocolo utilizado por las antiguas redes basadas en Microsoft LAN Manager. Es muy rápido en pequeñas redes que no lleguen a la decena de equipos y que no muevan ficheros de gran tamaño.

Ventajas	*Desventajas*
✓ Concebido expresamente para la comunicación dentro de redes locales pequeñas y, por lo tanto, muy rápido. ✓ Buena protección frente a errores. Utiliza poca memoria.	• No admite encaminamiento. • Su rendimiento en redes de área amplia (WAN) es pobre.

Tabla 1.7. Protocolo NetBEUI

Puesto que NetBEUI es muy rápido para comunicaciones dentro de redes locales de pequeño tamaño, pero su rendimiento es peor para las comunicaciones con redes de área amplia (WAN), un método recomendable para configurar una red es utilizar NetBEUI y otro protocolo, como TCP/IP, en cada una de las computadoras que necesiten acceder a otras computadoras a través de un encaminador o una red de área amplia.

Si instala ambos protocolos en cada una de las computadoras y configura NetBEUI como el primer protocolo que deberá utilizarse, Windows NT empleará NetBEUI para la comunicación entre las computadoras con Windows NT situadas dentro de cada uno de los segmentos de red local, mientras que empleará TCP/IP para las comunicaciones a través de encaminadores y con otras partes de la red de área amplia.

Protocolo IPX

IPX es un protocolo de red que permite la transmisión de datos en una red local, o bien, en una red de área ancha. Por su parte, el protocolo que permite el acceso de los usuarios a su servidor de ficheros es conocido como NCP[32].

Este protocolo, implementado por Novell, ha demostrado sobradamente su valía en redes de área local, es rápido, fácil de configurar y requiere pocas atenciones. Es el protocolo que

[32] NCP (Netware Core Protocol, Protocolo Centro de Red)

Microsoft recomienda para redes de área local basadas en DOS, Windows 3.x, Windows 95 y Windows NT.

El principal inconveniente que presenta para redes medianas y grandes es que no se puede enrutar o sea que no puede pasar de una subred a otra si entre ambas hay un encaminador (router) por lo que no puede usarse en redes WAN. Otro inconveniente que presenta en redes con un cierto número de equipos es que puede llegar a saturar la red con los broadcast que lanzan los equipos para anunciarse en la red.

NetBIOS

Windows proporciona un protocolo de compartición de dispositivos, normalmente discos o impresoras, llamado NetBIOS. Dicho protocolo, aunque muy útil, supone un importante riesgo de seguridad cuando no se configura correctamente o no se comprenden todas sus implicaciones. Así, es muy posible que un usuario esté exportando sus discos o impresoras, accesibles para el resto de máquinas de Internet, sin ni siquiera ser consciente de ello.

El protocolo NetBIOS es un protocolo de aplicación para compartir recursos en red. Dicho protocolo está soportado por Windows 3.11, Windows 95 y Windows NT, de forma nativa. Al mismo tiempo, este protocolo de aplicación debe transportarse entre máquinas utilizando, al menos, uno de los siguientes protocolos: IPX, NetBEUI, TCP/IP.

No podemos nunca hablar de NetBIOS como una alternativa a los protocolos mencionados anteriormente, pues se trata de un protocolo que se encuentra un escalón más arriba que los anteriores (más cerca del usuario). NetBIOS es un intermediario entre dichos protocolos y nuestras aplicaciones, que nos permite conectarnos al resto de los equipos de nuestra red usando nombres sencillos y fáciles de recordar (SERVIDOR, COMPRAS, ANDROMEDA, etc.) sin importar que protocolo de red estemos usando para comunicarnos con ellos. De esta manera para el usuario la red se convierte en algo transparente por la que puede navegar usando el icono "Entorno de red". Además no tenemos que preocuparnos nunca de él pues se instalará automáticamente sobre los protocolos que configuremos en nuestro equipo.

Protocolo Microsoft NWLink

Microsoft NWLink es una versión compatible con NDIS del protocolo IPX/SPX que se utiliza en las redes de Novell NetWare.

NWLink proporciona un protocolo compatible con el protocolo IPXISPX de Novell NetWare. Para mejorar aún más la compatibilidad de Windows NT con NetWare, Windows NT también proporciona Servicio cliente para NetWare y Servicio pasarela para NetWare.

Ventajas	*Desventajas*
✓ Ofrece compatibilidad con Novell NetWare.	• No es tan rápido como NetBEUI en redes locales de pequeño tamaño.

Tabla 1.8. Microsoft NWLink

Protocolos en Redes Inalámbricas

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance o CSMA/CA es un protocolo que censa el canal antes de producir una transmisión, y si éste está ocupado utiliza un algoritmo de backoff para volver a censar el canal hasta encontrarlo libre. Este protocolo evita las colisiones, enviando un paquete de reconocimiento (ACK) para confirmar la llegada al receptor del paquete enviado.

Una red inalámbrica presenta nuevos problemas al control de acceso al medio, entre éstos cabe destacar que no puede darse por sentado que todos los nodos tienen acceso a escuchar si cualquiera de los posibles emisores está utilizando el canal (recordar que el alcance es limitado) por lo tanto, el sensar el canal puede no llegar a útil. Además de esto, es necesario considerar que no resulta práctico tener un canal (frecuencia) para transmitir y otro distinto para recibir. Una sencilla aproximación de lo que debe usarse en una LAN inalámbrica puede ser CSMA: escuchar si hay otras transmisiones y sólo transmitir si no hay ninguna haciéndolo.

CSMA/CA trabaja de la siguiente manera:

1. La estación transmisora comprueba el medio (aire) si no detecta transmisión alguna en curso se pone a esperar una cantidad aleatoria de tiempo, si pasado este tiempo, el medio sigue "libre" comienza la transmisión.
2. Si el paquete se recibe intacto, la estación receptora envía un paquete ACK a la estación emisora. Si este paquete de reconocimiento llega al emisor, el ciclo es completado.
3. Si el emisor no recibe un ACK, bien porque el paquete de datos no llegó o porque se perdió el ACK, se asume que se produjo una colisión y se esperará de nuevo un tiempo aleatorio para volver a intentarlo.

MACA y MACAW

Un primer protocolo diseñado para redes inalámbricas LANs es MACA[33]. Se utilizó como base para el estándar IEEE 802.11 de redes inalámbricas. La idea básica es que el emisor para estimular al receptor le manda una trama corta, así estaciones cercanas pueden detectar esta transmisión y evitarán transmitir a la vez durante el tiempo que tarde la transmisión.

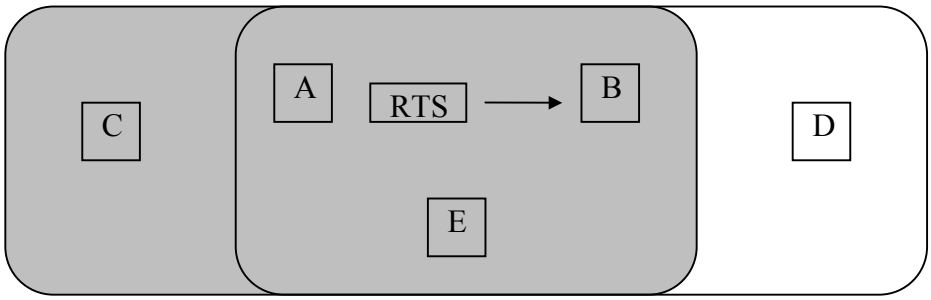


Figura 1.13. Rangos de Transmisión

Basado en simulaciones MACA se acabó obteniendo el protocolo MACAW[34] que es una versión mejorada de MACA que funciona de manera similar, pero ahora utiliza un intercambio de mensajes RTS-CTS-DS (Data Send = envío de datos) DATA-ACK (Acknowledge = verificación) además de implementar modificaciones al algoritmo de retransmisión o de backoff.

Para comenzar, diremos que las tramas perdidas no son retransmitidas en el nivel de enlace sino que se debe esperar a que la información llegue al nivel de transporte, o sea, mucho más tarde. Esto es resuelto obligando al receptor a enviar una trama ACK cada vez que la información llega correctamente.

Además el algoritmo de Backoff se ejecuta para cada trama de datos (fuente-destino) mejor que para cada estación. Este cambio provoca la imparcialidad del protocolo. Finalmente, se añade un mecanismo para estaciones que intercambian información sobre la congestión y para hacer que el algoritmo de backoff no reaccione tan violentamente ante problemas temporales.

La utilización de una trama de ACK en este nivel mejora los tiempos de respuesta, comparándolos con los que se obtendrían si se dejara manejar la situación por el protocolo de nivel de transporte. El nuevo frame CS permite distribuir la información de sincronización sobre los períodos de contienda, de forma que los nodos puedan ``pelear'' de igual forma por un periodo de tiempo para solicitar la transmisión. La trasmisión se lleva a cabo de la siguiente manera, el emisor envía (sin censar el canal) un RTS al receptor, quien

[33] MACA (Multiple Access with Collision Avoidance, Múltiple Acceso de Colisión Avanzada)
[34] MACAW (*MACA Wireless)*

responderá con un CTS, una vez recibido éste, el emisor envía un DS seguido de los datos a transmitir. En caso de recibirse correctamente los datos el receptor devuelve un ACK, caso contrario no lo hace y se retransmite la información siguiendo el mismo esquema partiendo con el RTS. En el caso de que el ACK se pierda, se enviará un nuevo RTS al cual se le responderá nuevamente con el mismo ACK.

Otra cosa es la seguridad. Los protocolos de Criptografía son usados para este propósito.

1.3.4.2 Estándares

Para poder entender el estado actual de las tecnologías inalámbricas es imprescindible conocer la diversidad que contemplan sus estándares. Los grupos de trabajo de la IEEE han estado trabajando en los nuevos estándares que deben cubrir las necesidades de este tipo de redes, sacando a la luz numerosas especificaciones dentro del marco del 802.11. Aunque actualmente no se han terminado muchas de estas especificaciones vamos a recorrer los diferentes trabajos y sus estados actuales ya que parece que la industria se está moviendo hacia compromisos y consensos que permitirán que muchos de los elementos de la próxima generación proporcionen mayor velocidad, fiabilidad, transmisión de voz, audio y vídeo, y las bases de seguridad que permitan sustentar las redes. En la actualidad existen varios estándares inalámbricos disponibles para el diseño de redes de datos: Bluetooth, HomeRF, HiperLAN 2 y 802.11.

Centraremos este estudio en el estándar 802.11 debido a que es el de mayor éxito en el mercado de las redes inalámbricas. A continuación se describirán las características de cada una de estas tecnologías.

Estándar Bluetooth

Bluetooth es una tecnología inalámbrica desarrollada por la compañía sueca Ericsson. En su diseño privó la importancia de obtener dispositivos de pequeño tamaño, bajo consumo y bajo coste. Esta tecnología está orientada a conectar cualquier dispositivo electrónico: ordenadores, PDA, teléfonos, electrodomésticos, etc.; en pequeños radios de cobertura (10 m.) conformando redes PAN (Personal Area Networks) o Redes de Área Personal, capaces de transmitir voz y datos. La velocidad de transmisión es de 720 kbps por canal. Si se emplean puntos de acceso, el radio de cobertura puede llegar a los 100 m.

Los dispositivos Bluetooth operan en la banda ISM[35] de los 2.4 GHz, para la cual no es necesario licencia. Este requisito permite la compatibilidad con los sistemas de radio actual y la disponibilidad de unas comunicaciones de calidad.

La banda de frecuencias empleada se extiende desde los 2.400 a los 2.4835 GHz, conformando un total de 79 canales de RF de la forma: $f = 2402 + k$ MHz, $k = 0,\ldots,78$. Emplean FHSS (Frequency Hopping Spread Spectrum) con señales full-duplex a 1600

[35] ISM (Industrial Scientific Medical) Banda autorizada para el uso de aplicaciones con Wireless LAN.

saltos o "hops" por segundo. Dependiendo de la potencia del dispositivo Bluetooth, existen 3 clases:

- Clase 1: Máx. pot. de salida = 100 mW y Mín. pot. de salida = 1 mW.
- Clase 2: Máx. pot. de salida = 2.5 mW y Mín. pot. de salida = 0.25 mW.
- Clase 3: Máx. pot. de salida = 1 mW y Mín. potencia de salida = (No disponible).

Estándar Homerf

Este estándar fue desarrollado por HomeRF Working Group como una tecnología de bajo coste para el hogar. Opera en la banda de frecuencia de los 2.5 GHz. Los dispositivos actuales HomeRF permiten transmisiones de hasta 2 Mbps en un rango de 137 m (450 feet). Actualmente la FCC[36] ha dado vía libre para poder diseñar dispositivos con velocidades de transmisión de 10 Mbps que tendrán un rango de 15 m (50 feet).

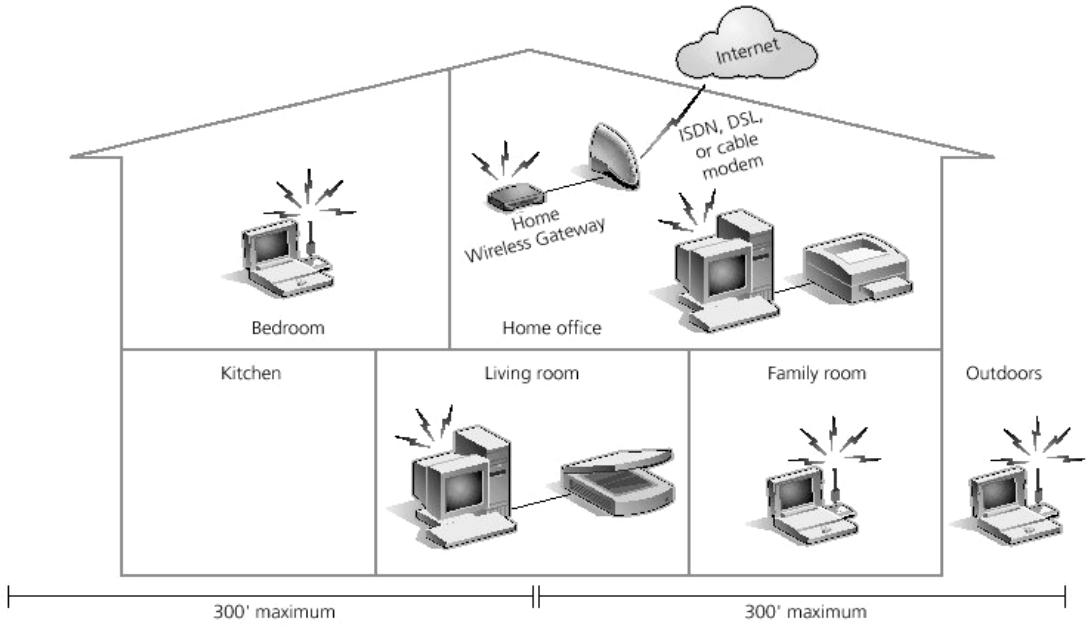


Figura 1.14. HomeRF

HomeRF emplea la tecnología SWAP-CA (Shared Wirelless Access Protocol – Cordless Access, Protocolo de Acceso Compartido Inalámbrico- Acceso Inalámbrico) que suma las cualidades de CSMA/CA para la transmisión de datos y las de TDMA (Time Division Multiple Access, Acceso Múltiple por División de Tiempo) para la transmisión de voz.

[36] FCC (Federal Communications Comision, Comisión Federal de Comunicación)

Entre sus características destacan:

- Soporta tres canales de voz, con lo que se puede emplear el teléfono a la vez que se envían datos.
- Soporta hasta 128 dispositivos en red.
- Emplea encriptación Blowfish y opcionalmente encriptación con claves de 56 bits.

Estándares Hiperlan2

HiperLAN2 es un estándar desarrollado por el ETSI (European Telecommunications Standard Institute) para redes WLAN. Destaca por:

- Alta velocidad de transmisión.
- Orientado a conexión.
- Calidad de servicio (QoS).
- Búsqueda automática de frecuencia.
- Seguridad.
- Movilidad.
- Bajo consumo.

Alta velocidad de transmisión. HiperLAN2 ofrece una velocidad de transmisión de 54 Mbits/s, equiparable a las velocidades de las actuales LAN. Para conseguir estas velocidades, la tecnología HiperLAN2 hace uso de OFDM (Orthogonal Frequency Digital Multiplexing) para transmitir las señales analógicas. OFDM es muy eficiente en entornos de trabajo como las oficinas, donde las señales de radio son reflejadas en varios puntos, llegando al receptor con tiempos de propagación diferentes.

Orientado a conexión. Los datos son transmitidos en conexiones entre los clientes inalámbricos y los puntos de acceso (AP), establecidas previamente a la transmisión. Las conexiones emplean multiplexación por división de tiempo y pueden ser punto a punto o punto a multipunto. Las primeras son bidireccionales, mientras que las segundas son unidireccionales.

Calidad de servicio. El hecho de que el estándar sea orientado a conexión permite proporcionar calidad de servicio, pudiendo establecer a cada conexión variables como el ancho de banda, el retraso, errores, etc. Además ofrece la posibilidad de establecer prioridades distintas a cada conexión, facilitando la transmisión simultánea de vídeo, voz y datos.

Búsqueda automática de frecuencia. En las redes HiperLAN2, no es necesaria la planificación manual de las frecuencias como en las redes celulares GSM. Los puntos de acceso (APs) seleccionan automáticamente el canal de radio adecuado para las transmisiones, basándose en la recepción de los puntos de acceso vecinos, evitando posibles interferencias.

Seguridad. Soporte de autenticación y encriptación. Los puntos de acceso y los clientes inalámbricos pueden autenticarse unos a otros para asegurar un acceso autorizado y válido a la red operadora. Todos los datos del usuario viajan encriptados para garantizar la confidencialidad.

Movilidad. El estándar ofrece la posibilidad de "roaming", por lo que el cliente inalámbrico puede desplazarse entre la cobertura de dos puntos de acceso distintos, sin perder por ello conectividad.

Bajo consumo. Se permite el establecimiento, entre el cliente inalámbrico y el punto de acceso, de periodos de inactividad, en los que el cliente inalámbrico entra en estado de bajo consumo.

Estándar 802.11

802.11 es un estándar de redes inalámbricas (WLAN), desarrollado por el Instituto de Ingenieros Electrónicos y Eléctricos (IEEE) cuya especificación apareció en el año 1997. En su primera versión del estándar, 802.11, proporcionaba unas velocidades de transmisión de 1 ó 2 Mbps y una serie fundamental de métodos de señalización y otros servicios. El primer escollo que se encontró en este estándar, fue el de su baja tasa de transferencia de datos, incapaz de soportar los requerimientos de las empresas en la actualidad. En consecuencia se trabajó en un nuevo estándar, el 802.11b (también conocido como 802.11 High Rate) que apareció en 1999 y proporcionaba unas tasas de transferencia de hasta 11 Mbps. Gracias a las prestaciones ofrecidas por 802.11b, similares a las de las redes cableadas, ha logrado tener bastante éxito en el mundo empresarial, siendo una de las tecnologías más expandidas y que posee un amplio abanico de productos y compañías que la soportan.

Muchas de las empresas dedicadas al desarrollo de equipamiento informático se han unido en una alianza denominada WECA[37], cuya misión es la de velar por la interoperatibilidad entre productos 802.11b de distintos fabricantes y promocionar dicha tecnología en el ámbito empresarial, PYMES y hogar. Cuando se comprueba que un producto funciona correctamente con otros dispositivos 802.11b, recibe el certificado de Wi-Fi (Wireless Fidelity) como garantía de interoperatibilidad y buen funcionamiento.

1.3.4.3 Configuraciones de Red

802.11 define dos modos de red denominados: modo *Infraestructura* y modo *Ad hoc*. En el modo *Infraestructura*, la red consiste en al menos un punto de acceso (AP) y varios clientes inalámbricos, a esta configuración se la conoce como *Conjunto Básico de Servicio* (BSS – Basic Service Set). Otra posible configuración es la de *Conjunto Extendido de Servicio* (ESS – Extended Service Set) y consiste en una agrupación de dos o más BSS. El modo *Ad*

[37] WECA (Wireless Ethernet Compatibility Alliance)

hoc, también conocido como Peer to Peer (de igual a igual) consiste en que cada cliente se comunique uno a uno con el resto de clientes inalámbricos, sin emplear por tanto un punto de acceso.

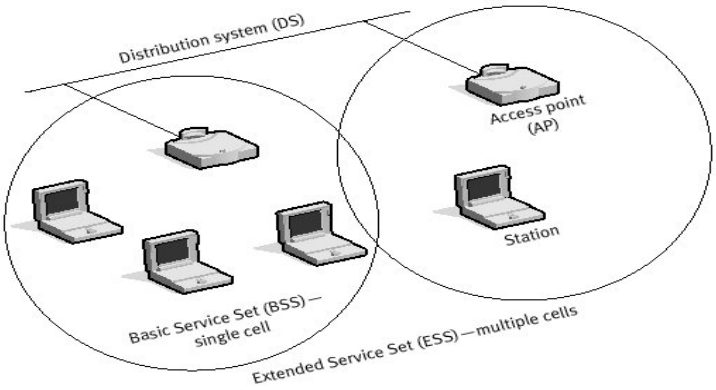


Figura 1.15. Modo infraestructura

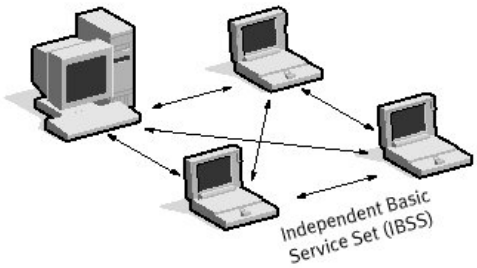


Figura 1.16. Modo Ad hoc o Peer to Peer

1.3.4.4 Modelo de Capas

El estándar 802.11b abarca las capas física y de enlace del modelo OSI. A nivel físico el estándar 802.11b trabaja en la banda ISM de los 2.4 GHz, reconocida por las Agencias Reguladoras americana (FCC), europea (ETSI) y japonesa (MKK) para transmisiones de radio sin licencia. En el primer estándar que trabajaba a 1 ó 2 Mbps se podía emplear FHSS o DSSS en la capa física, pero debido a las limitaciones de FHSS, para el estándar a 11 Mbps sólo se emplea DSSS.

Empleando FHSS, la banda de los 2.4 GHz se divide en 75 subcanales de 1 MHz. El emisor y el receptor se ponen de acuerdo en un patrón de salto o "hopping pattern" para enviar los datos sobre una secuencia establecida de subcanales. En cada conversación en 802.11 se emplea un patrón de salto, en cuyo diseño se ha buscado minimizar la posibilidad de que dos emisores empleen el mismo subcanal a la vez. Las limitaciones de velocidad de FHSS provienen de las restricciones de los anchos de banda de los subcanales a 1 MHz.

Por el contrario, DSSS divide la banda de los 2.4 GHz en 14 canales de 22 MHz. Los canales adyacentes se superponen parcialmente con un total de 3 canales de los 14 que no se superponen en ningún momento. Los datos son enviados en cualquiera de estos 22 canales, sin saltar de un canal a otro. Para compensar el ruido producido en cada canal se emplea la técnica del "chipping" o trocamiento.

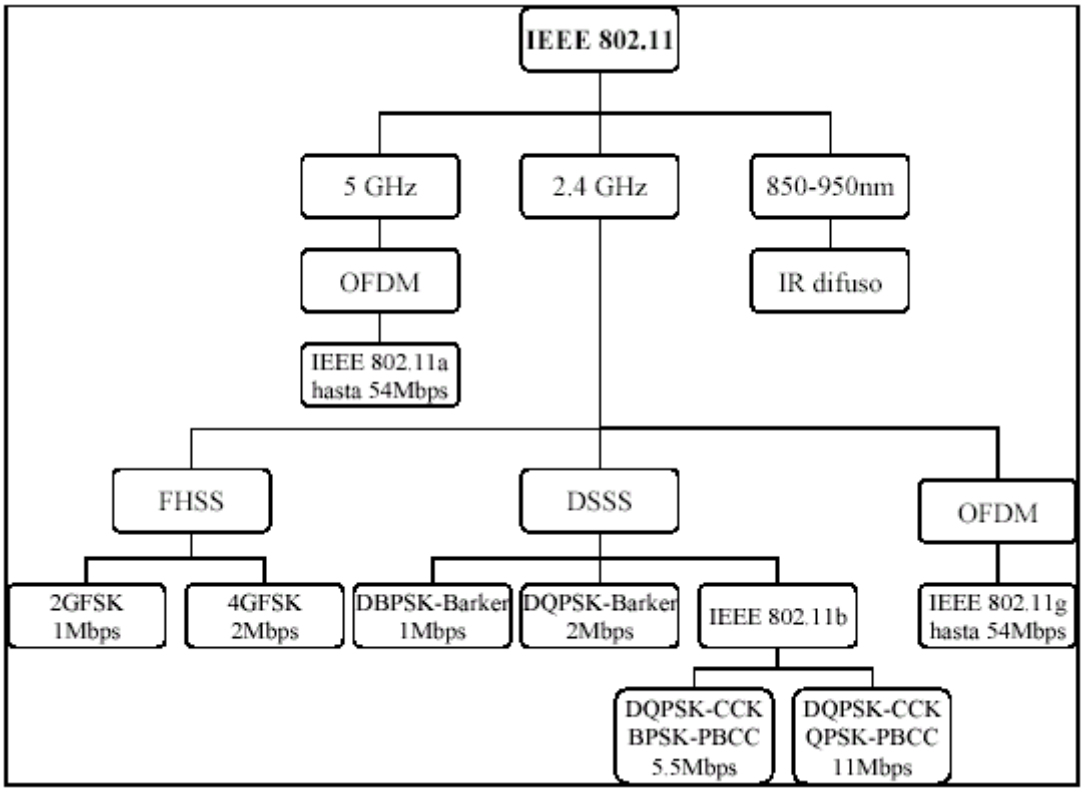


Figura 1.17. Estructura del 802.11

Para adaptarse a entornos con mucho ruido, esta tecnología dispone de desplazamiento dinámico de velocidad, que permite adaptar de manera automática la velocidad de transmisión para compensar el ruido del canal. Dependiendo de la cantidad de interferencia presente en el medio, el estándar es capaz de trabajar a: 11, 5.5, 2 ó 1 Mbp.

La capa de enlace de 802.11 consiste en dos subcapas: LLC[38] y MAC[39]. La primera de ellas emplea la misma subcapa LLC de 802.2 con una dirección de 48 bits empleada también en las redes LAN 802. Esto permite la facilidad de conexión entre un sistema cableado y no cableado.

La capa MAC es propia de 802.11, aunque en concepto es muy similar a la de 802.3, debido a que se basa en el principio de que muchos usuarios acceden al mismo y único

[38] LLC (Logical Link Control, Control de Enlace Lógico)
[39] MAC (Media Access Control, Control de Acceso Medio)

medio. Debido a la imposibilidad de emplear la misma tecnología CSMA/CD de 802.3, dada la imposibilidad de "escuchar" una colisión, 802.11 emplea una modificación del protocolo denominada CSMA/CA (Carrier Sense Múltiple Access with Collision Avoidance). Este protocolo evita las colisiones, enviando un paquete de reconocimiento (ACK) para confirmar la llegada al receptor del paquete enviado.

Debido al constante cambio en la tecnología y a las mejoras que se han hecho de este estándar a continuación se muestran las diferentes versiones o niveles de *802.11*:

- **802.11b.** Utiliza 2.4 GHz por medio de *"Direct-Sequence Spread-Spectrum"*. Puede alcanzar tasas de hasta 11 Mbit/s. Pero este estándar está a punto de ser mejorado en una nueva especificación **802.11g** que permitirá tasas de hasta 22 Mbit/s en la banda de 2.4 GHz de una forma totalmente compatible hacia atrás con 802.11b. El OFDM (Orthogonal Frequency División Multiplexing) desarrollado como codificador para 802.11a será adoptado por 802.11g como mecanismo de codificación. Texas Instruments está fabricando equipos con una codificación diferente llamada PBCC (Packet Binary Convolution Coding) que también será soportada por 802.11g.

- **802.11a.** Está provocando un gran debate en la comunidad de TI (Transmisión Inalámbrica) sobre si tiene sentido desarrollarla hoy o vale la pena esperar a nuevas especificaciones de 802.11, ya que no hay grandes ventajas en ella. Opera en la banda de 5 GHz lo que da un ancho menos poblado proporcionando más canales y un ancho de banda mayor. De esta forma podemos tener más puntos de acceso con menos interferencias y señales más limpias. 802.11a cuenta simplemente con una posición aventajada especialmente cuando en entornos donde el rendimiento de la red en el lado servidor es importante y el cableado físico es costoso.

  Los fabricantes producirán tarjetas duales que permitirán a un cliente enlazarse con 802.11g/b y 802.11a, aunque no a la vez. El objetivo de IEEE ha sido asegurarse de que todo menos la parte de radio de los estándares a, b y g sea compatible. De esta forma un fabricante puede proporcionar dos tipos de radios sin duplicar el resto del equipo manteniendo, así, los costes muy bajos.

- **802.11h.** Al contrario que en Ethernet, las especificaciones de radio 802.11 no escuchan la red antes de transmitir para comprobar que la línea esta libre. Éstas, en cambio, transmiten y sin esperar la respuesta apropiada, paran y retransmiten. Los dispositivos Ethernet escuchan, envían y, si encuentran algún problema, esperan una cantidad de tiempo determinada antes de retransmitir.

  802.11h se basa en 802.11a para resolver los problemas de interferencias y uso, así como mejorar la coexistencia con otras especificaciones que trabajan en el mismo

ancho de banda. La especificación *h* revisa si las frecuencias están en uso antes de la transmisión (Dynamic Frequency Selection o DFS) y de que transmitan con el nivel de energía mínimo (Transmit Power Control o TPC). Estas mejoras fueron formuladas para conseguir los requisitos de uso de la banda de 5 GHz en la Unión Europea que denomina a su especificación equivalente como HiperLAN2. Cada paquete que se envía por la red en 802.11b tiene las mismas posibilidades de llegar a su destino que cualquier otro.

- **802.11e.** Pretende cambiar esto, permitiendo incorporar calidad del servicio (QoS) que proporcione prioridad de unos paquetes sobre otros. Ésta es una tarea compleja que involucra la coordinación entre las radios de los diferentes clientes, puntos de acceso y administradores de sistemas.

  QoS es necesario para la emisión de voz de calidad utilizando VOIP (voz sobre IP) y para "*streaming"* multimedia. Las ventajas que proporcionan HomeRF y otras especificaciones de 2.4 GHz frente a 802.11b es la posibilidad de priorizar los paquetes lo que asegura el envío de voz sin cortes que también se soluciona con 802.11e.

  Inicialmente 802.11e cubría QoS y seguridad. Pero con los constantes informes de debilidad en el sistema de cifrado WEP[40] la parte de seguridad adquirió su propia identidad en **802.11i**. El grupo de esta especificación ha estado trabajando en la sustitución de WEP y afortunadamente se definirá con la suficiente compatibilidad como para no tener que revisar los sistemas ya creados.

- **802.1x.** Es un método de autenticación de usuarios de una forma segura. Algunas debilidades de esta solución han sido ya descubiertas ya que hay mucha facilidad para realizar acciones MITM (man in the middle).

[40] WEP (Wireless Equivalent Privacy, Privacidad Equivalente Inalámbrica)

Capítulo II

DESARROLLO DE LA RED

2.1. REQUERIMIENTOS DEL SISTEMA

Para realizar el diseño de cualquier proyecto necesitamos establecer primeramente aquellos parámetros que nos guiarán en la construcción del mismo. Al darnos cuenta de las necesidades que necesitamos cubrir, seremos capaces de definir las estrategias de solución más adecuadas, de la misma manera, el considerar prioridades respecto a lo que queremos realizar marcará la pauta para elegir entre distintas opciones que se presenten.

En el caso de nuestra propuesta, necesitaremos establecer que elementos guiarán la elección del diseño físico y lógico, además tendremos que realizar una elección respecto al hardware y el software que mejores resultados nos ofrezcan, pero considerando las limitaciones de la red de cómputo como la localización física, el presupuesto, la seguridad, etc.

A continuación describiremos los criterios más importantes que consideraremos para la creación de nuestro diseño.

Características del entorno físico.

Éste es un punto central del proyecto puesto que establece limitantes respecto a los enlaces que podemos realizar. Puesto que nuestro problema central es el crear una red de cómputo necesitamos encontrar la manera de establecer contacto entre los diferentes dispositivos, es por ello que primero debemos considerar las limitantes del entorno, lo cual nos permitirá decidir de que manera podemos establecer las conexiones necesarias y con que tipo de equipo es posible realizarlas.

Número y tipo de usuarios.

Obviamente éste será un factor que determinará en gran parte el diseño de nuestra red de cómputo ya que el número de usuarios de la red le dará al diseño su estructura esencial, además, nos obligará a considerar el uso de cierto tipo de equipo (servidores, “hubs”, “switchs”, etc.) que permita una conexión y administración adecuada de la red.

Al considerar de antemano que existirán distintos tipos de usuarios podremos sugerir ciertas herramientas para poder establecer privilegios y obligaciones adecuados para salvaguardar la seguridad del sistema y darle una mejor estructura.

Prestaciones técnicas.

Debemos considerar los requerimientos de hardware y de software para satisfacer las necesidades del sistema considerando lo existente en el mercado y aquello que realmente nos sea útil.

Seguridad.

La seguridad en la información es un aspecto primordial en el diseño de cualquier red de cómputo. La información es un activo sumamente importante para cualquier empresa o entidad y al diseñar un sistema que se encargue de manejar datos es muy importante el tomar las medidas pertinentes para lograr que dicha información sea confidencial, íntegra y oportuna. Estas herramientas pueden ser a nivel de hardware o software y se implementarán según sea o no conveniente a nuestro diseño, necesidades y presupuesto.

Expectativas de crecimiento.

Siempre que se diseña un proyecto se deben considerar las posibilidades que existen respecto a su crecimiento futuro ya que los sistemas no son estáticos y sufren cambios constantes. La elección de alternativas que nos brinden un panorama más conveniente conforme el sistema se modifica o que ofrezcan condiciones favorables para su expansión futura es siempre mejor que las que no toman en cuenta esta posibilidad. Un gasto mayor desde el inicio del proyecto que exceda las capacidades primordiales del sistema, puede representar en realidad un ahorro en el momento de ampliar el proyecto o simplemente puede facilitar su crecimiento y además ofrecer un mayor rango en las expectativas de su funcionamiento.

Integración e interoperabilidad con otras redes.

Puesto que el crecimiento de todos los sistemas es una posibilidad latente, debemos considerar que nuestro proyecto puede interactuar con otros sistemas de distinta naturaleza, ya sea a nivel físico o lógico; por lo tanto debemos tener cuidado en la elección de los elementos de hardware y software que posibiliten la integración e interacción con otros diseños (redes cableadas, distintos protocolos, etc.) y no hacer que nuestro diseño se convierta en una estructura cerrada y por ello problemática.

Los requerimientos del sistema descritos anteriormente nos permitirán orientar nuestro trabajo de la siguiente manera:

- Investigar las características físicas del ambiente involucrado midiendo los parámetros que van a influir en la elección del equipo y diseño de la red.
- Realizar el diseño estructurado de la red considerando cada una de las cantidades involucradas en el proyecto.
- Analizar y comparar los diferentes tipos de equipo (hardware) que existen en el mercado para la implementación del proyecto y elegir aquel que resulte óptimo para nuestras necesidades.

- Establecer el sistema (software) que contenga las mejores características para el manejo y transmisión de la información a través de la red cubriendo los requerimientos de fiabilidad, seguridad, velocidad y otras características requeridas.

El aspecto económico también será un factor a considerar en el momento de elegir las estrategias de solución del proyecto. Es evidente que el gasto excesivo es algo inaceptable en la actualidad, sin embargo debemos considerar que la inversión en soluciones sin la capacidad necesaria o el ahorro al adquirir equipos problemáticos o sin garantía representa un enorme riesgo, es por ello que deberemos analizar que opciones son más convenientes a nuestras necesidades.

En el capítulo 1 "Marco Teórico" se presentaron los conceptos fundamentales sobre comunicaciones y redes, los cuales forman parte de la investigación que se realizó para elegir los medios adecuados para implementar la solución, considerando que se deben cumplir ciertas especificaciones de acuerdo con los equipos y el sistema.

A continuación describiremos con más detalle los requerimientos del proyecto y posteriormente presentaremos nuestra propuesta de solución del problema especificando los componentes de nuestro sistema.

2.1.1. Descripción del ambiente a analizar

En este proyecto se pretende diseñar una red de datos inalámbrica para satisfacer las necesidades de comunicación de datos entre los diversos componentes de una cadena de restaurantes para mantener a la empresa a la vanguardia en cuanto al servicio que ofrece, además de proporcionar agilidad y versatilidad a sus operaciones manteniendo la seguridad que requiere una empresa con tales características. Esta comunicación se requiere para mantener el control de ventas, inventarios, precios de los productos, asistencia de personal, etc.

Las características físicas del proyecto hacen necesario implementar una red inalámbrica, que como se describirá en este trabajo, será la mejor opción en cuanto a costo y operabilidad. En principio se describirá la estructura de los edificios que conforman esta cadena de restaurantes para tener una idea más clara de lo que requerimos.

La red se instalará en tres entidades conformadas cada una de ellas por un edificio; a su vez una de ellas será la cabeza principal de toda la información resguardando datos de cada uno de las otras entidades a conectar, esto implica:

- La ubicación de nuestro primer edificio corresponderá a la CENTRAL A que se muestra en la Figura No. 2.1.

Figura 2.1. Ubicación del Edificio Principal Central "A"

Este edificio se encuentra ubicado en la calle de Arcos de Belen #230. Este inmueble está formado por 3 niveles: la planta baja que corresponde al restaurante, el primer piso que alberga la cocina y la bodega de materias primas y el segundo piso donde se encuentran las oficinas de la empresa que representa el lugar en donde se instalará el sistema de cómputo de nuestro proyecto.

Ya que este edificio contiene las oficinas principales de la cadena de restaurantes, se considera que albergará el sistema de información con mayores privilegios y podemos decir que se comportará como matriz del sistema.

Figura 2.2. Ubicación del Edificio Secundario Anexo "B"

- El segundo edificio corresponderá al ANEXO B que se muestra en la Figura No. 2.2; la cual será una de las 2 entidades "secundarias" que se conectarán. Este inmueble se encuentra ubicado en la calle de Francisco I. Madero # 49.

  Este edificio está conformado por una planta baja destinada al servicio de restaurante y la cocina, además de un primer piso que tendrá como objetivo albergar oficinas y por lo mismo el equipo de cómputo.

Figura 2.3. Ubicación del Edificio Secundario Anexo "C"

- El tercer y último edificio será el ANEXO C con una ubicación que corresponde a la Figura No. 2.3. Esta construcción se encuentra ubicada en la calle de Tacuba # 138.

  Mantendrá la misma distribución que el Anexo B; es decir, está conformado por una planta baja destinada al servicio de restaurante y la cocina, además de un primer piso destinado a oficinas.

Como podemos observar estos edificios guardan una distancia máxima de alrededor de 2.5 kilómetros y mínima de 500 metros. La Figura 2.4 muestra un mapa general donde apreciamos esta distribución.

Figura 2.4. Mapa General de las Entidades

NOTA: En todos los edificios tenemos los medios eléctricos necesarios para la conexión de equipo de cómputo, como: contactos, apagadores, lámparas, suministros de energía, etc.

2.1.2. Número y tipo de usuarios

Como hemos señalado anteriormente, es un hecho que una buena administración de cualquier tipo de negocio reditúa en un mejor aprovechamiento de recursos y de la misma manera, en un mejor funcionamiento del sistema de producción y sus ganancias.

En este proyecto el objetivo principal es proporcionar un sistema de administración de la información que cubra de manera óptima con las necesidades del cliente. Al realizar una discusión acerca de lo que se requiere para llevar a cabo esta tarea, se decidió que el sistema requiere de los siguientes usuarios/equipos para cada una de las entidades o edificios:

Usuarios

CENTRAL A

Equipo # 1: Administración de la nómina de empleados.
Registro de datos de los empleados.
Manejo de información contable de la sucursal.
Lista de precios de los productos.
Otro tipo de información de uso exclusivo de la administración.
Capacidad de recibir, enviar y copiar cualquier información registrada en los otros elementos de la red (equipo espejo).

Equipo #2: Información referente a proveedores y clientes.
Manejo de inventarios.
Posibilidad de ser un equipo que se pueda transportar para diversas necesidades.
Posibilidad de ser el equipo que aloje la página de Internet de la empresa en un futuro próximo.

Equipo #3: Registro de horarios de entrada y salida de los empleados.
Monitoreo del servicio de estacionamiento.

Equipo #4: Registro de ventas y extensión de comprobantes.
Atención de servicio a domicilio y reservaciones.
Este equipo se encontrará en la planta baja de los edificios y dará servicio directo a los clientes.

ANEXO B

Equipo #1: Manejo de la información contable de la sucursal.

Equipo #2: Registro de horarios de entrada y salida de los empleados.
Monitoreo del servicio de estacionamiento.

Equipo #3: Registro de ventas y extensión de comprobantes.
Atención de servicio a domicilio y reservaciones.
Este equipo se encontrará en la planta baja de los edificios y dará servicio directo a los clientes.

ANEXO C

Equipo #1: Manejo de la información contable de la sucursal.

Equipo #2: Registro de horarios de entrada y salida de los empleados.
Monitoreo del servicio de estacionamiento.

Equipo #3: Registro de ventas y extensión de comprobantes.
Atención de servicio a domicilio y reservaciones.
Este equipo se encontrará en la planta baja de los edificios y dará servicio directo a los clientes.

Tipos de usuarios

En la red de cómputo solo existirán dos tipos de usuarios: un *administrador* y nueve *clientes*.

El administrador de la red será el usuario del Equipo #1 de la CENTRAL A, el cual tendrá acceso a toda la información que manejen los otros equipos en la red y será el único con permisos para observar y modificar ciertos datos; como la nómina, precios, inventarios, información contable, etc. Generará un respaldo de toda la información de forma continua y enviará los datos actualizados a los equipos de la red que así lo requieran. Este equipo será manejado por el administrador de la red y la administración del negocio.

Los equipos clientes tendrán como finalidad el representar la interfaz para que los empleados registren información referente a su horario de entrada y salida, así como de ventas realizadas, consulta de precios, monitoreo del servicio de estacionamiento, etc., pero sin la capacidad de modificar cierta información y con la obligación de mantener al corriente al Equipo #1 de la CENTRAL A, de todos los movimientos realizados, así como generando un respaldo de información en cada equipo. Estos equipos serán manejados por la gerencia y el personal de cajas.

2.1.3. Prestaciones técnicas

Respecto a los equipos que se utilizarán como elementos de la red, hemos convenido que las características básicas que deben cumplir son las siguientes:

1. Velocidad de procesamiento de 2.4 GHz.
2. Memoria RAM 256 MB.
3. 80 GB Disco Duro.
4. Unidad de disco 3.5”, CD-RW.
5. Mouse y teclado.
6. Tarjeta de vídeo y tarjeta de red óptimas para vídeo conferencia.

Se estima que esta configuración será más que suficiente para que el software contemplado por la empresa para la administración del sistema funcione perfectamente y además nos permita cubrir nuestras expectativas respecto al almacenamiento de datos, velocidad de transmisión, manejo de vídeo, etc. Estas capacidades exceden por mucho las necesidades convencionales y nos permiten una buena expectativa de crecimiento y tiempo de vida útil sin obsolescencia.

En cuanto a la red, se recomienda que la tasa de transmisión de datos o "ancho de banda" sea de 10 a 100 Mbps[1] para una red cableada, ya que éste es el estándar más común capaz de satisfacer las necesidades de cualquier sistema de considerable complejidad.

Si se trata de una red inalámbrica, la tecnología de acceso al medio empleado por los Puntos de Acceso o Puentes CSMA/CA[2], suele ofrecer, atendiendo a datos empíricos, un rendimiento de un 40-50% sobre el total de la tasa de transmisión. Si utilizamos equipos capaces de transmitir de 11 a 22 Mbps la tasa de transmisión en la práctica será de unos 4.4 a 5.5 Mbps.

Según los datos de varios fabricantes, utilizando esta tasa de transmisión, la capacidad máxima de usuarios soportados por cada punto de acceso viene determinada por el uso que hagan éstos de la red:

a) 50 usuarios que se encuentran ociosos a menudo y que sólo acceden a su correo electrónico.
b) 25 usuarios que hacen uso intensivo del correo electrónico, páginas Web y transmiten/reciben ficheros de tamaño medio.
c) 10-20 usuarios que hacen un uso constante de la red y transmiten/reciben ficheros de gran tamaño.

Podemos observar que si usamos equipos capaces de transmitir de 11 a 22 Mbps estaremos cubriendo ampliamente las necesidades del proyecto, manteniendo un tráfico de datos bastante ágil y con buenas expectativas de crecimiento. Para corroborar estos datos, hemos observado el comportamiento de equipos con esta tasa de transmisión y hemos comprobado que son capaces de transmitir datos con casi la misma velocidad que enlaces cableados para aplicaciones que van desde el despliegue de páginas Web hasta la transmisión de videoconferencias, lo cual nos indica que una red de pocos usuarios y tareas no tan complicadas como la nuestra estaría bien cubierta con esta tasa de transmisión.

2.1.4. Seguridad

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado nuevos riesgos de seguridad. La salida de estas ondas fuera del edificio donde está ubicada la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible a la empresa y a la seguridad informática de la misma.

La topología de estas redes consta de dos elementos clave, las Estaciones Cliente (EC) y los Puntos de Acceso (PA). La comunicación puede realizarse directamente entre estaciones cliente o a través del PA. El intercambio de datos sólo es posible cuando existe una verificación entre EC y PA y se produce la asociación entre ellos (una EC pertenece a un

[1] Mbps. Mega bits por segundo.
[2] CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance, Múltiple Acceso mediante el Sensado de la línea Portadora / con Anulación de Colisiones).

PA). Por defecto, el PA transmite señales de gestión periódicas, el PA las recibe e inicia la autenticación mediante el envío de una trama de autenticación. Una vez realizada está, la estación cliente envía una trama asociada y el PA responde con otra.

Varios son los riesgos derivables de este factor. Por ejemplo, se podría penetrar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un punto de acceso ilegal más potente que capte las estaciones cliente en vez del punto de acceso legítimo interceptando la red inalámbrica. También sería posible crear interferencias o una posible denegación de servicio con solo introducir un dispositivo que emita ondas de radio a una frecuencia de 2.4 GHz (frecuencia utilizada por las redes inalámbricas).

La posibilidad de comunicarnos entre estaciones cliente directamente, sin pasar por el punto de acceso permitiría atacar directamente a una estación cliente, generando problemas si esta estación ofrece servicios TCP/IP o comparte ficheros. Existe también la posibilidad de duplicar IP o MAC[3] de estaciones legítimas.

Los puntos de acceso están expuestos a un ataque de fuerza bruta para averiguar los passwords, por lo que una configuración incorrecta de los mismos facilitaría la entrada en una red inalámbrica por parte de intrusos.

A pesar de los riesgos anteriormente expuestos, existen soluciones y mecanismos de seguridad para impedir que cualquiera con los medios suficientes pueda introducirse en una red; unos mecanismos son seguros, otros de menor efectividad. El tema de la seguridad de nuestro proyecto será ampliado en la parte correspondiente a la implantación de la red.

2.1.5. Expectativas de crecimiento

Este proyecto no tiene expectativas de crecimiento a corto plazo, sin embargo, es posible que en el siguiente año se implemente un servicio de atención vía Internet, por lo que las capacidades de los equipos sugeridos no quedarán obsoletas. Se tratará de elegir alternativas que posibiliten el incremento de equipos conectados a la red, esto se logrará al considerar equipos rápidos y con un número de conexión superior a las que plantea el proyecto.

Existe la expectativa de enlazar más sucursales por manera similar, pero la decisión de la administración de la empresa dependerá del funcionamiento que presente este proyecto prototipo y de las alternativas tecnológicas que surjan en el transcurso de este año respecto a costos y capacidad.

En la sección correspondiente a la implantación de la red se abordarán con mayor amplitud las posibilidades de crecimiento que tiene nuestro sistema según los equipos elegidos y el diseño lógico del sistema.

[3] MAC (Media Access Control, Control de Acceso Medio)

2.2. DISEÑO DE LA RED

2.2.1. Justificación de la tecnología inalámbrica

En resumen, las características físicas del entorno donde se instalará la red de computadoras son las siguientes:

a) Distribución de las instalaciones en 3 diferentes edificios, separados por calles y diversas construcciones con una distancia máxima de 2 kilómetros.
b) Imposibilidad de instalar cable coaxial, par trenzado o fibra óptica a través de las calles para comunicar los edificios.
c) Necesidad de instalar el sistema en el primer o segundo piso de los edificios.
d) Conectar una computadora que se encuentre en la planta baja de cada edificio.

Estas características del entorno nos orientan hacia las redes inalámbricas como solución del problema ya que este tipo de tecnología es aplicable o deseable en sistemas como el nuestro que requieren la funcionalidad y los beneficios que ofrecen las redes como Ethernet, pero sin la limitante de los cables. Esta tecnología tiene aplicaciones inmediatas como:

- Cuando se desea movilidad dentro de la organización, tal vez en adición a la red de cableado.
- Cuando se necesita flexibilidad para realizar cambios y movimientos dentro de la organización, o en algunas áreas específicas.
- Cuando el edificio no permite la instalación de cables.
- Cualquier organización que requiera flexibilidad y obtener ahorros eliminando rentas de enlaces probados.

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 o si se trata de comunicar dos puntos distantes: a escasos metros, en edificios con problemas de instalación de cableado o distancias donde no llega el tendido de cables, un par de kilómetros uno del otro, etc.

La solución más común a este inconveniente es la utilización de líneas telefónicas o de fibra óptica para lograr la transmisión de datos. Lamentablemente estas suelen transportar información a poca velocidad o se transforman en muy costosas. Sin embargo, gracias a los avances tecnológicos en telecomunicaciones, se ha conseguido transmitir datos a grandes distancias, con velocidades de hasta 11 Mbps, a un muy bajo costo.

Básicamente, ellos son radio módems que permiten comunicar computadoras punto a punto o como punto a multipunto con "Access Points", estableciendo enlaces como el mostrado en la Figura 2.5.

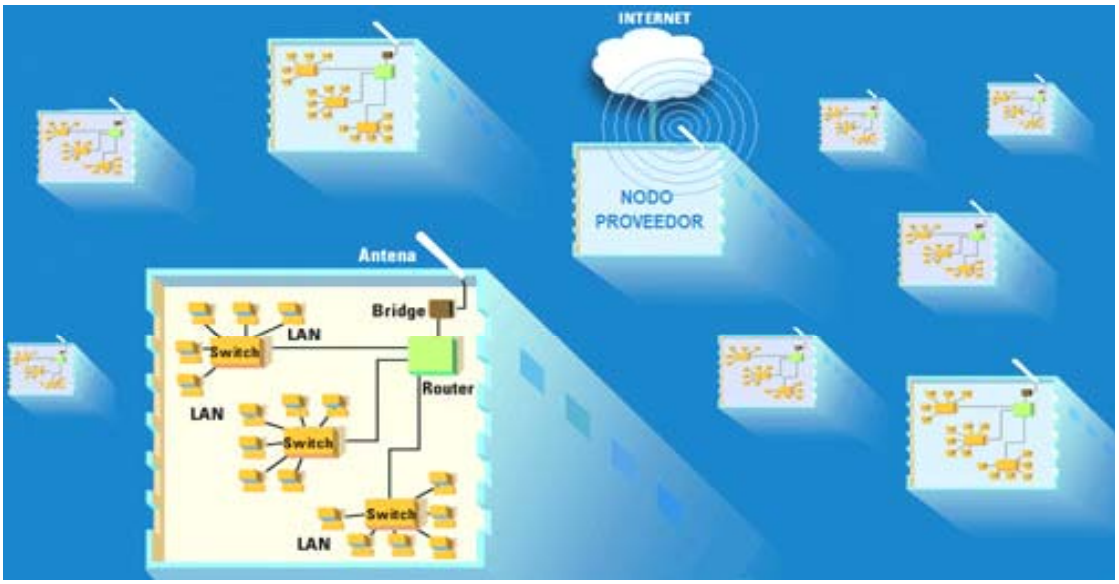


Figura 2.5. Ejemplo de transmisión inalámbrica

Otra conveniente prestación de estos dispositivos reside en el acceso a Internet, ya que es posible proveer conexión a la red mundial, a través de este sistema inalámbrico, llegando a lugares ajenos a las últimas tecnologías (ADSL, fibra óptica, etc.).

Otro punto a favor para la implementación de esta tecnología es la frecuencia de trabajo que es de 2.4 Ghz, una frecuencia libre (ISM Band) y no requiere licencia para la transmisión de datos ante la CNC (Comisión Nacional de Comunicaciones) lo cual disminuye notablemente el costo final de su implementación.

Es por ello que en nuestro diseño utilizaremos esta clase de tecnología bajo la estructura que plantearemos a continuación.

2.2.2. Diseño

Nuestro primer edificio que corresponde a la CENTRAL A, llevará a cabo la función de servidor, ya que difundirá a cada una de las otras entidades conectadas toda la información para su funcionamiento y la actualización de cada datos requerido.

En el segundo piso se instalarán 4 computadoras, las cuales estarán conectadas entre sí por medio de cable de par trenzado hacia un interruptor (switch).

Este "switch" tendrá conectado a su vez un "Access Point" – "Bridge" que nos permitirá realizar la interconexión entre edificios de manera inalámbrica.

Puesto que el “Access Point” – “Bridge” necesita comunicarse a gran distancia, será necesario proveerlo de una antena, la cual se colocará en el exterior del edificio. Nos ayudará el hecho de que nuestro sistema se encuentre en la parte más alta del inmueble ya que esto servirá para una mejor recepción y transmisión de datos. La estructura anterior se muestra en la Figura 2.6.

Figura 2.6. Conexiones de la Central “A”

El segundo edificio corresponderá al ANEXO B, el cual será una de las 2 entidades que se conectarán. Este edificio está conformado por una planta baja destinada al servicio de restaurante y la bodega, además de un primer piso que tendrá como objetivo albergar oficinas y el equipo de cómputo, el cual tendrá como función el recibir y mandar todo tipo de datos requeridos a la CENTRAL A, únicamente.
Contará con 3 computadoras unidas en red por medio de cable de par trenzado en un “switch”, que a su vez, tendrá conectado un “Access Point” – “Bridge” con una antena para realizar la comunicación inalámbrica con la CENTRAL A. La siguiente figura ilustra el modelo.

Figura 2.7. Conexiones del Anexo “B”

El tercer y último edificio será el ANEXO C (mismo número de pisos, equipos de cómputo y conexiones que el ANEXO B). De la misma manera, sólo se comunicará con la CENTRAL A.

Figura 2.8. Conexiones del Anexo "C"

La siguiente figura ilustra la estructura global antes descrita:

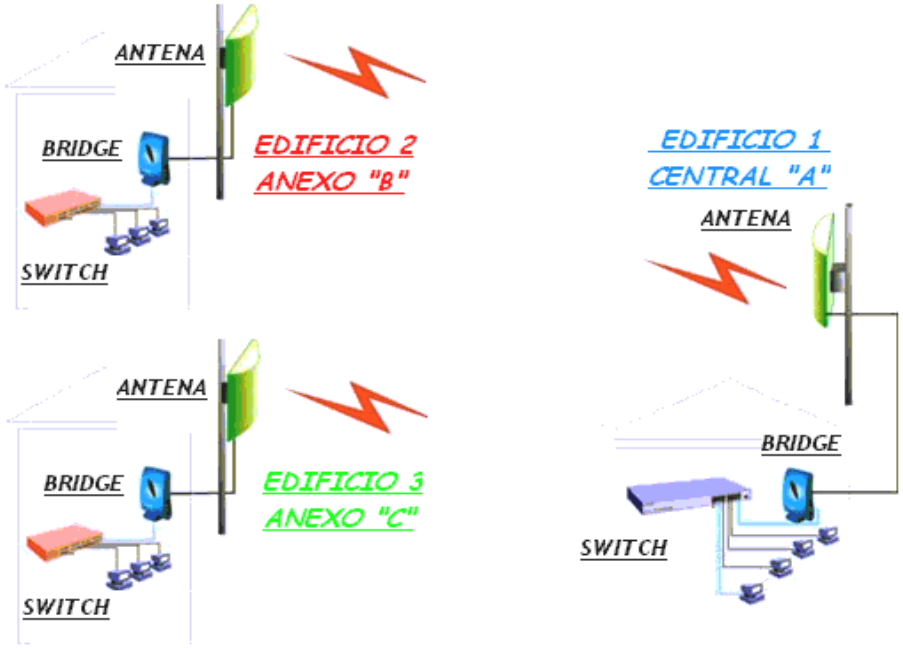


Figura 2.9. Conexión global

2.2.3. Diseño alternativo

El diseño anterior nos permite satisfacer las principales necesidades de nuestro proyecto, sin embargo, la tecnología inalámbrica nos ofrece otra solución más cómoda, elegante y con mejores expectativas respecto a la movilidad del sistema pero obviamente con un mayor costo. Esta alternativa consiste en sustituir la conexión cableada de cada uno de los equipos de las tres entidades a su respectivo "switch", por una conexión inalámbrica de la siguiente manera:

- Mediante el uso de tarjetas de red inalámbricas podemos ser capaces de darle libertad a las computadoras de escritorio. Estas tarjetas se instalan directamente en la ranura PCI Bus dándole acceso inalámbrico a los equipos de redes o a Internet permitiéndonos crear una red sin cables. Podemos conectar varios equipos con tarjeta inalámbrica a un Punto de Acceso y eliminar todos los cables que van desde la tarjeta de red convencional de la computadora hacia un nodo.

De esta forma, para nuestro proyecto podemos establecer la siguiente configuración (válida para las tres entidades, puesto que son prácticamente iguales):

- Colocaremos un "switch" de 4 puertos; en un puerto podemos conectar un "Access Point" con antena externa que servirá como "Bridge" y realizará la conexión a través de edificios y en otro puerto conectaremos otro "Access Point" que se solamente comunicará con las computadoras de la entidad, cada una de las cuales contará con su respectiva tarjeta de red inalámbrica. Esta configuración se muestra en las siguientes figuras:

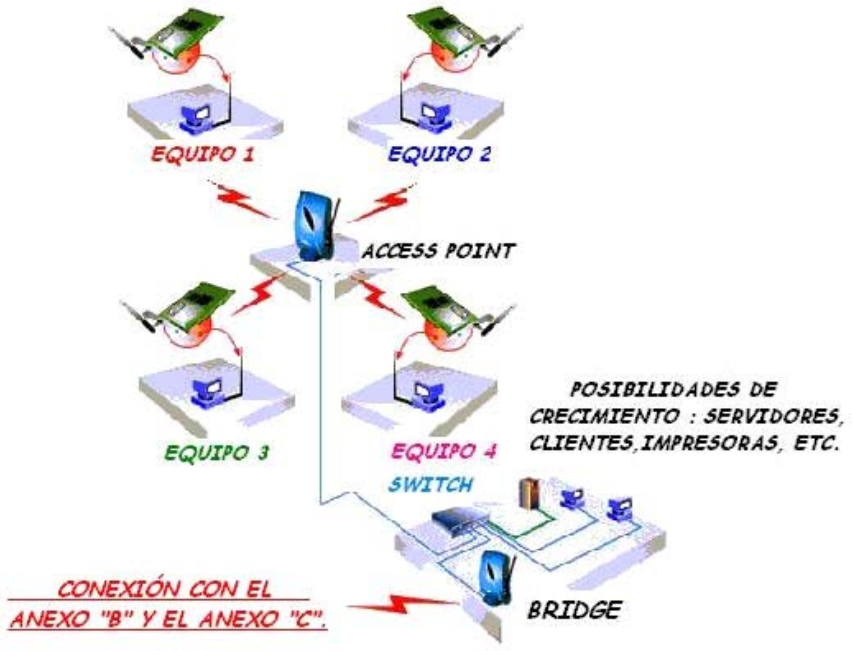


Figura 2.10. Conexiones de la Central "A"

Figura 2.11. Conexiones del Anexo "B"

Figura 2.12. Conexiones del Anexo "C"

2.3. HARDWARE

En esta sección presentaremos las opciones de hardware que existen para ser implementado. Analizaremos las características básicas de equipos de diversos fabricantes y en el capítulo destinado a la implementación indicaremos cuáles fueron las opciones seleccionadas y las razones de su elección.

***NOTA*:** Todos los precios están expresados en pesos mexicanos y vigentes al mes de Febrero del año 2004.

2.3.1. Tecnología aplicada

Las tecnologías consideradas para el desarrollo de la red inalámbrica han sido: 802.11, (en sus modalidades a,b,g), Bluetooth, HomeRF e Hiperlan 2. La siguiente tabla resume las características de cada una de estas tecnologías y nos ofrece las razones para elegir alguna de ellas para nuestro proyecto.

Tecnología Inalámbricas						
Características	**Bluetooth**	**HomeRF**	**HiperLAN 2**	**802.11b**	**802.11g**	**802.11a**
Espectro	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz
Velocidad máx.	1 Mbps	2 Mbps	54 Mbps	11 Mbps	54 Mbps	54 Mbps
Alcance	~10 m	~100 m	~100 m	~100 m en interiores y varios kilómetros en exteriores con ayuda de antenas	~70 m en interiores y varios kilómetros en exteriores con ayuda de antenas	~100 m en interiores y menor a 300 metros en exteriores
Redes	PAN	WLAN	WLAN	WLAN	WLAN	WLAN
Voz y datos	Sí	Sí	Sí	Sí	Sí	Sí
Seguridad	Sí	Sí	Sí	Sí	Sí	Sí
Topologías	Punto a punto	Punto a punto y estrella	Punto a punto y estrella	Punto a punto y estrella	Punto a punto y estrella	Punto a punto y estrella
Selección de frecuencias	FHSS	FHSS	DSSS	DSSS	DSSS	DSSS
Otras Características						
Tipo de red	PAN	WLAN	WLAN	WLAN	WLAN	WLAN
Órgano estandarizado	Bluetooth SIG	HomeRF Working Group	ETSI	IEEE	IEEE	IEEE
Disponibilidad de productos	Media	Media	Baja	Alta	Alta	Escasa
Coste	Medio	Medio	Muy Alto	Alto	Muy Alto	Alto

Tabla 2.1. Características Tecnológicas Inalámbricas

La tecnología escogida para el desarrollo de la red inalámbrica de nuestro proyecto es la 802.11b del IEEE. Esta tecnología cumple los requisitos impuestos para nuestro sistema de flexibilidad, prestaciones, disponibilidad, seguridad y costo. Las otras tecnologías estudiadas han sido rechazadas por los siguientes motivos:

1. **Bluetooth:** Los motivos principales para la desestimación de esta tecnología fueron la escasa velocidad (1 Mbps) y su corto alcance (~10 m). Esta tecnología está enfocada a la comunicación en interiores y dado que nuestro proyecto requiere comunicación a través de edificios resulta inadecuada.
2. **HomeRF:** Los motivos principales para la desestimación de esta tecnología fueron su escasa velocidad (2 Mbps) y el enfoque de dirigir los productos al hogar.
3. **HiperLAN 2:** Esta tecnología es la más avanzada actualmente (junto con 802.11a), disponiendo de las velocidades de transmisión más altas (54 Mbps), equiparándose a las redes cableadas convencionales. A pesar de ello, es una tecnología bastante reciente y solo algunas pocas compañías disponen de productos competitivos para el mercado. Los costos también son algo elevados, aunque se espera que a medida que se vaya incorporando al mercado éstos bajen.
4. **802.11 a:** Es la mejor tecnología, sin embargo es tan reciente que se encuentran muy pocos proveedores de ella en nuestro país y su precio es bastante alto. Además, resulta incompatible con las tecnologías 802.11b y 802.11g, lo que tal vez genere problemas en cuanto se presenten alternativas de crecimiento que seguramente implicarán la utilización de dispositivos de diferente tecnología, además no estamos seguros de su éxito para un futuro y corremos el riesgo de atarnos permanentemente a este tipo de equipos.
5. **802.11 g:** Esta tecnología tiene las mismas prestaciones que 802.11b y además una velocidad de transmisión superior (54 Mbps), sin embargo aunque las especificaciones acerca del equipo nos indican que se puede utilizar para conexiones entre edificios no encontramos equipos disponibles en el mercado bajo este estándar que pudieran superar la distancia de 250 metros, ni tampoco equipos que tuvieran la capacidad de conexión con antenas que incrementaran su rango de cobertura a una distancia adecuada, por lo cual no podemos considerarla para el presente proyecto.

Las características ofrecidas por 802.11b permiten cumplir con las expectativas del cliente, principalmente respecto al costo, disponibilidad y lo más importante la distancia de conexión.

A continuación vinculamos las necesidades del cliente con las características disponibles en 802.11b.

- *Velocidad de transmisión de 11 Mbps*, equiparable a redes convencionales de cable, que permitirá en la zona de almacenaje actualizar de manera rápida los datos de inventario, asistencia de personal, precios, etc., tanto en la central como en las sucursales para disponer de los datos actualizados en cualquier momento.

- *Rango de cobertura de varios kilómetros* que proporcionará conectividad a la red entre los distintos edificios.
- *Topología de estrella* que permitirá la administración de la red desde un único punto (al igual que los "hubs" en las redes cableadas), además de minimizar el impacto derivado del fallo de un equipo de un usuario final. De la misma manera, la topología de estrella nos permite realizar conexiones Punto- punto y Punto-multipunto.
- *Roaming o itinerancia* que permitirá estar continuamente conectado a la red en cualquier desplazamiento por el interior del edificio.
- *Seguridad en las comunicaciones*, maximizando la confidencialidad de los datos de la compañía que viajan por la red.
- *Interoperatibilidad con redes Ethernet* que permitirá el acceso a los recursos de una red cableada que pudiera existir en el futuro.
- *Soporte de voz y vídeo*, pese a no ser una necesidad del cliente, éste puede verse beneficiado por una instalación de este tipo que permita la comunicación por Voz IP[4], además el proyecto contempla la posibilidad de ofrecer un monitoreo de seguridad por medio de cámaras de vídeo conectadas a los equipos de cómputo.

2.3.2. Access Point - Bridges

Cuatro han sido las soluciones que consideramos más adecuadas para el proyecto. Los productos analizados fueron: "RadioLink LAN Access Point with Bridge (Radio enlace LAN Punto de Acceso con Puente) de MICRONET, "Aironet 350 Series Wireless Bridge" (Puente Inalámbrico) de Cisco, "TEW-212APBO" de TRENDnet y "Wireless LAN Building-to-Building Bridge" (Puente de Edificio a Edificio) de 3Com.

A continuación se hará una descripción de las características principales de estos equipos para establecer un comparativo entre ellos y elegir el más conveniente para el sistema.

MICRONET RadioLink LAN Access Point with Bridge

Figura 2.13. MICRONET

[4] Voz IP. Tecnología de transmisión de voz a través de paquetes IP capaces de transmitirse por redes de datos, incluso Internet. Se encuentra en etapa de desarrollo para mejorar su calidad y velocidad.

Estándar	IEEE802.11 & 802.11b & 802.1x
Protocolo para Transmisión	TCP/IP, IPX/SPX, NetBEUI, AppleTalk, SNMP
Banda de Frecuencia	2.4 GHz hasta 2.484 GHz
Tasa de Datos	11, 5.5, 2, 1 Mbps
Tipo de Modulación	Direct Sequence Spread Spectrum (DSSS)
Antena	Viene con una antena de tipo L, Soporta una Antena Externa
Rango de Cobertura	250 m en un área abierta, alcanzando hasta varias millas con una antena externa
Potencia de salida	De 20 mW : 13 dBm a 100 mW : 20 dBm
Sensibilidad	-83 dBm @ 10E-5 BER
Seguridad	40/128bit WEP Codificación, Access Control List.
Tipo de arquitectura de red	Soporta Ad-hoc, Infraestructura y Roaming (IEEE802.11b compatible). Topología Punto-Punto y Punto- Multipunto
Suministro de Corriente	12 V DC 1000 mA (incluye alimentador AC)
Canal de Operación	11/N. America, 14/Japan, 13/Europe (ETSI)
Temperatura de Funcionamiento	0 - 50 grados C
Humedad	5% hasta 90%
Dimensiones	23 cm(Ancho) x 16cm (Profundidad) x 3.2 cm(Alto)
Peso	1.2 kg
Certificaciones	FCC part 15 Network Operating, CE, ETS 300.328
Configuración	Directa: Por medio del puerto de la consola (además de cable serial)
Garantía	Un año
Precio	$6500 aproximadamente
Disponibilidad	Se adquiere bajo pedido en 30 días aprox.

Tabla 2.2. Características de MICRONET

Cisco Aironet 350 Series Wireless Bridge

Figura 2.14. CISCO

Estándar	IEEE 802.11b
Protocolo para Transmisión	TCP/IP, IPX/SPX, NetBEUI, AppleTalk
Banda de Frecuencia	2.4 GHz hasta 2.497 GHz
Tasa de Datos	11, 5.5, 2, 1 Mbps
Tipo de Modulación	Direct Sequence Spread Spectrum (DSSS)
Antena	Dos conectores RP-TNC y capacidad de conexión con antenas opcionales
Rango de Cobertura	250 m en un área abierta, alcanzando hasta varias millas con una antena externa (28.9 km @ 11 Mbps y 40.2 km @ 2 Mbps)
Potencia de salida	100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 5 mW (7 dBm) 1 mW (1 dBm)
Sensibilidad	1 Mbps: -94 dBm, 2 Mbps: -91 dBm 5.5 Mbps: -89 dBm, 11 Mbps: -85 dBm
Seguridad	Codificación WEP de 128 bit en modo Bridge, IEEE 802.1x (incluye EAP y RADIUS en modo Access Point)
Tipo de arquitectura de red	Soporta Ad-hoc, Infrastructura y Roaming (IEEE802.11b compatible)
Suministro de Corriente	24 V DC +/- 10% a 60 V DC (Linea de poder Ethernet)
Canal de Operación	11/Norte America, 14/Japan, 13/Europe (ETSI)
Temperatura de Funcionamiento	-20° a 55° grados C
Humedad	10% hasta 90%
Dimensiones	17.1 cm(Ancho)x 15.9cm(Profundidad)x 3.3cm(Alto)
Peso	0.648 kg
Certificaciones	FCC para 15 Network Operating, CE, ETS 300.328
Configuración	Directa: Por medio del puerto de la consola (además de cable serial);Remota: Telnet, HTTP, FTP, TFTP y SNMP
Garantía	Un año
Precio	$7500 aproximadamente
Disponibilidad	Se adquiere bajo pedido en 30 días aprox.

Tabla 2.3. Características de Cisco

TRENDnet TEW-212APBO

Figura 2.15. TRENDnet

Estándar	IEEE802.11 & 802.11b & 802.1x
Protocolo para Transmisión	TCP/IP, IPX/SPX, NetBEUI, AppleTalk, SNMP
Banda de Frecuencia	2.4 GHz hasta 2.484 GHz
Tasa de Datos	11, 5.5, 2, 1 Mbps
Tipo de Modulación	Direct Sequence Spread Spectrum (DSSS)
Antena	Viene con una antena dipolo, soporta una antena externa
Rango de Cobertura	Hasta 3.5 km
Potencia de salida	De 20 mW : 13dBm a 100 mW : 20 dBm
Sensibilidad	-83dBm @ 10E-5 BER
Seguridad	64/128/256 bit de codificación WEP, Lista de control de acceso
Tipo de arquitectura de red	Soporta Ad-hoc, Infrastructura y Roaming (IEEE802.11b compatible). Hasta 100 usuarios
Suministro de Corriente	12 V DC 1000 mA (incluye alimentador AC)
Canal de Operación	11/N. America, 14/Japan, 13/Europe (ETSI)
Temperatura de Funcionamiento	0 - 50 grados C
Humedad	5% hasta 90%
Dimensiones	23 cm(Ancho)x 16 cm(Profundidad)x 3.2 cm(Alto)
Peso	1.2kg
Certificaciones	FCC part 15 Network Operating, CE, ETS 300.328
Configuración	Directa: Por medio del puerto de la consola (además de cable serial)
Garantía	Un año
Precio	$2,070 IVA incluido
Disponibilidad	Inmediata.

Tabla 2.4. Características de TRENDnet

3Com® Wireless LAN Building-to-Building Bridge

Figura 2.16. 3Com

Estándar	IEEE 802.3, IEEE 802.3af, IEEE 802.11b/Wi-Fi
Protocolo para Transmisión	TCP/IP, IPX/SPX, NetBEUI,
Banda de Frecuencia	2.4 GHz
Tasa de Datos	11, 5.5, 2, 1 Mbps
Tipo de Modulación	Direct Sequence Spread Spectrum (DSSS)
Antena	Capacidad de conexión con antenas opcionales
Rango de Cobertura	Alcance de transmisión de datos de hasta 16,9 kilómetros (10 millas), en función de la antena seleccionada (mayores distancias requieren dos 3Com Wireless LAN Building-to-Building bridges)
Potencia de salida	100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 5 mW (7 dBm) 1 mW (1 dBm)
Sensibilidad	1 Mbps: -94 dBm 2 Mbps: -91 dBm 5.5 Mbps: -89 dBm 11 Mbps: -85 dBm
Seguridad	Encriptación WEP de 40 y 128 bits y encriptación Dynamic Security Link (enlace dinámico de seguridad) de 128 bits
Tipo de arquitectura de red	Soporta Ad-hoc, Infrastructura y Roaming (IEEE802.11b compatible).
Suministro de Corriente	24V DC +/- 10% a 60 V DC (Linea de poder Ethernet)
Canales de Operación	11/Norte América, 14/Japón, 13/Europa (ETSI)
Temperatura de Funcionamiento	-20° a 55° grados C
Humedad	10% hasta 95%
Dimensiones	20.8 cm(Ancho)x 14.4 cm(Profundidad)x 4.1 cm(Alto)
Peso	0.748 kg
Certificaciones	US: FCC Part 15B&C; Canadá: Industry Canada, RSS-210; Europa: ETS 300, 328, ETS 300 826; Australia: C-Tick
Configuración	Local de manera directa y remota por medio de red
Garantía	Un año

Precio	$11,050 más IVA
Disponibilidad	Inmediata.

Tabla 2.5. Características de 3Com

NOTA: Todos los equipos antes mencionados tienen compatibilidad con redes cableadas (Ethernet), tienen la capacidad de conectarse a tarjetas PCI inalámbricas de todos los fabricantes mencionados y soportan el uso de todos los sistemas operativos más conocidos: (Windows en sus diferentes versiones: 2000 Server, NT, XP, etc., UNIX, Linux y Novell).

2.3.3. Tipos de antenas

Las antenas suelen usarse para solventar problemas como enlace visual o para añadir potencia si van acompañadas de un amplificador. Hay 2 tipos de antenas: **omnidireccional** y **direccionales**. Las omnidireccionales emiten y reciben señal desde cualquier punto y las direccionales apuntan a otra antena (que puede ser omnidireccional o direccional). Existen instrucciones para construirlas de forma casera. Esto dependerá del Access Point que vayamos a seleccionar por el cual la antena que tendrá cada punto de acceso y su dimensión será la mejor en cuestión de direccionamiento y alcance.

2.3.4. Computadoras

Los equipos de computación del restaurante deben listarse de manera que se dé un enfoque de lo que se tiene y lo que se incluirá en el sistema de red, tomando en cuenta que tipo de equipo es, con que procesador cuenta, que memoria en RAM tiene, que capacidad de disco duro tiene, con cuantos drivers cuenta y de que capacidad. Haremos una comparación de ciertas marcas, su fiabilidad y su desempeño para nuestro caso, así como sus componentes.

En el proyecto contemplamos utilizar de 3 a 4 computadoras así como una computadora portátil.

Equipos	Dispositivos	Características y redes inalámbrica	Costo
Compaq Presario 5020U 	*Procesador Intel Pentium 4 2.5GHz. *128MB en memoria RAM expandible. *40GB Disco Duro *4 ranuras de expansión libre *Unidad de disco 3.5", CD-RW / DVD *Video hasta 64MB Monitor 17"	Este es uno de los procesadores más rápidos y permite terminar sus tareas en menos tiempo. Más memoria le permite ejecutar más programas de software al mismo tiempo, pero tienen la dificultad de no permitir una acentuación para las redes inalámbricas la cual dificulta el trabajo de las mismas. Accesa difícilmente con 2 tarjetas de red en la máquina, e interrumpe la conexión y el funcionamiento de la misma red.	Precio $11,000 pesos mas IVA.
HP Pavilion T330U 	*Procesador Intel Pentium 4 a 2.4GHz. *256MB en memoria RAM expandible. *80GB Disco Duro. *4 ranuras de expansión libre. *Unidad de disco 3.5", CD-RW / DVD. *Mouse y Keyboard Wíreless. *Flat Panel 17".	Tiene un alto desempeño y facilidad de uso para cada uno de los usuarios que se encuentran en constante movimiento y llegan a un centro digital, con el cual puedes combinar música, videos, fotos y mucho más. El cual su compatibilidad con los accesorios para una red inalámbrica llega a tener una confiabilidad pero su costo eleva nuestros costos hacia la misma.	Precio $14,000 pesos mas IVA.
Computadora Armada 	*Procesador para servidor Intel Xeon a 2.4GHz Bus de 400MHz. *256MB memoria DDR ECC expandible. *80GB Disco Duro. *4 ranuras de expansión libre. *Unidad de disco 3.5", CD-RW. *Mouse y Keyboard Wíreless. *Flat Panel 17"	En toda las pruebas que se efectuaron, las pruebas salieron efectivas en cuanto al manejo de "Swits" y "Access Point" y tarjetas de red conjuntas, la rapidez de su "motherboard" y su procesador el cual desempeña con un 95% de éxito las pruebas y soluciones requeridas	Precio $8,500 más IVA.

TOSHIBA SATELLITE PRO M10-S405 	*Procesador Centrino Pentium M Intel. 1.4 GHz. *512 MB Memoria RAM. *37.24Gb Disco Duro. *Tarjeta de vídeo y sonido. *Unidad de disco 3.5", CD-RW / DVD. *Mini PCI 802.11b wireless con antena. *Puerto lector de MS y SD USB 2.0.	Es el primer portátil en México con tecnología Centrino que brinda conexión móvil a redes (wireless) con el máximo ahorro de energía y mayor tiempo de duración de baterías. Rendimiento excepcional diseñado para la PyME con conectividad inalámbrica en una PC móvil que remplaza una de escritorio.	Precio $13,000 más IVA.

Tabla 2.6. Características de PC´s

Selección del equipo

Una de las primeras decisiones que se deberá tomar acerca de la instalación es: ¿Qué tipo de hardware de red inalámbrica emplear?

En las organizaciones que cuentan ya con una red y se desea mejorarla, si es necesario, satisfacer estándares corporativos, las opciones pueden estar limitadas por la necesidad de ser compatibles con lo que ya se tiene. En las instalaciones completamente nuevas la selección del hardware de red, dependerá de varios factores, incluyendo el costo, el rendimiento y la compatibilidad.

Costo

El factor más importante es el costo, frecuentemente está relacionado directamente; con el rendimiento: en general, mientras más costosos sean los componentes de la red, más rápida será pero en algunas ocasiones no sucede así ya que pueden existir equipos con un costo bajo y el rendimiento es mejor. Por lo tanto, si se gasta mucho o poco dinero, la red inalámbrica será sorprendentemente eficiente dependiendo del equipo y más aún si las PC´s son poderosas.

Rendimiento

Cuanto más alta sea la frecuencia de datos bruta, es decir la información que viaja junto con los datos para especificar la dirección fuente, la dirección destino y el control de errores, por lo tanto la frecuencia de datos real siempre es de 4 % a 50% menor, dependiendo del diseño que el fabricante haya definido en la tarjeta de interfaz de red, y mientras más alta sea dicha frecuencia bruta mejor será el rendimiento, esto se notará al accesar los recursos de la red.

Compatibilidad

Algunas interfaces de red podrían no ser compatibles con el sistema operativo que se planea utilizar. Se debe asegurar que cualquier adaptador que se toma en consideración está certificado por el fabricante del sistema operativo de red y por el fabricante del adaptador para funcionar con la versión específica del sistema operativo que va a usar. De manera ideal, el fabricante del sistema operativo de red deberá estar de acuerdo con que el producto del fabricante del adaptador realmente funcione con su producto.

2.3.5. SWITCHS

En este apartado solamente presentaremos algunas opciones del mismo fabricante que el "Access-Point" ó "Bridge" que elegiremos para la implementación, buscando evitar conflictos de compatibilidad y una mejor oferta económica del proveedor.

TRENDnet TE100-S16E **16-port 10/100Mbps Fast Ethernet Switch** Número de puertos: 16 Costo :$1,225 IVA incluido	
TRENDnet TE100-S88Eplus **8-port 10/100Mbps Auto-MDIX Fast Ethernet Mini Switch** Número de puertos : 8 Costo :$500 IVA incluido	
TRENDnet TE100-S5Pplus **5-port 10/100Mbps Auto-MDIX Fast Ethernet Mini Switch** Número de puertos : 5 Costo :$385 IVA incluido	

Tabla 2.7. "Switchs"

2.3.6. TARJETAS INALÁMBRICAS

De la misma manera que para los "switchs", sólo presentaremos algunas de las opciones del fabricante que escogeremos para los "Access-Point" ó "Bridge". El uso de estas tarjetas, está condicionado al diseño de la implementación final.

TEW-401PC Tarjeta de red Wireless Tasa de transmisión: 54 Mbps Costo : $1,430 IVA incluido	
TEW-223PI Tarjeta de red Wireless Tasa de transmisión: 11Mbps Costo : $890 IVA incluido	

Tabla 2.8. Tarjetas de red "Gíreles"

2.4. SOFTWARE

2.4.1. Sistemas operativos para establecer una red inalámbrica

En una red es muy importante para su operación, el software adecuado ya que permite la interacción con el usuario y el correcto funcionamiento de la misma.

Dentro de este software se encuentran los sistemas operativos que es un conjunto de programas que regulan el funcionamiento de la misma, dando todos los elementos para la interface con el usuario ya que éste debe ser de manera transparente es decir, que el usuario vea de una forma fácil y accesible el manejo de la misma. Así como por medio del sistema operativo se definen los niveles de seguridad de la red otorgando o limitando accesos a ciertos archivos asegurando la integridad de la información, de la misma forma asignando y limitando el uso de recursos lógicos. También el sistema operativo le da al usuario una administración correcta de todos los recursos de una red ya sean físicos o lógicos.

2.4.1.1 Arquitectura del sistema operativo para red

Las arquitecturas de los sistemas operativos son:

- Servidores de Discos
- Servidores de archivos
- Cliente - Servidor
- Punto a Punto

A continuación explicaremos en qué consiste cada una de las arquitecturas mencionadas anteriormente.

Servidores de Discos

En un sistema operativo servidor de disco, simplemente define secciones en el disco duro del servidor y se las asigna a cada usuario, de forma que, cuando desde cualquier estación de trabajo quiera entrar al disco duro de la red, solamente es necesario seleccionar una unidad lógica y en ese momento se entrar a la partición del disco duro asignada a dicho usuario. En esta arquitectura cada sección es independiente de la otra, ya que si dos usuarios quieren entrar a una misma aplicación ésta deberá estar cargada en las dos partes del disco duro correspondiente a cada uno de los usuarios. Esta tecnología ya no se usa actualmente pero sirve como referencia para servidores de CD´s y servidores de respaldos.

En un servidor de discos, los programas que se ejecutan en una PC cliente pueden leer y escribir en lo que se consideran como un recurso de disco local y lógico. Lo que es importante en esta situación es que el cliente tiene que hacer todo el trabajo de mantenimiento. Por ejemplo, cuando se abre un archivo para leerlo, el cliente lee la información del directorio que describe qué archivos están en determinado lugar y lee los datos contenidos en él.
Un sistema de servidor de discos es uno de los sistemas de compartición de recursos más fáciles de implantar. Todo el trabajo duro de controlar el ambiente y coordinar múltiples PC´s que acceden a las mismas áreas de datos tiene que llevarse a cabo por las aplicaciones.

Servidores de Archivos

En esta arquitectura del sistema operativo se comparten los archivos que se almacenan en el servidor, de esta forma no se comparte disco duro físico, si no que se resuelve el problema de la administración de archivos de la red.

También administra el acceso al disco compartido y a la información que contiene de tal forma que dos o más usuarios puedan entrar a la misma aplicación sin que ésta esté cargada doble vez como sucedía en el servidor de discos; es decir, se comparten archivos en un ambiente multiusuarios (muchos usuarios pueden entrar a un mismo archivo).

En los sistemas servidor de archivos, las PC´s pueden ser ya sea servidores o clientes. Los servidores controlan el acceso de los clientes a sus servicios, les proporcionan acceso a los archivos que se encuentran almacenados en ellos, manejan el acceso a múltiples clientes, proporciona servicios de impresión y constituyen de hecho, el foco de los recursos de una red.

En los sistemas servidor de archivos, la seguridad es mucho más estricta. Dado que ésta representa una inversión mucho mayor.

Ventajas de las redes basadas en un sistema servidor de archivos:

- Rendimiento: dado que los sistemas de servidor de archivos deben dar apoyo a muchos clientes a la vez, están diseñados y optimizados para proporcionar una respuesta rápida y un alto flujo de datos.
- Seguridad: se requieren características de seguridad avanzadas, ya que los sistemas de servidor de archivos deben apoyar muchos usuarios, los principales fabricantes ofrecen servicios de seguridad sólidos y avanzados.
- Manejo: como los servicios están centralizados, los sistemas de archivos son más fáciles de manejar que los ambientes punto a punto. Así mismo, los servicios están diseñados para ser manejados de manera más avanzada.
- Facilidad de actualización: los sistemas de servidor de archivos están diseñados para ser escalables y soportar a muchas más estaciones de trabajo que los sistemas punto a punto que están diseñados para grupos de trabajo pequeños.

Desventajas de los sistemas servidor de archivos:

- Costos: sistemas de servidor de archivos generalmente son más caros, tanto en costo por usuario como en costos de instalación ya que se requiere de una PC especializada.
- Complejidad: los sistemas de servidor de archivos son bastante complejos. Los problemas de manejo y diagnóstico exigen bastante experiencia.

Arquitectura Cliente – Servidor

Esta arquitectura es una tecnología de punta. La mayoría de los procesos se efectúan en el servidor, el cliente hace peticiones a los servidores y éste atiende dichos procesos ya que en una red existen procesos distribuidos, donde el procesador del servidor ejecuta las instrucciones del sistema operativo de red, el procesador de las estaciones de trabajo procesan las tareas locales, esto implica que la Arquitectura cliente-servidor, el servidor con procesadores poderosos hace los trabajos más pesados y las tareas más sencillas se las deja al procesador de las estaciones de trabajo, de esta forma las tareas se reparten en forma más eficiente entre todos sus recursos.

Esta arquitectura se utiliza principalmente para explotar las aplicaciones de base de datos, como los manejadores de base de datos donde una parte corre en el servidor, a esta parte se le llama back-end y la parte que corre el cliente se le llama front-end. El cliente hace una solicitud, el servidor hace una búsqueda de archivo y localiza los datos, después entrega la información, el cliente recibe la información y posteriormente regresa la información al servidor guardándola.

Algunas ventajas de los sistemas cliente - servidor:

- Seguridad: es mayor porque los datos de una base de datos del servidor son tomados de manera indirecta. Los usuarios no pueden ver en realidad los archivos de datos al menos que se les dé acceso explícito.
- Rendimiento: se puede mejorar, ya que un servidor de aplicación posterior bien diseñado puede proporcionar una mejor coordinación de usuarios múltiples y por lo tanto, un mejor rendimiento. En el caso de los servidores de base de datos para encontrar lo que quieren, pueden enviar solicitudes al servidor y el servidor entrega solamente lo que necesita.
- Efectividad: en relación con el costo es mucho mayor. Los clientes sólo necesitan el poder suficiente para ejecutar adecuadamente la aplicación frontal.

Las desventajas de los sistemas cliente - servidor son:

- Complejidad: los sistemas cliente-servidor generalmente no son fáciles de configurar ni de manejar.
- Requerimientos: para dar servicio a muchos usuarios, el componente cliente de un sistema cliente-servidor frecuentemente necesita ejecutarse en una computadora funcional y eficaz.
- Las aplicaciones de servidor: tienden a ser grandes, complejas y generalmente necesitan mucha memoria.
- Costo: el rendimiento del servidor se reduce conforme aumenta el número de usuarios. Para recuperar los altos niveles de rendimiento, el software del servidor tal vez tenga que ejecutarse en una máquina dedicada especialmente a este servicio.

Arquitectura Punto a Punto:

En esta arquitectura todos los nodos son servidores y estaciones de trabajo a la vez y se comparten archivos, disco duro e impresoras, de esta forma todas las máquinas tienen los mismos privilegios o no los tienen, lo único que no se pueden compartir son los módems. El sistema operativo de red se tiene que instalar en cada nodo de las estaciones de trabajo y aquí no se requieren de servidores dedicados.

Esta arquitectura es muy frecuente que la utilicen las pequeñas empresas que tienen la necesidad de intercambio de información, pero no disponen de recursos monetarios para hacer grandes inversiones en un departamento de sistemas demasiado complejo.

Ventajas de los sistemas punto a punto:

- Costos: los sistemas punto a punto suelen ser más baratos que los sistemas servidor de archivos y la cantidad de estaciones de trabajo es pequeña.
- Flexibilidad: la naturaleza descentralizada de las LANs punto a punto, le permite organizarlas conforme a la situación lo demande.
- Simplicidad: en conjunto, los sistemas de punto a punto son más simples que los sistemas servidor de archivos.

Desventajas de los sistemas punto a punto:

- Rendimiento: los sistemas de punto a punto generalmente son más lentos que los sistemas servidor de archivos.
- Manejo de seguridad: dado que los sistemas punto a punto están distribuidos a todo lo largo y ancho de las organizaciones, son más difíciles de controlar que uno o varios sistemas servidor de archivos de servicios centralizados.

2.4.2. Principales Sistemas Operativos comerciales en una red inalámbrica

La mayoría de los sistemas operativos existentes en el mercado utiliza cualquiera de estas arquitecturas de sistemas operativos de red mencionadas anteriormente. Sin embargo se debe determinar cuál de estas arquitecturas es la que cubre las necesidades de nuestro proyecto y cuál de los productos comerciales cubren nuestras necesidades al igual que los proveedores en el mercado.

2.4.2.1. Netware de Novell

Todas las versiones de Netware tienen ciertas características en común:

- Soporte para clientes el MS-DOS, Windows, Macintosh, el OS/2 y UNIX.
- Soporte para una amplia gama de tarjetas adaptadoras de red así como nuevas tecnologías Wireless.
- Extensos servicios de seguridad que le otorgan control sobre qué usuarios pueden establecer una conexión a un servidor de archivos, entrar a directorios, controlar el servidor, controlar empresas y manejar cuentas de usuario.
- Soporte para procesos residentes en el servidor. Estos programas se ejecutan dentro del servidor de Netware para mejorar los servicios de red.
- En todas las versiones se ofrece tolerancia de fallas a varios niveles, aunque algunos son niveles especiales.
- Los productos de Netware están estratificados en versiones que soportan diferentes números de usuarios conectados: 5, 10, 20, 50, 100, 250 y 1000.

Netware 4.x.

Netware 4.x. es un sistema operativo de 32 bits, usa un único espacio de direccionamiento sin segmentación, esto permite que los programas trabajen de un modo más eficiente. Puede manipular miles de peticiones de clientes por segundo. Incluye soporte para redes de gran alcance, principalmente mediante la incorporación de los servicios de directorio Netware NDS. Los servicios de directorio global ofrecen significativas ventajas organizacionales y administrativas.

Los servicios que ofrece Netware 4.x. integrándole NLMs son los siguientes:

- Servicio de comunicaciones.
- Servicio de base de datos.
- Soporte para distintos sistemas operativos.
- Servicio de mensajería.
- Servicio de administración de la red.
- Servicio de almacenamiento y copia de seguridad.

Requerimientos de software para ejecutar Netware

- Netware 3.x y 4.x requieren PCs Pentium 1 o superiores, con 64MB de RAM para la versión 3.x y 128MB para la versión 4.0
- Los servidores Netware 3.x y 4.x pueden soportar hasta 64 gigabytes de RAM.
- Los servidores Netware pueden soportar hasta 32 terabytes de almacenamiento en disco, además sólo se puede lograr un rendimiento realmente alto si se usa Netware en una PC verdaderamente rápida, con un procesador Pentium 4 a 2 gigabytes y un disco duro mínimo de 60 gigabytes.

2.4.2.2. Windows para grupos de Trabajo

Windows para grupos de trabajo es una colección de servicios de red punto a punto integrados en su producto insignia, Windows de Microsoft, está basado en Windows 3.1, pero este producto ofrece más que funcionalidad punto a punto, también incluye aplicaciones especiales para el ambiente de red y en combinación con Windows NT, Windows 2000 Server y Windows XP, es una solución completa de redes.

Los principales aspectos técnicos de Windows para grupos de trabajo son:

- Permite compartir archivos e impresoras para un mejor uso de los recursos.
- El administrador de Archivos Microsoft ha incluido una barra de herramientas que se personaliza y un diálogo de conexión en red para conectar unidades lógicas, para conectar en red servidores y directorios. Cuando se ejecuta el programa Mail, aparece un nuevo objeto en la barra del menú de File Man. Este objeto le da la

opción de enviar un mensaje por correo electrónico y conectarlo con un archivo seleccionado en File Man.

- El administrador de Impresión incluye una barra de herramientas y una mejor manera de conectarse a las impresoras en red. También sirve el administrador de impresión para especificar si una impresora es para compartir, así como para exigir una contraseña antes de otorgar acceso a tal impresora.
- Cuenta con un proceso de instalación inteligente que permite automáticamente configurar la tarjeta y el software de red.
- Aprovecha el poder de la PC y no tiene la necesidad de requerir un servidor dedicado.
- Aplicaciones para MS-DOS y Windows funcionan con Windows para grupos de trabajo.
- Compatibilidad con la mayoría de tarjetas de redes cableadas e inalámbricas.

Requerimientos de Hardware para redes inalámbricas

- Sistema Operativo y versiones posteriores.
- PC con procesador Intel Xeon a 2.4 o superiores.
- 128MB de RAM DDR (se recomienda 256 MB) para compartir archivos o impresoras.
- Una unidad de disco de 3.5" de alta densidad o un CD ROM y un disco duro con 40 MB de espacio disponible.
- Tarjeta de vídeo PCI 32 MB, AGP 128 MB G/FORCE y monitor a color compatible con Windows 2000 Server.
- Tarjeta de red inalámbrica compatibles con Microsoft para Windows.

WINDOWS NT

La arquitectura cliente-servidor es una tecnología que puede ayudar a construir una moderna arquitectura de información para las empresas actuales.

Microsoft Windows NT fue diseñado para el sistema cliente / servidor. Windows NT ofrece el poder, la confiabilidad y la apertura para satisfacer las exigencias de las operaciones de cómputo de misión crítica en las empresas y las de computación personal de alto nivel.

Windows NT le ayuda a realizar tareas complejas con mayor rapidez a través de su capacidad multitarea con prioridad de 32 bits y procesamiento simétrico. Al ser un sistema abierto, Windows NT tiene una gran variedad de opciones, de aplicaciones y de hardware.

Windows NT utiliza el ambiente gráfico de Windows 98 y 2000, crece con las necesidades de cómputo de la empresa, es escalable ya que funciona en diversos sistemas INTEL y RlSC y con capacidad de procesamiento simétrico. Tiene avanzado sistema de seguridad, planificado para cumplir requisitos de control central de perfiles. También soporta aplicaciones para los sistemas operativos MS- DOS, Windows, POS IX, OS/2 1.x basado en caracteres. Soporta una amplia gama de sistemas y dispositivos periféricos.

Windows NT cuenta con las siguientes características:

- Administrador de archivos: maneja archivos y directorios con soporte para el sistema de archivos de Windows NT (NTFS) y el sistema de archivos de alto nivel (HPFS) que permite el uso de nombres y archivos largos. Soporta también el sistema de archivos MS-DOS.
- Administrador de impresoras: permite conectar, instalar, proteger y compartir impresoras, observando las colas de trabajos de impresión y poder modificar el estado de los trabajos de impresión.
- Administrador de usuarios: administra la seguridad de la estación de trabajo, incluyendo la creación y el manejo de cuentas y grupos de usuarios, y políticas de seguridad.
- Administrador de discos: se puede configurar y administrar recursos del disco duro para aumentar su eficiencia, incluyendo particiones de discos adicionales y la creación de divisiones y volúmenes.
- Copia de seguridad: tiene la facilidad de respaldar datos de su propia estación de trabajo u otras máquinas a las que pueda tener acceso.

Opciones de conectividad en red:

Windows NT cuenta con el siguiente soporte en las siguientes redes:

- Banyan VINES. *
- DEC Pathworks. *
- IBM LAN Server.
- Redes IBM SNA.
- Microsoft Lan Manager.
- Microsoft Windows para grupos de trabajo.
- Novell Netware.*
- Redes TCP/IP

* Requiere software adicional

WINDOWS 2000 SERVER

Con el sistema operativo Windows 2000 Server, se ha logrado una meta en la industria del software: ser un producto evolucionado y revolucionario al mismo tiempo. Evolucionado porque Windows 2000 se construye sobre las mejores características del sistema operativo Windows NT 4.0. Revolucionario porque Windows 2000 Server establece un nuevo estándar sobre lo bien integrado que puede ser un sistema operativo con la Web, las aplicaciones, las redes inalámbricas, las comunicaciones y la infraestructura de servicios. Otras innovaciones incluyen el soporte sin precedente para los últimos dispositivos de hardware, Servicios de Terminal integrados, soporte para Redes Privadas Virtuales (Virtual Private Networks, VPN) interconstruido y mucho más.

Windows 2000 proporciona seguridad punto a punto que permite a las organizaciones integrar sistemas dentro y fuera de los límites de la red corporativa, a la vez que proporciona control de acceso completo y protección de datos. Las funciones de seguridad incluyen técnicas avanzadas para identificar quién está entrando el sistema, incluyendo el uso de claves digitales para incluir datos seleccionados y una ID única que permite a los usuarios entrar no solamente su propia computadora corporativa, sino también otros recursos compartidos (como impresoras o archivos) dentro de la red corporativa, Internet o incluso la red de sus socios de negocios.

Windows 2000 Server proporciona servicios de seguridad completos basados en estándares, incluyendo autentificación flexible, encriptación de datos, acceso de redes flexible y seguro, protección de redes privadas virtuales (virtual private networks, VPNs) utilizando estándares de Internet tales como Seguridad IP (IPSec), procesamiento seguro de transacciones y extensiones de seguridad para la plataforma de seguridad, tales como la CryptoAPI.

Al utilizar una nueva herramienta de análisis de código fuente y una nueva herramienta verificadora de controladores, reducimos la cantidad de fallas por "pantallas azules[5]" potenciales.

Windows 2000 Server es más fácil de instalar, configurar y utilizar. Proporciona servicios de administración configurables para reducir el TCO. Estos servicios de administración funcionan con las soluciones de administración existentes y con redes distribuidas heterogéneas, por tanto permiten a los departamentos de sistemas obtener el máximo valor de sus servicios de infraestructura actual. Los administradores de sistemas, personal de soporte e incluso los usuarios se beneficiarán de los completos servicios de administración interconstruidos en Windows 2000 Server.

Para nuestro caso usar en una máquina cliente también hacen que sea más sencillo instalar y administrar dispositivos de hardware que funcionan con el sistema operativo Windows 2000 Server el cual soporta un amplio rango de las últimas tecnologías de hardware y periféricos, incluyendo:

- Hardware multiprocesador.
- Dispositivos “Plug and Play”.
- Dispositivos USB.
- Adaptadores de red y “Access Point”.
- Enrutadores con capacidades QoS (Quality of Service, QoS).
- Tarjetas inteligentes (smartcards).
- Dispositivos infrarrojos.
- **Comunicaciones inalámbricas:** Windows 2000 soporta las últimas tecnologías de comunicación inalámbrica. En casos donde los cables son difíciles de usar,

[5] Pantallas Azules: Fallas directas del software adjudicado principalmente al sistema operativo Windows Microsoft debido a la inconsistencia del programa.

las comunicaciones inalámbricas ofrecen una manera alternativa para que el cliente pueda crear sus conexiones de red. Por ejemplo, ésta puede ser una manera útil de instalar un servidor en un restaurante o cuarto donde no existe cableado de red o donde no es posible instalarlo.

Windows 2000 Server cuenta con las siguientes características:

- Más rápido: "Windows 2000 ha sido hasta 100% más rápido que Windows NT Server 4.0 en pruebas realizadas. Los resultados también demuestran que Windows 2000 Server es hasta 49% más rápido cuando se implementa como servidor de archivo. Adicionalmente, Windows 2000 Server ofrece una mejora de 262% con 100 impresoras y es hasta 2.8 veces más rápido, cuando ejecuta aplicaciones basadas en ASP (basadas en la prueba interna de Microsoft).
- Mejor para integrar sus soluciones en Internet: con tecnologías completas del Web, seguridad y comunicación incorporadas, además de la escalabilidad y rendimiento para manejar la demanda de tráfico de Internet, Windows 2000 Server ofrece una plataforma única y habilitada para Internet en la cual se puede aprovechar Internet empresarial.
- Más fiable: con las mejoras a la arquitectura del sistema para proporcionar un mayor tiempo activo del servidor, tolerancia a errores, además de sistemas redundantes para mayor disponibilidad así como capacidades en línea para configuración y mantenimiento, Windows 2000 Server ofrece la confianza de que sus servidores van a estar activos y funcionando y que los clientes estarán abiertos para el negocio.
- Más fácil de usar y administrar: con las mejoras que hacen que sea más fácil de administrar y utilizar el sistema, administración eficaz centralizada y habilitada para el servicio Active Directory, además de un enfoque basado en estándares para lograr interoperabilidad con sus sistemas existentes, Windows 2000 Server incrementará la productividad de sus clientes.
- Mejor para nuevos dispositivos: Windows 2000 Server admite los avances más recientes en hardware de periféricos además de dispositivos de red para ancho de banda superior y habilitados para el directorio con el fin de asegurar que la plataforma que se integre hoy pueda aprovechar los avances más recientes de la tecnología del milenio.

Requisitos de Hardware

Windows 2000 Server

- CPU compatible con Pentium a 133 MHz o superior.
- Windows 2000 Server admite hasta cuatro CPU en un solo equipo.
- 256 megabytes (MB) de RAM recomendados como mínimo, admite un mínimo de 128 MB; 4 gigabytes (GB) máximo.
- 1.0 GB de espacio libre en disco duro.*
- Unidad de CD-ROM o DVD.

- Monitor con resolución VGA o superior.
- Teclado.
- Microsoft Mouse o periférico compatible (opcional).

* Se requiere espacio libre adicional en el disco duro si instala sobre la red.

Windows 2000 Advanced Server

- CPU compatible con Pentium a 133 MHz o superior.
- Windows 2000 Advanced admite hasta ocho CPU en un solo equipo.
- 256 megabytes (MB) de RAM recomendados como mínimo, admite un mínimo de 128 MB; 8 gigabytes (GB) máximo.
- 1.0 GB de espacio libre en disco duro.*
- Unidad de CD-ROM o DVD.
- Monitor con resolución VGA o superior.
- Teclado.
- Microsoft Mouse o periférico compatible (opcional).

* Se requiere espacio libre adicional en el disco duro si instala sobre la red.

WINDOWS XP

Por ser el último sistema operativo que ha salido al mercado ha conllevado a tener dificultad de errores en cada una de sus operaciones pero denotaremos alguna de las características para ser candidato a utilizar este software. Windows 2000 incluía mejoras para detectar la disponibilidad de una red y actuar en consecuencia.

Estas mejoras se han ampliado y complementado en Windows XP para dar cabida a la naturaleza transicional de una red inalámbrica. En Windows 2000, se utilizaba la capacidad de detección de medios (detectar una red que está conectada) para controlar la configuración de la pila de red e informar al usuario de cuándo la red no estaba disponible.

Con Windows XP esta característica se emplea para mejorar la experiencia de la movilidad inalámbrica mediante la detección de los desplazamientos a nuevos puntos de acceso; en el proceso, se exige una nueva autenticación para garantizar un acceso correcto a la red y se detectan los cambios de la subred IP de manera que se pueda utilizar una dirección adecuada para obtener un acceso óptimo a los recursos.

En un sistema Windows XP pueden existir múltiples configuraciones de direcciones IP (direcciones asignadas por DHCP o estáticas) y la configuración correcta se selecciona automáticamente. Cuando se produce un cambio de dirección IP, Windows XP permite que se realicen nuevas configuraciones si es adecuado. Por ejemplo, las reservas de calidad de servicio (QoS) se pueden actualizar y la configuración Proxy de IE se puede volver a detectar. A través de extensiones de Windows Sockets, si se desea que las aplicaciones

reconozcan la red (servidores de seguridad, exploradores, etc.), éstas pueden recibir notificación de los cambios de conectividad y actualizar su comportamiento basándose en dichos cambios. La detección automática y la posibilidad de realizar una nueva configuración eliminan la necesidad de que IP móvil actúe como mediador y resuelven la mayoría de los problemas de los usuarios al desplazarse de una red a otra.

En los desplazamientos de un punto de acceso a otro, hay información de estado y de otro tipo sobre la estación que debe moverse con la estación. Entre otros datos, se incluye información sobre la ubicación de la estación para la entrega de mensajes y otros atributos de la asociación. En lugar de volver a crear esta información en cada transición, un punto de acceso puede transmitirla al nuevo punto de acceso. Los protocolos necesarios para transferir esta información no se definen en el estándar, pero varios distribuidores de redes LAN inalámbricas se han unido para desarrollar un protocolo de punto de interacceso (IAPP) con esta finalidad, lo que mejora todavía más la interoperabilidad entre los distintos distribuidores.

Una de las nuevas características que ofrece Windows XP es que se ha mejorado la compatibilidad con las redes inalámbricas basadas en el estándar 802.11b. Las mejoras con XP con las versiones preliminares, aprovechaba cada oportunidad para dar a conocer las características que, se suponía, convertirían a XP en una plataforma ideal para las redes LAN inalámbricas (Wireless Local Area Network o WLAN) con el estándar 802.11. Para comprobarlo hemos decidido someter a prueba la funcionalidad WLAN de Windows XP Professional.

Sin embargo, y antes de compartir los resultados obtenidos, debemos explicar unos cuantos detalles acerca las redes WLAN, y ver los inconvenientes que se pueden dar con Windows XP para nuestro proyecto.

La IEEE aprobó el estándar 802.11b para marcar el comienzo de la era inalámbrica con velocidades de 11 Mbps. El incremento en el rendimiento, junto con una caída del 80 por ciento como término medio en el coste del hardware inalámbrico, provocó que las redes WLAN se convirtieran en una tecnología atractiva para empresas de cualquier tamaño, una novedad que Microsoft con Windows 2000 Server y XP contempló con sumo interés.

Debido al gran potencial de las redes inalámbricas 802.11b, dicha tecnología permanece en continuo desarrollo. Las dos áreas en las que es necesario perfeccionar el estándar son el acceso móvil y la seguridad. Ya que para Microsoft este centrando sus esfuerzos en ellas a la hora de integrar la tecnología inalámbrica en Windows XP.

Pero su deficiencia al hacer pruebas con dos tarjetas de red no queda claro en la compatibilidad con los “Access Point”.

Windows ideal para nuestro proyecto ¿Por qué?

A medida que las empresas dependen cada día más de Internet, tienen la oportunidad de hacer crecer y ampliar sus redes ya sea cableada o inalámbrica a proveedores y clientes y considerar nuevas maneras de llevar productos y servicios al mercado. Para aprovechar estas oportunidades, los negocios necesitan una infraestructura que pueda responder rápidamente a las fuerzas de mercado, con una alta fiabilidad, administración eficiente, facilidad de uso y que admite los avances más recientes en el hardware de red en este caso inalámbricas. Para lograr estas oportunidades, las empresas necesitan continuar construyendo sobre sus inversiones existentes en habilidades y sistemas. Windows 2000 Server está diseñado para satisfacer estas necesidades de las empresas de todos los tamaños, desde las organizaciones pequeñas y centralizadas hasta la empresa más grande y distribuida.

Capítulo III

IMPLEMENTACIÓN DE LA RED INALÁMBRICA

3.1. DISEÑO LÓGICO

3.1.1. Configuración Lógica

Para establecer la configuración lógica de la red debemos establecer las máscaras y submáscaras correspondientes para las direcciones IP.

La configuración lógica de IPs de la red queda como sigue:

- Tenemos la **red clase B:** 172.16.0.0 (network)
- Por lo tanto la máscara de red es: 255.255.0.0 (mask)
- Y la submáscara es: 255.255.255.0 (submask)

Si aplicamos el operador AND entre la dirección IP de la red y la submáscara se pueden definir las siguientes redes y subredes válidas para la configuración deseada.

Si solamente queremos 3 subredes y por lo menos 5 dispositivos usaríamos una submáscara:

255.	255.	11111111.	00000000
172.	016.	00000011.	00000111
172.	16.	3.	0

Por lo tanto, las direcciones para cada subred son:

Direcciones para la subred	
Dirección de red	172.16.0.0
Subred de la CENTRAL “A”	172.16.1.0
Subred del ANEXO “B”	172.16.2.0
Subred del ANEXO “C”	172.16.3.0

Tabla 3.1. Direcciones de subred

Las máquinas con direcciones válidas posibles van desde la **172.16.1.1** hasta la **172.16.1.126** para la subred de la CENTRAL "A".

De esta manera, los equipos de la CENTRAL "A" tendrán las siguientes direcciones IP:

Edificio Principal CENTRAL "A"	
Equipos	*Direcciones IP*
No. 1	172.16.1.1
No. 2	172.16.1.2
No. 3	172.16.1.3
No. 4	172.16.1.4

Tabla 3.2. Direcciones IP "CENTRAL A"

Las máquinas con direcciones válidas posibles van desde la **172.16.2.1** hasta la **172.16.2.126** para la subred del ANEXO "B".

Así, los equipos del ANEXO "B" tendrán las siguientes direcciones:

Edificio Secundario ANEXO "B"	
Equipos	*Direcciones IP*
No. 1	172.16.2.1
No. 2	172.16.2.2
No. 3	172.16.2.3

Tabla 3.3. Direcciones IP "ANEXO B"

Las máquinas con direcciones válidas posibles van desde la **172.16.3.1** hasta la **172.16.3.126** para la subred del ANEXO "C".

Los equipos del ANEXO "C" tendrán las siguientes direcciones:

Edificio Secundario ANEXO "C"	
Equipos	*Direcciones IP*
No. 1	172.16.3.1
No. 2	172.16.3.2
No. 3	172.16.3.3

Tabla 3.4. Direcciones IP "ANEXO C"

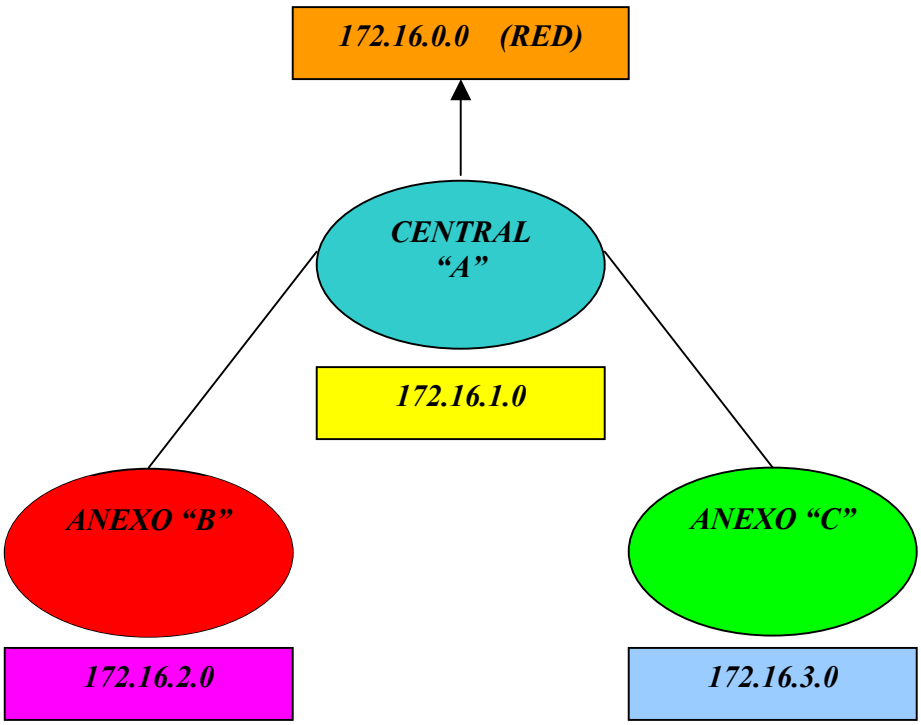


Figura 3.1. Diagrama de direcciones IP para cada entidad

3.1.2. Diseño Estructural y de configuración

Una vez que se ha creado un diseño básico es necesario "depurarlo". Es necesario diseñar y detallar los puntos específicos de la red hasta el punto en que se conozca con exactitud lo que se obtendrá cuando la instalación esté terminada.

La configuración detallada

El siguiente paso es elaborar una configuración detallada de la distribución física de la red. Esto requiere el análisis del sitio y su distribución de los equipos al igual que la estructura que se creó con anterioridad y las adiciones y modificaciones planeadas:

- Puntos de Acceso
- Switch
- Suministros de energía
- PC´s. y servidores: nuevos y reubicados.
- Impresoras

Como nuestra red tendrá que efectuarse de manera híbrida y no totalmente inalámbrica (la razón es por el costo y la seguridad que tendría que ser mucho mayor para cada equipo) no

conviene montarle a cada uno de los equipos adaptadores PCI LAN Wireless 11Mbps ya que se dispararía el costo de la red. Al consultar las reglas de cableado para el soporte de un tipo de red en particular, usted podrá determinar la longitud que tendrán los segmentos de cable y los componentes alámbricos e inalámbricos necesarios.

Éstos son algunos de los puntos que deben considerarse en la lista de compras:

- Piezas de equipo principales nuevas como PC´s e impresoras.
- Componentes inalámbricos como puentes, puntos de acceso, antenas, etc.
- Componentes de cableado, como conectores terminadores etc.
- Clips y sujetadores de cable.
- Para rayos y cobertizos para antenas.
- Cobertura de cables.
- Cables de energía extra.

En el capítulo anterior se cotizaron algunos proveedores y se optó por comprar puntos de acceso, "switch" y antenas marca TRENDware (TRENDnet), ya que los productos de este proveedor con respecto a todas las marcas es económico y es compatible con todos los sistemas operativos y además ofrecen un periodo más largo de garantía cosa que otros proveedores no proporcionan.

La referencia total de los equipos con que se van a contar por todas las características de funcionalidad, costo y seguridad son:

- *3 Servidores Xeon.*
- *7 a 9 Computadoras Pentium 4.*
- *3 Impresoras.*
- *3 Puntos de Acceso (Bridge).*
- *3 "Switches".*
- *3 Antenas omnidireccionales o direccionales.*
- *7 a 9 "No Break".*

Para el Principal A "Bisquet´s Históricos Arcos" se comprará:

1 Servidor.
3 Computadoras.
1 Tarjeta de red.
1 Impresora.
1 "Access Point".
1 "Switch".
1 Antena omnidireccional o direccional.
3 "No Break".
10 Conectores RJ45.
Cable UTP categoría 5.

Para el Anexo B "Bisquet´s Históricos Madero" comprará:

1 Servidor.
3 Computadoras.
1 Tarjeta de red.
1 Impresora.
1 "Access Point".
1 "Switch".
1 Antena omnidireccional o direccional.
3 "No Break".
10 conectores RJ45.
Cable UTP categoría 5.

Para Anexo C "Bisquet´s Históricos Tacaba" se comprará:

1 Servidor.
2 Computadoras.
1 Tarjeta de red.
1 Impresora.
1 "Access Poin"t.
1 "Switch".
1 Antena omnidireccional o direccional.
3 "No Break".
12 Conectores RJ45.
Cable UTP categoría.

3.1.3. Costos aproximados del proyecto

Software	Precio $pesos
Windows 2000 Server	$2,500.00

Cantidad	HARDWARE	Costo Unitario por Articulo en $pesos + IVA.	Costo Total en $pesos + IVA.
3	Servidor Xeon	$8,500.00	$25,500.00
8	Computadoras Pentium 4	$7,000.00	$56,000.00
3	Impresoras	$3,500.00	$10,500.00
3	"Access Point"	$2,070.00	$6,210.00
3	"Switch"	$500.00	$1,500.00
3	Antenas	$800.00	$2,400.00
8	"No Break"	$3500.00	$28,000.00
11	Tarjetas de red	$200.00	$2,200.00
100	Cable UTP categoría 5 por metro	$3.00	$300.00
40	Conectores RJ45	$3.00	$120.00

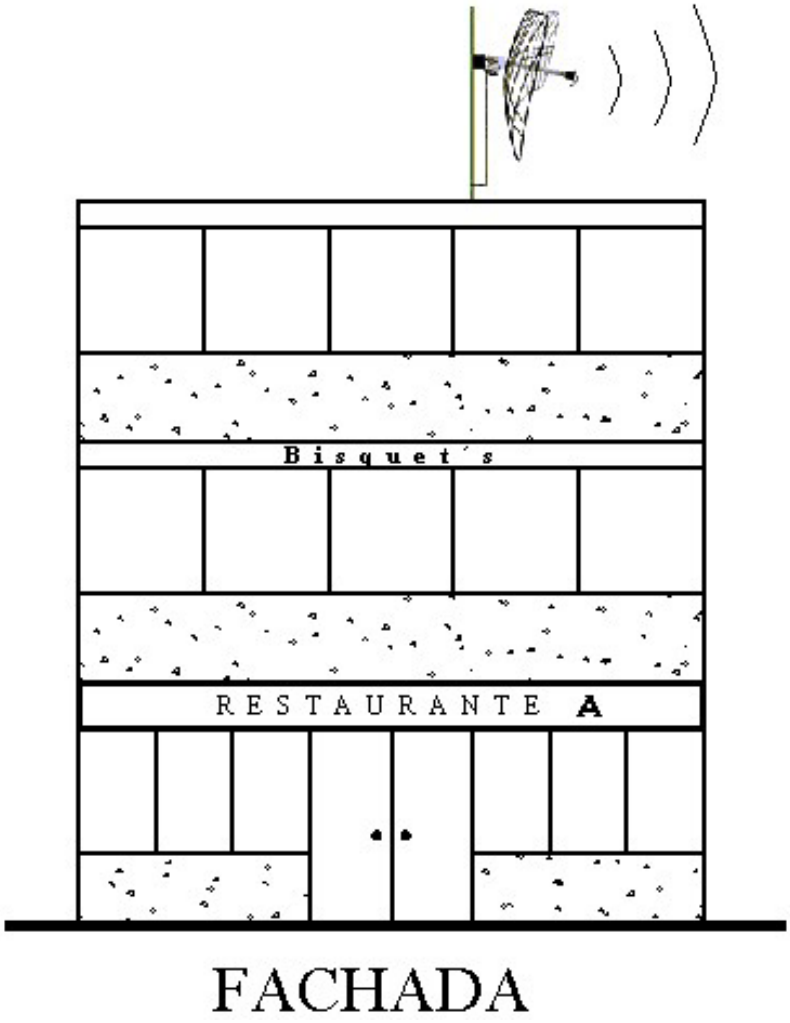
Subtotal	$112,820.50
IVA	$19,909.50
TOTAL	$132,730.00

Tabla 3.5. Costos para el Proyecto

3.1.4. Planos Estructurales

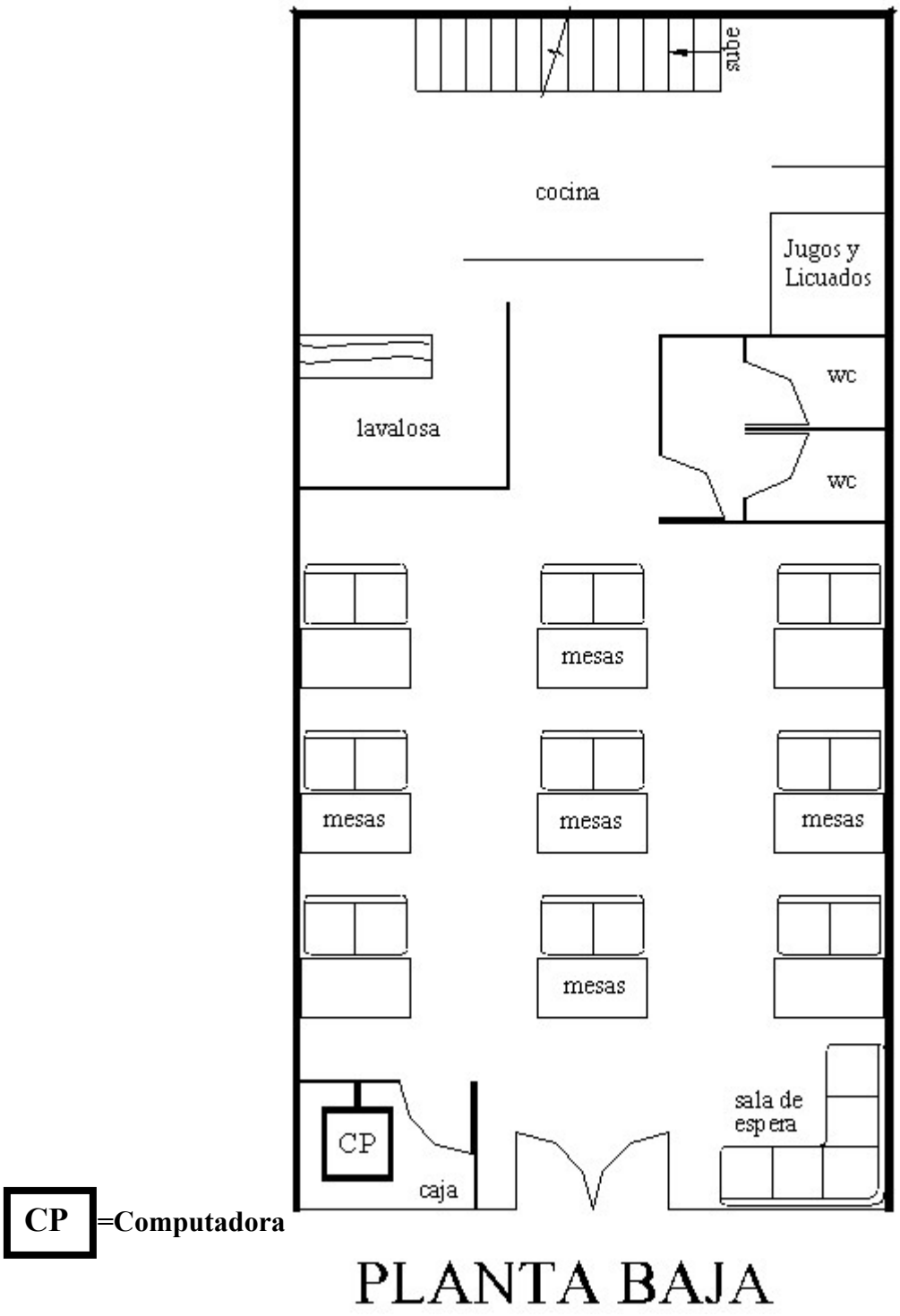
Por lo tanto la red inalámbrica de todos los restaurantes quedará instalada de la siguiente forma:

Para el Restaurante Principal A Bisquet´s Históricos Arcos tenemos los siguientes planos:



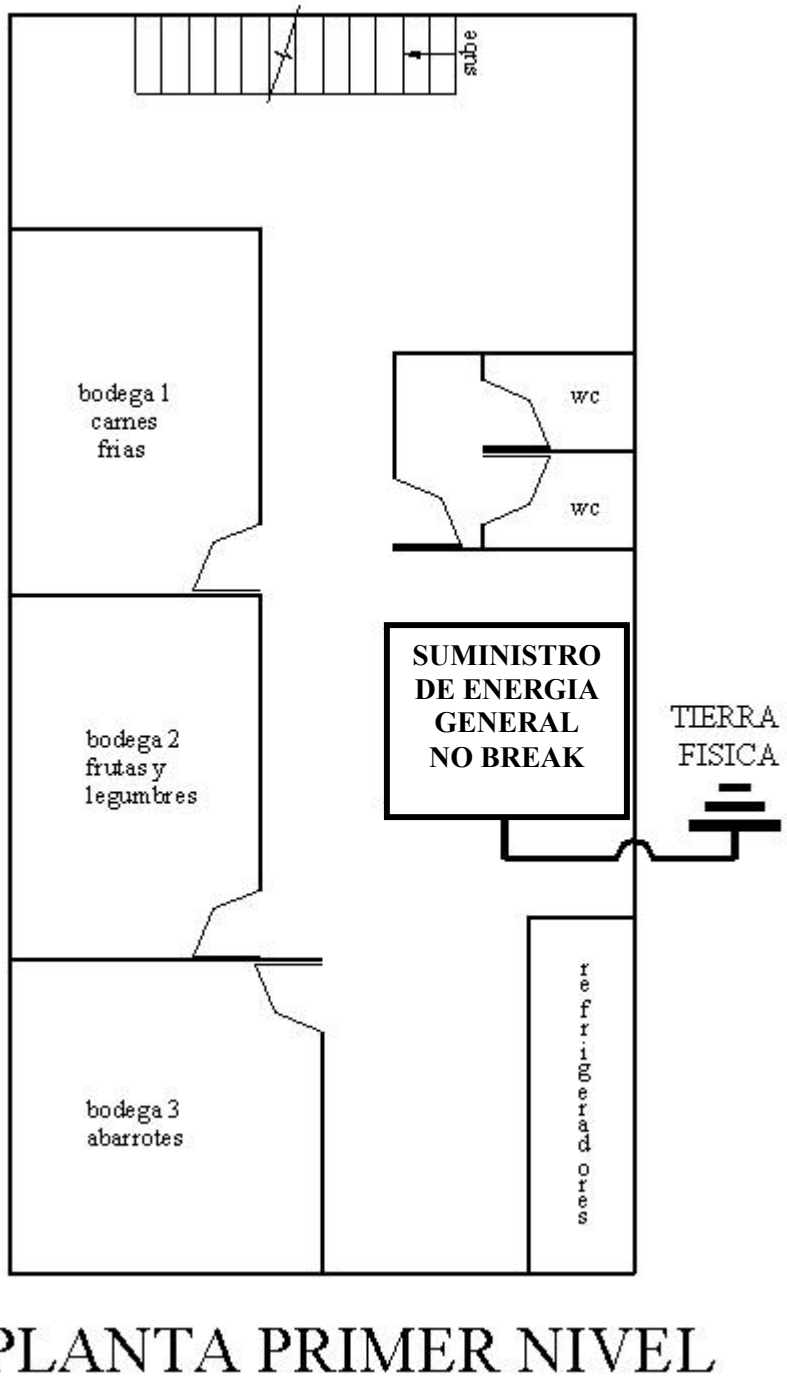
Plano 3.1. Fachada Edificio Principal Central A

Donde mostramos la fachada de nuestro proyecto a seguir el cual tendrá la antena de comunicación en la parte de la azotea.



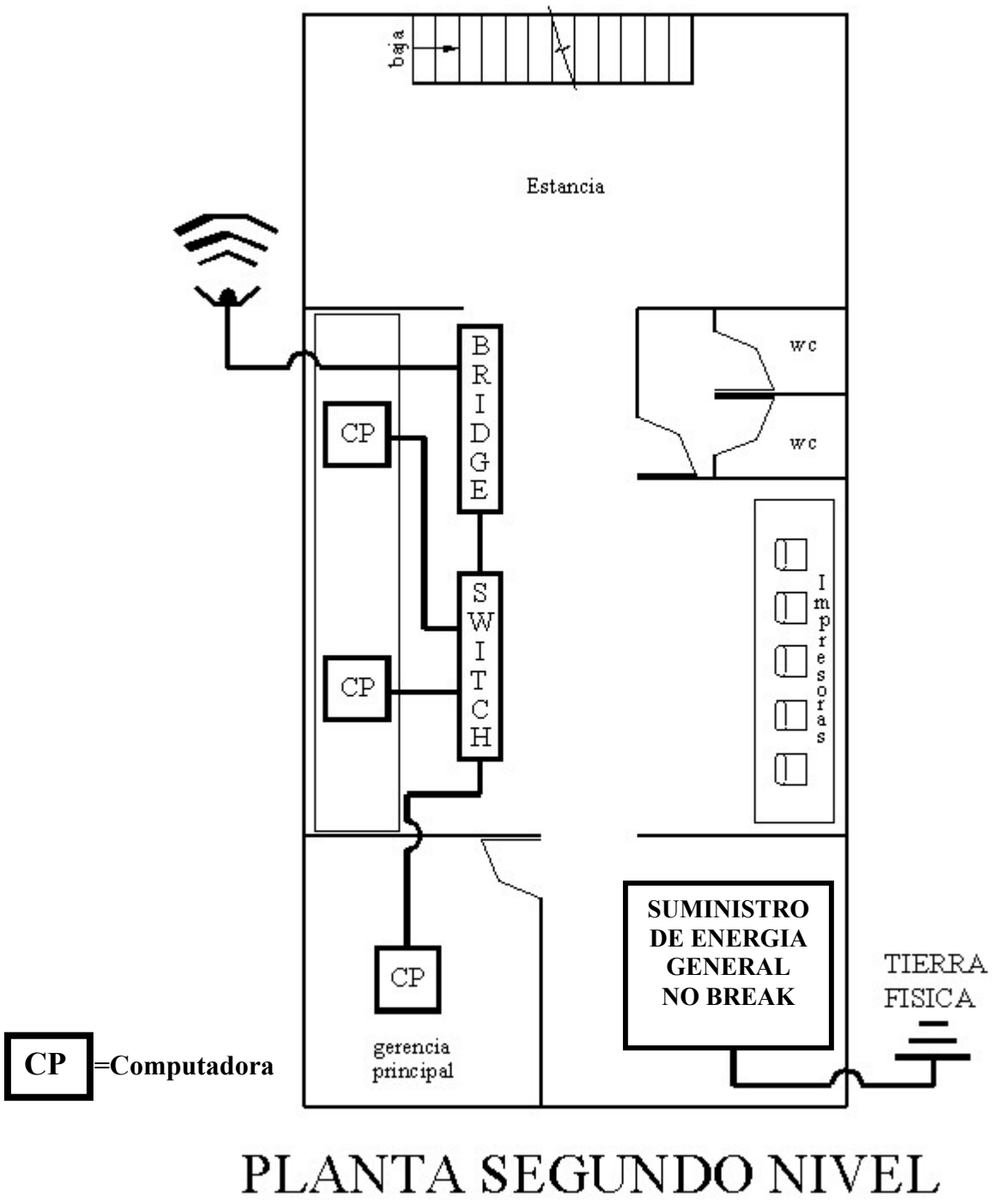
Plano 3.2. Planta Baja Edificio Principal Central A

Ésta será la entrada del edificio en donde se tendrá el servicio del restaurante, la caja que llevará una de las computadoras, sala de espera, gabinetes, baños, lavaloza, jugos y licuados, cocina y el acceso al primer piso.



Plano 3.3. Planta Primer Nivel Edificio Principal Central A

En este nivel encontraremos las bodegas de abastecimiento para la entidad, así como los refrigeradores, baños, el suministro de energía secundario y el acceso al segundo piso en donde se encontrarán las oficinas principales.

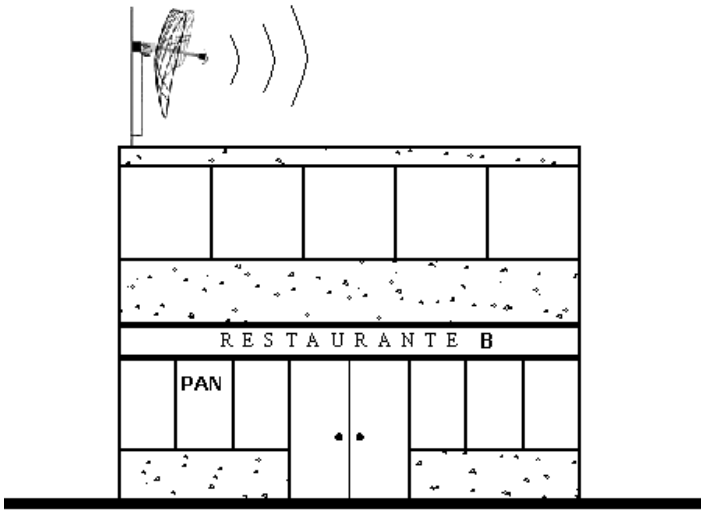


Plano 3.4. Planta Segundo Nivel Edificio Principal Central A

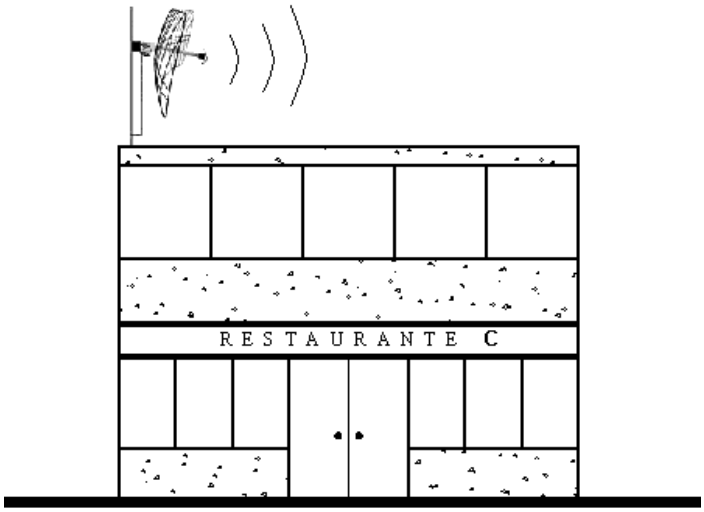
En esta parte se encontrará la red inalámbrica la cual llevará toda la administración de los anexos y hará el papel de las oficinas principales las cuales contendrán una gerencia y contemplarán tres computadoras e impresoras, 1 “Switch”, 1 “Access Point” y por último la antena para comunicarse a los demás recintos. Este edificio tendrá la mayor responsabilidad

en el manejo de la red así como toda la administración y actualización de datos e informes para cada una de las entidades conectadas a esta red.

Para el Restaurante Anexo B y C que son las sucursales Bisquet´s Históricos Madero y Tacuba tenemos los siguientes planos:



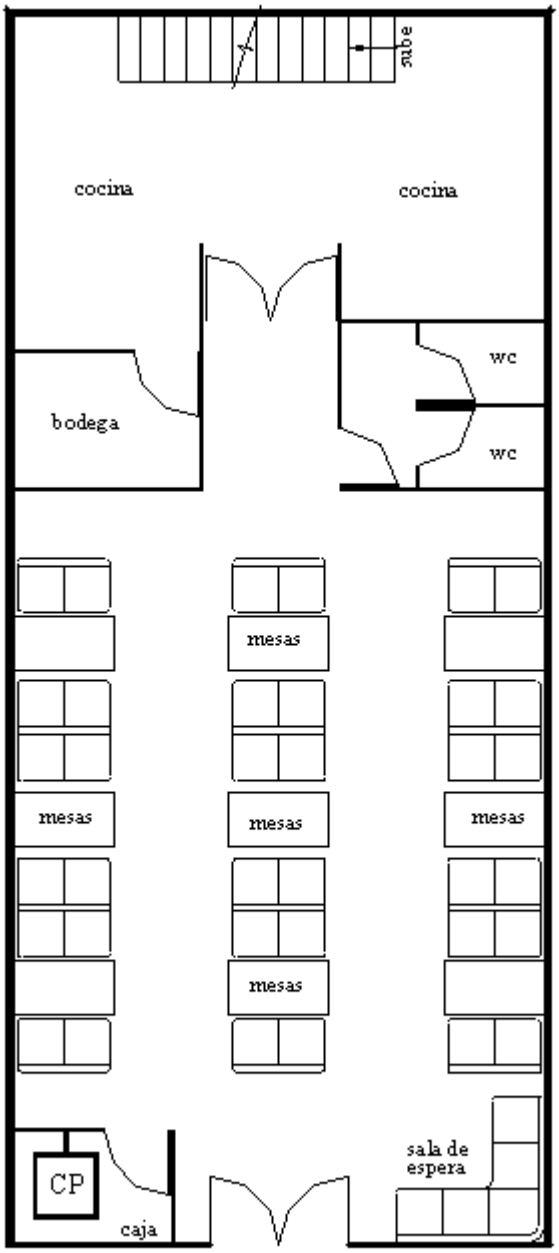
FACHADA



FACHADA

Plano 3.5. Fachada Edificios Secundarios Anexo B y C

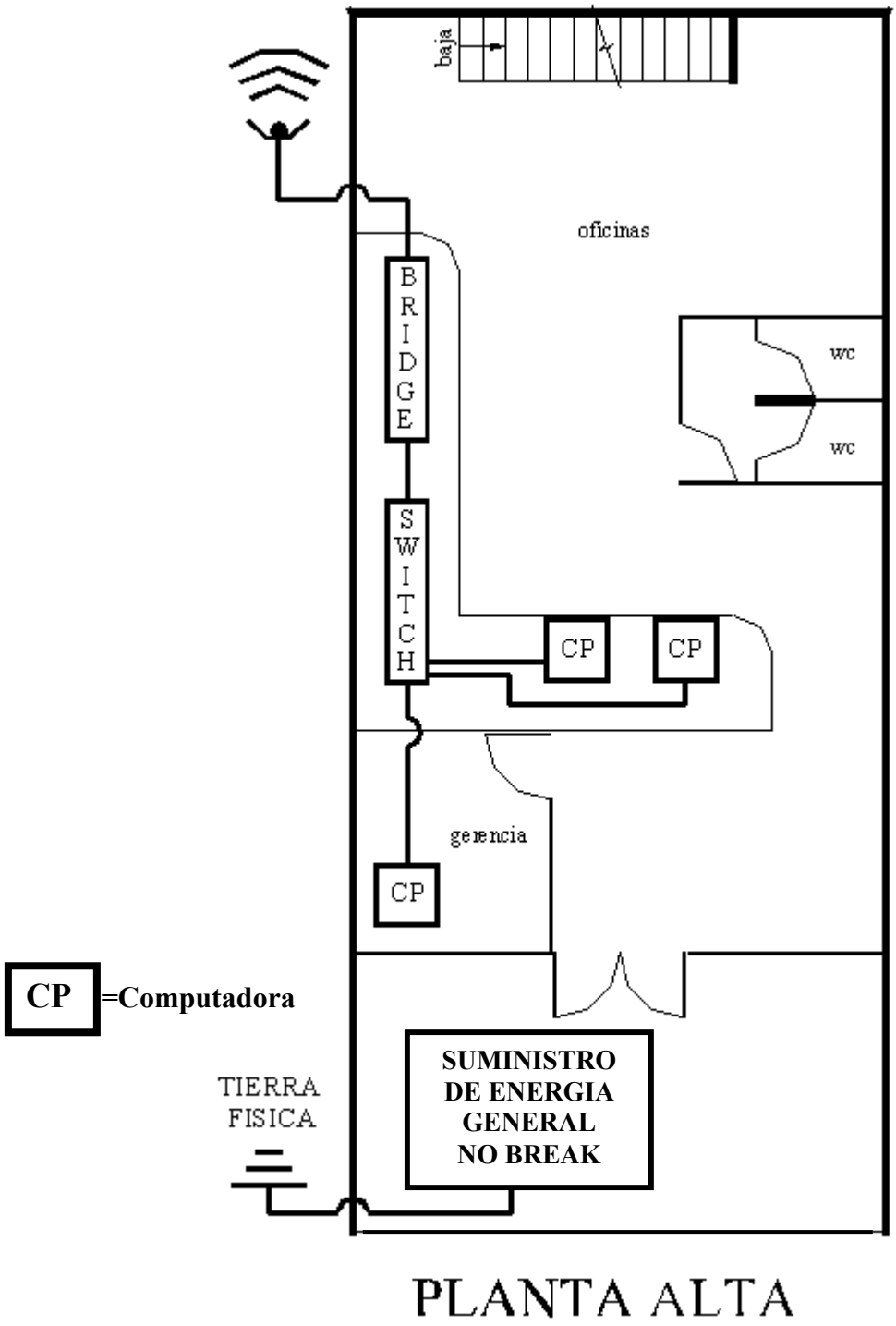
Estos dos edificios serán los dos anexos que mantendrán la conexión por medio de una antena con el edificio principal de este consorcio restaurantero y tendrán la tarea de mandar toda la información, ya sea datos generales así como la novedad de cada uno de las entidades a la Central A.



CP **=Computadora**

Plano 3.6. Planta Baja Edificio Secundario Anexo B y C

Al igual que el edificio principal ésta será la entrada del restaurante y mantendrá la misma estructura, solo que aquí por lo reducido de los edificios estará la bodega y el acceso al primer piso.



Plano 3.7. Planta Alta Edificio Anexo B y C

En esta parte del edificio estarán las oficinas y la estructura de la red inalámbrica la cual trasmitirá todo el proceso de administración a la Central A así como las incidencias que puedan suceder en el transcurso del mismo. Estos dos anexos solo tendrán los privilegios de

mandar y recibir información del edificio principal y no podrán comunicarse de un anexo a otro sin haber pasado por la Central A.

3.2. Recomendaciones de Instalación y Administración (Software y Hardware)

El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red y las recomendaciones es asegurar por medio de este mismo hardware y software el punto de acceso a la red de quienes puedan entrar desde el exterior y comprobar que no tengan autorización para usar nuestros servicios. Es más fácil decirlo que hacerlo, pero intentaremos definir unas líneas esenciales.

Una red inalámbrica es más difícil y compleja de asegurar frente a una red física, principalmente porque mientras una red física tiene unos determinados puntos de acceso o conexión, a una red inalámbrica se puede entrar desde cualquier lugar accesible en el rango cubierto por las antenas.

Independientemente de las dificultades inherentes al sistema, proteger apropiadamente nuestra red inalámbrica es la llave para salvaguardar nuestros sistemas de un problema serio de seguridad. Si desarrollamos una red inalámbrica insegura, podríamos obtener como resultado una pérdida de servicio o de uso de la red como una plataforma desde la que alguien pueda lanzar ataques a otras redes.

3.2.1. Instalación del hardware

Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento y abarcan un dispositivo completo, como un "switch", un "Access Point" o un "ruteador"; o solo una parte de los mismos, como una tarjeta de red inalámbrica, tarjeta procesadora, un módulo, etc. El proceso de instalación consiste de las siguientes etapas:

- Realizar un estudio previo para asegurar que la parte que será instalada es compatible con los componentes ya existentes.
- Definir la fecha de ejecución y hacer un estimado sobre el tiempo de duración de cada paso de la instalación.
- Notificar anticipadamente a los usuarios sobre algún cambio en la red.
- Generalmente, a toda instalación de hardware corresponde una instalación o configuración en la parte de software, entonces es necesario coordinar esta configuración.

- Generar un plan alterno por si la instalación provoca problemas de funcionalidad a la red.

- Realizar la instalación procurando cumplir con los límites temporales previamente establecidos.

- Documentar el cambio para futuras referencias.

- Cambie el SSID[1] (identificación de su red). La mayoría ha sido sorprendida ya que dejan el SSID de default del proveedor. Cambie su SSID y no con una opción obvia como el nombre de la compañía, dirección, división o nombre de productos.

- Cambie el password que viene por default en el punto de acceso o ruteador inalámbrico. Cualquier "hacker" digno de llamarse así, conoce los password por default y será los primeros que intente.

- Cambie la localización de los puntos de acceso. Piense en la localización de los puntos de acceso hacia el centro de su edificio en lugar de junto a las ventanas. Planifique su cobertura de radiación hasta las ventanas, no más allá de las ventanas.

3.2.2. Instalación y administración del software

Es la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además, de mantener un control sobre los programas que son creados para obtener información específica en los dispositivos.

Antes de realizar una instalación, se debe tomar en cuenta lo siguiente.

- Que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de software.

- Asegurar que no exista conflicto alguno, entre las versiones actuales y las que se pretenden instalar.

[1] SSID (Identificador de conjunto de servicios). Para que los dispositivos inalámbricos se puedan comunicar entre sí a través de una red inalámbrica, cada sistema debe estar configurado en el mismo canal y utilizar el mismo número SSID. Los números SSID proporcionan un modo de identificar a las computadoras que forman parte de la red inalámbrica.

En la Instalación del software se contemplan lo siguiente:

Instalación del Sistema Operativo de Red: en la máquina principal (servidor), en este caso el sistema operativo de la red será Windows 2000 Server, ya que nuestras aplicaciones funcionan con Windows y DOS, además los empleados estarán familiarizados con Windows, será más fácil para ellos operar la red. Además este sistema operativo soporta compartición de archivos y de impresoras, así como el protocolo de comunicación que se usará que será TCP /IP.

Instalación de Aplicaciones: la mayoría son programas de contabilidad como COI, NOI Y SAE en ASPEL para el manejo de entradas y salidas de dinero así como algún otro programa que se vaya a ocupar. Y sin falta los programas de diseño y Office Windows.

Configuración del Sistema Operativo de RED.

Para las configuraciones de los equipos con respecto a la red inalámbrica tomaremos como base algunos puntos que se deben emplear sus funciones y la administración que llevará:

Nombres de las máquinas en la red inalámbrica.
Los nombres que se pongan a las estaciones de trabajo y servidores son de forma arbitraria. En general se deberá nombrar a cada una de las máquinas para su distribución y organización los cuales llevarán nombres fáciles de recordar y deben estar relacionados con su función.

Funciones del equipo.
Si se desea contar con mayor grado posible de acceso a todos los recursos de la red se debe especificar qué función va a desempeñar cada máquina si va ser estación de trabajo o servidor y qué tipo de servidor ya sea dedicado o no dedicado. Si el número de servidores es muy numeroso se incrementan las funciones de mantenimiento de dichos servidores.

Funciones de cada servidor.
Agrupar todas las funciones posibles en un solo sistema de servidor es un error y el resultado general es una disminución en el rendimiento. En general, lo óptimo es tratar de distribuir el trabajo entre todos los servidores de tal forma que se pueda repartir la carga de trabajo de los servicios de impresión, base de datos y funciones de archivado.

Si un servidor, es un servidor no dedicado el rendimiento de la red disminuirá. Llamaremos servidor dedicado a la computadora que se dedicará, como su nombre lo indica, a mandar, distribuir y archivar toda la información únicamente en la entidad que tenga a cargo este servidor.

Como en realidad no son muchos equipos en cada restaurante, va existir un servidor de archivos en cada restaurante y los nombres son los siguientes los cuales van a hacer dedicados:

- Bisquet´s Históricos Arcos
- Bisquet´s Históricos Madero
- Bisquet´s Históricos Tacuba

Configuración de los servidores.

Una vez que se haya establecido la distribución y la configuración general de la red, se necesita efectuar una configuración detallada para cada servidor y ésta deberá cubrir:

- Configuración general de cada uno de los servidores, como su nombre, el tipo de equipo que es, qué capacidad tiene.
- Recursos del servidor es decir qué servicios va a otorgar, por ejemplo: administración de la red, servidor de bases de datos o servidor de impresión, es decir recursos compartidos de cada servidor.
- Usuarios del servidor qué usuarios van a poder entrar a dicho servidor y con qué privilegios cuenta.

3.2.3. Administración

Administración centralizada de la seguridad. Windows 2000 Server permite crear dominios y establecer relaciones de confianza, con el fin de centralizar las cuentas de usuario de la red y otro tipo de información de seguridad, facilitando el uso y la administración de la red. Con una administración centralizada de la seguridad, sólo es necesario administrar una cuenta por cada usuario. Dicha cuenta permite al usuario tener acceso a todos los recursos de la red.

Administración de las estaciones de trabajo de los usuarios. Los perfiles de usuario de Windows 2000 Server le permiten proporcionar mayor facilidad de uso a los usuarios y al mismo tiempo restringir sus actividades en las estaciones de trabajo. Si desean utilizar perfiles para aumentar la productividad de los usuarios, puede guardar en los servidores un perfil con la configuración y las preferencias de los usuarios, tales como las conexiones de red, los grupos de programas e incluso los colores de la pantalla. Este perfil se utilizará cada vez que el usuario inicie una sesión en cualquier computadora con Windows 2000 Server, de forma que el entorno definido por el usuario le siga de una estación de trabajo a otra. Si desea utilizar los perfiles de usuario para limitar las actividades de los usuarios, deberá agregar restricciones al perfil, como por ejemplo, impedir que el usuario cambie los grupos y los elementos de programas que usted haya definido, o inhabilitar parte de la interfaz de Windows 2000 Server cuando el usuario haya iniciado una sesión.

Administración de la Impresión en red. Windows 2000 Server incorpora una potente interfaz del Administrador de impresión que simplifica los procedimientos de instalación y administración de las impresoras que deben realizar los administradores, y que facilita las operaciones de examen y conexión de impresoras que deben realizar los usuarios. Los usuarios de las computadoras que se conecten a impresoras compartidas por computadoras en las que se esté ejecutando Windows 2000 Server no necesitarán disponer de controladores de impresora instalados en la propia estación de trabajo al igual que es plenamente compatible con impresoras que disponen de interfaz de red (como algunas marcas de impresoras por ejemplo: Hewlett-Packard, Epson, etc.) que cuentan con una tarjeta adaptadora de red incorporada y que se conectan directamente al cable de la red y no a un puerto serie o paralelo del servidor.

Monitorización del rendimiento. Windows 2000 Server incluye también una sofisticada aplicación que permite monitorizar el rendimiento. Puede utilizar esta herramienta para observar, representar gráficamente y registrar cientos de datos estadísticos acerca de tipos específicos de rendimiento, agrupados en categorías generales tales como tráfico entre servidores de la red, rendimiento de los discos, uso de los procesadores y estadísticas de los servidores y las estaciones de trabajo. El Monitor de sistema le permite supervisar simultáneamente el rendimiento de un gran número de computadoras remotas, de forma que pueda controlar y comparar simultáneamente el rendimiento y el uso de un gran número de servidores.

Seguimiento de la actividad de la red. Windows 2000 Server proporciona numerosas herramientas para realizar el seguimiento de la actividad y el uso de la red. Puede observar los servidores y examinar qué recursos están compartiendo, ver qué usuarios están conectados a un servidor de la red y observar qué archivos tienen abiertos, registrar y ver las anotaciones de auditoría de seguridad, mantener registros de error exhaustivos y especificar las alertas que se deben enviar a los administradores en caso de que se produzcan determinados sucesos. Si la red inalámbrica utiliza el protocolo TCP/IP, podrá emplear también la utilidad de administración SNMP[2], suministrada con Windows 2000 Server.

Administración Remota. Todas las funciones administrativas de la red, incluyendo la administración de servidores, la administración de seguridad, la administración de impresoras y la monitorización del rendimiento, pueden realizarse de forma remota. Es posible utilizar una computadora de la red inalámbrica para monitorizar las actividades de cualquier servidor en la misma.

[2] SNMP (Simple Network Management Protocol, Protocolo Simple de Administración de Red). Protocolo que se utiliza para administrar y monitorear dispositivos conectados a una red

3.3. SEGURIDAD EN REDES INALÁMBRICAS.

Las redes inalámbricas presentan nuevos desafíos debido a que los datos viajan por el aire, por ondas de radio. Otros retos se deben a las posibilidades únicas de las redes inalámbricas. Con la libertad de movimiento que se obtiene al eliminar las ataduras (cables), los usuarios pueden desplazarse de sala en sala de edificio en edificio, de ciudad en ciudad, etc., con las expectativas de una conectividad in-interrumpida en todo momento.

Un **punto de acceso**, también conocido como una estación base, es el servidor que conecta a los clientes con la red interna. Estos puntos normalmente actúan como puentes para los clientes. Normalmente las estaciones disponen de una dirección IP y de un agente SNMP que permite su configuración de forma remota. El costeo de un punto de acceso o de tarjetas para equipos clientes (PDAs, portátiles, PC´s,...) se ha reducido mucho en los últimos meses. Este costeo tan económico de los equipos proporciona a los atacantes un acceso fácil a las redes inalámbricas lo que aumenta los riesgos de ataques, que pueden alcanzar tanto a empresas como a particulares que utilicen este tipo de redes.

Actualmente existen muchas empresas sin infraestructura inalámbrica que permiten accesos remotos a sus empleados por medio de medios tradicionales. En ese caso, no hay que olvidar la posibilidad de que esos empleados dispongan de redes inalámbricas en casa con el riesgo que eso supone, al convertirse las redes locales de los empleados en casa en puntos de acceso autorizados pero desconocidos en muchas ocasiones. El hecho de que muchos establecimientos públicos empiecen a ofrecer acceso a Internet a sus usuarios con portátiles por medio de tecnología inalámbrica provocará un gran riesgo de seguridad para los usuarios que no estén bien protegidos como por ejemplo tener antivirus actualizados y las demás protecciones que se comentarán en este capítulo más adelante.

3.1.1. Riesgos de seguridad en las redes inalámbricas actuales

La colocación apropiada de la antena dentro de un edificio puede ayudar a reducir los riesgos de intercepción debido a la necesidad de que los intrusos tengan que estar dentro del radio de acción de la señal.

A pesar de que los ataques a sistemas 802.11b, y otros sistemas inalámbricos, se incrementarán a lo largo del tiempo con técnicas más sofisticadas, las actuales se pueden clasificar entre estas siete categorías:

- Ataques por penetración.
- Monitorización e intercepción no autorizada del tráfico inalámbrico.
- Problemas de configuración.
- Denegación del servicio (jamming).
- Ataques de cliente a cliente.
- Ataques por fuerza bruta contra las claves de los puntos de acceso.
- Ataques de cifrado.

Ataques por penetración.

Estos ataques se basan en introducir dispositivos inalámbricos dentro de una red o en crear una nueva red que no pase por los procesos de seguridad.

Cliente no autorizado. El atacante conecta un cliente inalámbrico, normalmente un portátil, a un punto de acceso sin autorización. Los puntos de acceso se pueden configurar para que soliciten una clave antes de permitir el acceso. Pero, si no es así el atacante se puede conectar a la red solo con activar el dispositivo inalámbrico. Otro peligro es utilizar una clave de acceso única para todos los clientes que se conectan a un punto de acceso, requiriendo, además, la notificación de ésta a todos los clientes cada vez que es actualizada.

Punto de acceso no autorizado. Una organización puede no estar informada de nuevos puntos de acceso que hayan creado sus empleados. Esta desinformación puede llevarnos a ataques como el descrito anteriormente, con clientes no autorizados que entran al sistema por medio de puntos de acceso no autorizados. Las empresas deben establecer políticas de seguridad para asegurar la configuración de los puntos de acceso y disponer de procesos que busquen dispositivos no autorizados en la red.

Monitorización e intercepción no autorizada del tráfico inalámbrico.

Como en las redes de cable, en las redes inalámbricas es posible interceptar y monitorizar el tráfico. Para poder realizar esta tarea el atacante debe encontrarse en el rango del punto de acceso. La ventaja de la red inalámbrica sobre la red de cables es que esta última necesita de la colocación de un agente de monitorización dentro de la red mientras que para la inalámbrica sólo se necesita acceso al flujo de datos.

Hay dos consideraciones importantes sobre el rango de acceso en las redes 802.11:

- Primero, las antenas direccionales pueden conseguir un gran aumento del rango lo que permite ampliar las posibilidades de transmisión y recepción de los dispositivos, lo que también aumenta los riesgos de seguridad.
- Segundo, los puntos de acceso transmiten su señal en un patrón circular, lo que significa que la señal se puede extender más allá de los límites físicos en los que se quiere utilizar la red. Esta señal puede ser interceptada fuera del edificio o en otras plantas del mismo para los que no fue pensada. Por lo tanto, la colocación de la antena es un punto muy importante cuando hablamos de riesgos de seguridad.

Análisis de paquetes. Un atacante especializado puede capturar tráfico inalámbrico de la misma forma que lo haría con redes de cable. Muchas herramientas pueden capturar la primera parte de la conexión de sesión, donde normalmente viajan el nombre de usuario y la clave de acceso. Entonces un intruso podría pasarse por un usuario legítimo utilizando la información obtenida para entrar a la sesión del usuario y ejecutar comandos no autorizados.

Monitorización por broadcast. Si un punto de acceso está conectado a un "*hub"* en vez de a un "*switch",* cualquier dato que pase por el "hub" puede ser enviado potencialmente a la red inalámbrica. Por este motivo, cualquier información, aún cuando ésta no esté destinada a la red inalámbrica, podría ser monitorizada por un atacante.

Intercepción de tráfico por punto de acceso clónico. Un atacante engaña a los clientes de redes inalámbricas para que éstos se conecten a la red del atacante por medio de la colocación de un punto de acceso clónico no autorizado que emite una señal más potente que la original. Los usuarios se conectan al servidor sustituto proporcionando nombres de usuarios y claves de acceso, así como datos importantes.

Problemas de configuración.

Muchos de los puntos de acceso se entregan con configuraciones inseguras para facilitar su uso y conseguir una instalación rápida. Al menos que los administradores de estos equipos sean conscientes de los riesgos de seguridad y configuren de forma apropiada estos dispositivos, se mantendrán puntos de acceso con un alto riesgo de seguridad que puede provocar ataques.

Server Set ID (SSID). Una máquina que quiera conectarse a una red inalámbrica tiene que proporcionar su número de Identificador de Servicio (SSID) antes de permitirle conectarse a la red. Este identificador es una línea de texto que identifica a cada red, pero es la misma línea para todos los usuarios de esa red. El SSID no ofrece ningún beneficio de seguridad y puede conocerse fácilmente conectado un "sniffer" y visualizando el texto libremente en cada paquete de datos. Lo único que hace SSID es restringir el tráfico a una sola red.

También es posible fijar una lista de autorización de acceso basada en la dirección MAC[3] del usuario. Sin embargo, tampoco aquí hay mucha seguridad, ya que la dirección MAC puede ser fácilmente falseada. Los puntos de acceso se venden con SSIDs con valores por defecto. Si éstos no son cambiados podemos comprometer la seguridad de la red. Ya que el SSID viaja por la red como texto claro se permite que sea capturado por monitores de tráfico que puedan existir en la red. WEP, el mecanismo de cifrado de 802.11 solo cifra los paquetes de datos permitiendo que el SSID pueda ser obtenido fácilmente por medio de monitorización.

Algunos puntos de acceso pueden trabajar en modo seguro lo que obliga a tener el mismo SSID en el cliente y en el punto de acceso. La mayoría de las estaciones base están configuradas con SSID que funciona como una clave compartida por todos los clientes. Un atacante puede adivinar el SSID de un punto de acceso por medio de un diccionario aplicado por la fuerza bruta. Muchas empresas utilizan nombres sencillos de recordar como SSID lo que simplifica los ataques de seguridad.

[3] MAC (Media Access Control, Controlador de Acceso a Medios). El acrónimo MAC se suele utilizar para describir el uso de direcciones MAC.

Una vez que el intruso obtiene el SSID, puede entrar a la red por medio de ese punto de acceso. El SSID también puede ser obtenido por medio de dispositivos clientes que hayan sido comprometidos. Una vez obtenido el SSID se permite el acceso hasta que éste sea cambiado. Si hay muchos clientes puede ser muy problemático el cambio del SSID de forma periódica ya que todos los clientes y puntos de acceso tienen que ser actualizados con el SSID nuevo.

Muchos puntos de acceso tienen activado por defecto el broadcasting del SSID. Éste puede ser desactivado pero no evita que los atacantes puedan obtener el SSID cuando los clientes lo envíen al punto de acceso para asociarse a la red.

Wired Equivalent Privacy (WEP). Resulta evidente a todas luces que las comunicaciones inalámbricas ofrecen un punto de vulnerabilidad en la transmisión de datos, puesto que las emisiones difícilmente pueden acotarse a la zona de cobertura, sino que habitualmente suelen alcanzar puntos fuera del área de transmisión deseada. Para evitar que otros receptores ajenos a la red corporativa y a los intereses de la empresa puedan hacer un uso indebido de la información que viaje por el aire se ha adoptado un sofisticado mecanismo de control de acceso al medio (DSSS), lo cual evita en gran medida las escuchas indiscretas. No obstante, este sistema no es suficiente, por lo que opcionalmente se puede realizar un proceso de cifrado de los datos que se transmiten por la red inalámbrica.

A la hora de proteger la información que viaja por el espacio mediante sistemas cifrado se puede hacer uso de las técnicas WEP-40 y WEP-128. Estos dos sistemas son funciones opcionales de la especificación IEEE 802.11 que proporcionan una confidencialidad de datos equivalente a la de una LAN cableada sin cifrar. Es decir, el sistema WEP hace que el enlace LAN inalámbrico en una red sea tan seguro como el enlace con cable.

Como se especifica en el estándar, WEP (Wired Equivalent Privacy) utiliza el algoritmo RC4 con una clave de 40 bits para WEP-40 o una clave de 128 bits para WEP-128. Cuando la función WEP está activada, a cada estación (cliente o punto de acceso) se le asigna una clave común. Esta clave desordena los datos y se mezcla entre la información antes de ser transmitida, de tal modo que si una estación recibe un paquete que no está mezclado con la clave correcta, la estación descartará el paquete.

La instalación de esta función es opcional, aunque sumamente sencilla de poner en marcha. Simplemente habrá que seleccionar el tipo de encriptación WEP que se desea implementar, 40 ó 128 bits, y a continuación elegir la clave que se utilizará. Obviamente, si la función WEP está activada en uno o más puntos de acceso, todos los dispositivos inalámbricos de la red deberán tener el mismo código WEP, que se establece fácilmente mediante las utilidades de software suministradas.

No obstante, existe la posibilidad de establecer una comunicación con células combinadas. Una célula combinada es una red de radio en la que algunos dispositivos utilizan WEP y otros no. Esta opción es posible mediante la simple activación del parámetro "Allow Association To Mixed Cells (Permitir asociación de redes mixtas)".

802.11 requiere que se mantenga una lista con las direcciones MAC de los dispositivos autorizados a conectarse a la red inalámbrica. En los procesos de conexión iniciales con las estaciones base se comprueban las direcciones MAC contra la lista permitiendo el acceso si

las direcciones están autorizadas. El filtrado de direcciones MAC nunca ha formado parte del estándar pero ha sido muy utilizado para asegurar la conexión segura de dispositivos.

Pero, evidentemente, no es una solución acertada. La autorización se realiza contra dispositivos y no contra usuarios por lo que el filtrado no nos asegura de su utilización maliciosa pudiendo provocar grandes destrozos con software apropiado para los ataques. Además, un usuario con suficientes privilegios sobre el sistema operativo puede modificar las direcciones para enmascarar un equipo.

WEP está basado en el algoritmo RC4 del cual se descubrieron grandes debilidades. El algoritmo de planificación de claves del RC4 es débil ya que se puede diseñar un ataque escuchando de forma pasiva durante un periodo de tiempo relativamente corto, unas horas, de forma que se recojan un número suficiente de paquetes cifrados con claves débiles para, a partir de ellos, obtener la clave WEP secreta. Actualmente existen multitud de programas *open-source* que implementan este tipo de ataque. Uno de los más conocidos, el AirSnort, es capaz de obtener la clave WEP secreta en solo unos segundos después de haber obtenido suficientes tramas débilmente cifradas.

Para proporcionar un mecanismo mejor para el control de acceso y la seguridad, es necesario incluir un protocolo de administración de claves en la especificación. Para hacer frente a este problema se creó específicamente el estándar 802.1x. A pesar de que 802.1x es imperfecto, es una solución de autenticación de usuario mucho más completa que WEP y en estos momentos los dispositivos 802.1x están empezando a aparecer.

Seguridad – 802.1X. Para ofrecer una mayor seguridad de la que proporciona WEP, el equipo de conexiones de red de Windows XP trabajó con IEEE, distribuidores de red y otros colaboradores para definir IEEE 802.1X.

802.1X es un borrador de estándar para el control de acceso a redes basado en puerto que se utiliza para proporcionar acceso autenticado para las redes Ethernet. Este control de acceso a red basado en puerto utiliza las características físicas de la infraestructura LAN conmutada para autenticar los dispositivos conectados a un puerto LAN. Si el proceso de autenticación no se realiza correctamente, se puede impedir el acceso al puerto. Aunque este estándar se ha diseñado para redes Ethernet con cable, se puede aplicar a las redes LAN inalámbricas 802.11.

Concretamente, en el caso de las conexiones inalámbricas, el punto de acceso actúa como autenticador para el acceso a la red y utiliza un servidor del Servicio de Usuario de Acceso Telefónico de Autenticación Remota (RADIUS) para autenticar las credenciales del cliente. La comunicación es posible a través de un “puerto no controlado” lógico o canal en el punto de acceso con el fin de validar las credenciales y obtener claves para obtener acceso a la red a través de un “puerto controlado” lógico. Las claves de que dispone el punto de acceso y el cliente como resultado de este intercambio permiten cifrar los datos del cliente y que el punto de acceso lo identifique. De este modo, se ha agregado un protocolo de administración de claves a la seguridad de 802.11.

Los pasos siguientes describen el planteamiento genérico que se utilizaría para autenticar el equipo de un usuario de modo que obtenga acceso inalámbrico a la red:

- Sin una clave de autenticación válida, el punto de acceso prohíbe el paso de todo el flujo de tráfico. Cuando una estación inalámbrica entra en el alcance del punto de acceso, éste envía un desafío a la estación.
- Cuando la estación recibe el desafío, responde con su identidad. El punto de acceso reenvía la identidad de la estación a un servidor RADIUS que realiza los servicios de autenticación.

Posteriormente, el servidor RADIUS solicita las credenciales de la estación, especificando el tipo de credenciales necesarias para confirmar su identidad. La estación envía sus credenciales al servidor RADIUS (a través del "puerto no controlado" del punto de acceso). El servidor RADIUS valida las credenciales de la estación (da por hecho su validez) y transmite una clave de autenticación al punto de acceso. La clave de autenticación se cifra de modo que sólo el punto de acceso pueda interpretarla.

El punto de acceso utiliza la clave de autenticación para transmitir de manera segura las claves correctas a la estación, incluida una clave de sesión de uní-difusión para esa sesión y una clave de sesión global para las multi-difusiones.

Para mantener un nivel de seguridad, se puede pedir a la estación que vuelva a autenticarse periódicamente.

Este planteamiento de 802.1X saca partido del uso extendido y creciente de RADIUS para la autenticación. Un servidor RADIUS puede realizar consultas en una base de datos de autenticación local si ello es adecuado para el escenario. O bien, la solicitud puede transmitirse a otro servidor para su validación. Cuando RADIUS decide que se puede autorizar el equipo en esta red, vuelve a enviar el mensaje al punto de acceso y éste permite que el tráfico de datos fluya hacia la misma.

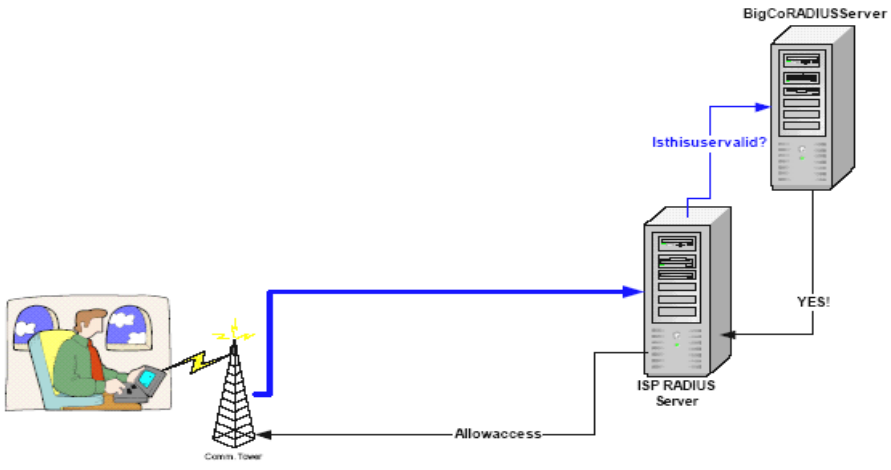


Figura 3.2. Ejemplo de escenario de acceso público

Para ofrecer este nivel de seguridad, Microsoft incluye una implementación del cliente 802.1X en Windows XP y mejora el servidor RADIUS de Windows, el servidor de autenticación de Internet (IAS), para admitir la autenticación de dispositivos inalámbricos. Microsoft también ha trabajado con muchos distribuidores de dispositivos 802.11 para que admitiesen estos mecanismos en sus controladores NIC y en el software de punto de acceso. Actualmente, muchos de los principales distribuidores incluyen o pronto incluirán la compatibilidad con 802.1x en sus dispositivos.

Configuración de interfaces. Muchos puntos de acceso ejecutan agentes SNMP como mecanismo de gestión. Algunos fabricantes utilizan SNMP v1 lo que significa que toda la información de gestión viaja descifrada. Otros permiten la lectura de las claves WEP, a pesar de que éstas deben permanecer en secreto. Otros utilizan Telnet como mecanismo para la ejecución de comandos sin utilizar OpenSSH. Algunos disponen de interfaz WEB por medio de http y no de http´s que permite el envío de la información de forma cifrada.

SNMP. Un problema asociado a los agentes SNMP es la configuración errónea de las "*Community words"* provocando que un intruso pueda leer o escribir datos peligrosos en el punto de acceso. Si los agentes están activados en los dispositivos clientes éstos corren el mismo peligro. Por defecto, muchos puntos de acceso utilizan palabras como "public" o "com" como *Community words* por defecto, provocando así un fácil acceso a la información. El diseño de una red inalámbrica segura debe considerar los mecanismos tan inseguros que utilizan las herramientas de administración SNMP para conseguir que el tráfico de la red vaya cifrado tanto como sea posible.

Riesgo de seguridad en el lado cliente. Los clientes conectados a los puntos de acceso almacenan información sensible utilizada en el proceso de autenticación y comunicación. Esta información puede ser comprometida si el cliente no está configurado de forma apropiada. Algunos fabricantes, como Cisco, Lucent/Cabletron y 3Com, almacenan los SSID en el registro de Windows y las claves WEP en el firmware, donde es más difícil de acceder a ellas, o en el propio registro de Windows, pero utilizando un algoritmo de cifrado, o no, como es el caso de 3Com. Windows XP tiene una configuración para 802.11 que permite la visualización de los SSIDs disponibles. Todas estas configuraciones hacen bastante fácil el acceso a datos de seguridad muy comprometidos.

Instalación. Por defecto todos los aparatos vienen configurados de la forma más sencilla para permitir a los usuarios una instalación rápida y sin problemas. Y normalmente, esto supone que las configuraciones de seguridad estén en unos modos muy inseguros.

Denegación del Servicio (Jamming).

El problema más grande con la tecnología inalámbrica es que está sujeta a interferencia, haciéndola un candidato ideal a los ataques de Denegación del Servicio. Los ataques de Denegación del Servicio pueden ser intencionales, como cuando alguien deliberadamente satura la frecuencia, o no-intencionales, generados cuando alguien hace palomitas en el microondas. La exposición a los ataques para la Denegación de Servicio se evalúa, normalmente, como el coste que supone la parada del negocio durante el periodo de tiempo en el que éste se encuentra deshabilitado. Después de todo, no se roban ni se modifican los

datos, simplemente queda inaccesible por un rato. No representa esto, un gran problema si se le niega el acceso a su correo o las cotizaciones de bolsa. Pero sí es un gran problema si efectúa movimientos de acciones sobre una red inalámbrica. En una red inalámbrica, no hay buenas soluciones para los ataques de Denegación de Servicio.

Interferencias.

Los ataques de negación de servicio son bastante populares en las redes cableadas tradicionales. El mismo principio se puede aplicar a las redes inalámbricas, donde es posible bloquear tráfico legítimo saturando las frecuencias disponibles con tráfico falso, provocando que el tráfico legítimo no pueda progresar.

Un atacante con el equipamiento y las herramientas adecuadas puede inundar fácilmente la frecuencia de trabajo de las redes inalámbricas (2.4 GHz para redes de tipo 802.11b) de tal manera que la relación señal ruido se reduce de tal manera que la red deja de funcionar.

Éste puede ser un riesgo incluso sin tener intenciones maliciosas, ya que existen diferentes tecnologías que utilizan las mismas frecuencias y pueden provocar bloqueos no intencionados. Teléfonos inalámbricos basados en tecnología DECT, transmisores para monitorizar bebes como los wacky talks o incluso otros dispositivos Bluetooth que operen en las proximidades de un punto de acceso (AP) pueden causar interferencias que paralicen la red.

3.1.2. Ataques cliente – cliente.

Dos clientes inalámbricos pueden comunicarse directamente sin utilizar un punto de acceso como intermediario. Por este motivo, deben protegerse de los demás clientes. Por ejemplo, si un cliente emplea algún servicio TCP/IP, ya sea un servidor Web o sistema para compartir ficheros, un atacante puede intentar explotar las vulnerabilidades o errores en la configuración desde otro cliente.

Otro tipo de ataque se puede producir si un cliente inunda con tráfico falso a otro cliente, creando un ataque de negación de servicio. Un atacante, o incluso un empleado de forma no intencionada, puede configurar su cliente con una dirección IP o MAC de otro cliente. Al detectar una dirección duplicada la red sufre cortes de servicio.

Por último, cabe mencionar las cada vez más sofisticadas generaciones de virus que se han convertido en programas de ataque multivectoriales que son capaces de propagarse a través de cualquier interfaz TCP/IP, incluyendo las interfaces inalámbricas. Si un ordenador de la red inalámbrica se infecta con uno de estos virus híbridos, es posible que consiga propagarse a otros clientes inalámbricos o incluso a otros ordenadores que estén situados por detrás de la red inalámbrica.

War driving.

Para comprender el significado del término “war driving” hay que remontarse algunos años cuando se acuñó el término “war dialing”: se trataba de una técnica en la cual se empleaba un módem conectado a una computadora que marcaba sistemáticamente todos los números de teléfono y anotaba aquellos en los que encontraba un módem. De esta manera aparece el término war driving: se trata de descubrir puntos de acceso mediante una tarjeta inalámbrica y una laptop portátil mientras conducimos por la ciudad. Se suele añadir un receptor GPS Garmin (www.garmin.com) para marcar exactamente las coordenadas del punto de acceso y así poder regresar a inspeccionar el punto de acceso con más detenimiento. El problema aparece cuando un atacante divulga la localización de estos puntos de acceso en Internet. Si se publica la información de un punto de acceso de una compañía en Internet, automáticamente se convierte en un potencial objetivo de atacantes y su riesgo aumenta. Uno de los lugares más populares para encontrar localizaciones de puntos es NetStumbler que incluye un mapa visual y una herramienta de consulta a la base de datos de puntos de acceso.

Redes parasitarias.

Recientemente están apareciendo iniciativas para desplegar zonas gratuitas de acceso inalámbrico en las zonas metropolitanas. Este movimiento, llamado "red parasitaria" por algunos o simplemente "red metropolitana gratuita de acceso inalámbrico" ya se ha instalado en multitud de ciudades: New-York, San Francisco, Londres. etc. Estas redes parasitarias permiten un acceso anónimo a atacantes e intrusos y además hace virtualmente imposible su localización y rastreo.

3.1.3. Herramientas para disminuir el riesgo en redes inalámbricas

Hay muchas opciones disponibles que una organización puede emplear hoy en día para proporcionar cierta seguridad alrededor de las redes inalámbricas que despliegue. Lo principal es definir un conjunto de políticas que especifiquen lo que está y lo que no está permitido con este tipo de tecnología. Desde un punto de vista de seguridad, las estaciones base o puntos de acceso se deben evaluar y establecer si se deben tratar como un dispositivo en el que no se confía y por lo tanto es necesario poner barreras adicionales antes de que el cliente acceda a la red interna. El diseño de la arquitectura de red puede incluir cortafuegos (firewall), redes privadas virtuales (Virtual Private Network, VPN), sistemas de detección de intrusos (Intruder Detection Systems, IDS) o autenticación entre el punto de acceso y la red interna.

La política de seguridad en la red inalámbrica debe hacer especial hincapié en los parámetros de configuración de los puntos de acceso. Debe cubrir aspectos de seguridad como el SSID, configuración SNMP, encriptación y claves WEP. Puede ser muy interesante desactivar los avisos por difusión (broadcast pings) del punto de acceso y así hacerlo invisible a herramientas de detección como NetStumbler.

Una alternativa al uso de WEP como mecanismo de seguridad del punto de acceso puede ser el estándar 802.1X. De hecho, Windows XP y muchos fabricantes están incorporando este estándar a sus puntos de acceso. El estándar 802.1x incorpora en su especificación un protocolo de gestión de claves que proporciona un mecanismo eficaz para generar claves y cambiarlas automáticamente a intervalos programados. Sin embargo, ya se han descubierto debilidades y pone de relieve la necesidad de una buena infraestructura de redes privadas virtuales a pesar de este estándar.

Otra actividad recomendable es la búsqueda de puntos de acceso desconocidos o infiltrados. Esto se puede hacer simplemente mediante una búsqueda de agentes SNMP ya que las estaciones base suelen incorporar este protocolo, para ello basta con lanzar una consulta a través de SNMP y analizar en detalle todos los dispositivos que respondan al parámetro *host id* con la cadena 802.11. Otra manera de localizar estaciones base intrusas es mediante búsquedas sistematizadas de servidores WEB o Telnet, otro de los mecanismos de configuración incorporada en este tipo de dispositivos. Adicionalmente, se pueden utilizar atributos únicos TCP/IP que conforman una huella única y así tratar de identificar dispositivos como estaciones base. La mayoría de implementación TCP/IP poseen un conjunto único de características y muchas herramientas utilizan estas diferencias para determinar el tipo de sistema operativo: ese mismo concepto se puede aplicar a las estaciones base.

Por último, es posible configurar una "sniffer[4]" de banda 2.4 GHz para capturar y analizar todo el tráfico 802.11 y así determinar si existen estaciones base infiltradas. El análisis de los paquetes revelará la dirección IP y así se podrá determinar en que red se encuentra la estación base. El inconveniente de este método es que en una zona densamente poblada de zonas inalámbricas distintas, es posible capturar más tráfico del deseado, haciendo más complicado el análisis.

No hay que olvidar que un punto muy importante es la configuración de la estación base. Debe hacerse una auditoria de seguridad para determinar si las contraseñas y nombre de la comunidad están aún con los valores por defecto o se pueden adivinar fácilmente y, por supuesto, si se han activado modos de seguridad tales como encriptación.

Proveedores de soluciones de seguridad.

En este apartado vamos a clasificar por una parte soluciones comerciales y por otra parte mencionaremos herramientas de análisis.

BlueSocket: ofrece una familia de pasarelas inalámbricas que proporcionan una solución escalable a los problemas de seguridad, calidad de servicio y aspectos de gestión relacionados con el despliegue de redes inalámbricas.

Ecutel: su enfoque se basa en una mejora de las redes VPN, en las que la conexión se mantiene al pasar de una red inalámbrica a otra e incluso de una red física a una

[4] Sniffer: Es un programa que monitoriza los paquetes de datos que circulan por una red.

inalámbrica. La seguridad está garantizada al utilizar túneles VPN y como valor añadido aporta la movilidad llevada al extremo.

Netmotion Wireless: es una solución parecida a la anterior; se basa en utilizar túneles VPN para evitar que el tráfico capturado se pueda desencriptar y además impide que clientes no autorizados se introduzcan en la VPN.

Airsnort: es una herramienta para la recuperación de las claves de encriptación. Funciona monitorizando pasivamente las transmisiones y extrayendo la clave cuando se han recolectado suficientes paquetes. Airsnort funciona para encriptaciones de 40 y 128 bits.

Wepcrack: es una herramienta que emplea las últimas debilidades descubiertas del algoritmo RC4 para obtener las claves de encriptación del protocolo WEP.

Network Stumbler: se trata de una herramienta de detección de redes inalámbricas. Permanece a la escucha y cada segundo hace un barrido para detectar redes nuevas. Es capaz de extraer el SSID del punto de acceso, su dirección MAC, la mejor relación señal ruido captado y la hora exacta de descubrimiento. Si se añade un receptor GPS es capaz de almacenar también la longitud y latitud exacta del punto de acceso. Lo verdaderamente sorprendente es que Network Stumbler no trabaja en modo promiscuo, sino que se limita a escuchar los avisos por difusión (broadcast pings). Una medida de protección eficaz contra esta herramienta es precisamente desactivar los broadcast pings.

3.1.4. Recomendaciones para mejorar la seguridad de redes inalámbricas

Hay muchas cosas que se pueden hacer para mejorar la seguridad de las redes. En este punto pretendemos reflejar algunas buenas prácticas que pueden ayudar a conseguir redes inalámbricas más seguras.

1) Coloque el punto de acceso en el lugar correcto. Piense en la localización de los puntos de acceso hacia el centro de su edificio, en lugar de junto a las ventanas. Planifique su cobertura de radiación hasta las ventanas, no más allá de las ventanas.

2) Defina su alcance. Los administradores de redes deben analizar su sitio periódicamente utilizando herramientas como NetSumbler para ver cualquier punto de red levantado. Las tarjetas inalámbricas ya son económicas, por lo que se incrementa la posibilidad de que un exempleado tome un par de NIC y puntos de accesos y se conecte a la red de la compañía.

3) Proteja los equipos instalados en el exterior. En el caso de la utilización de equipos de conexión inalámbrica a distancia es muy frecuente ubicar los “bridges” o sus antenas en las azoteas, por lo cual debemos de verificar que se encuentren en un lugar adecuado. Todos los equipos electrónicos deben permanecer en lugares frescos y secos protegidos de la intemperie. En el caso de las antenas, éstas deben instalarse en un punto en el cual no resulten estorbosas o peligrosas para las

personas del inmueble; deben asegurarse correctamente anticipando la acción del viento contra ellas. Si es necesario, debe instalarse un pararrayos para prevenir la posibilidad de que durante una tormenta eléctrica un rayo pueda caer en los equipos con las consecuencias tan peligrosas que esto implica.

4) Limite las conexiones. Muchos puntos de acceso permiten controlar accesos basados en direcciones MAC del NIC para conectarse. Si la dirección MAC del NIC no está en la tabla de puntos de accesos, no se le permitirá la entrada. La utilización de listas de control de acceso ACLs (Access Control Lists) basadas en direcciones MAC, otorgará acceso únicamente a los dispositivos que estén registrados en la red. Aunque los datos pueden ser falsificados (spoofed), la filtración de direcciones MAC funciona como otro candado en su puerta principal: mientras más obstáculos ponga, más factible será que los "hackers" se vayan a intentar entrar en organizaciones menos seguras.

5) Administre la identificación de su red inalámbrica. Todas las WLANs vienen con un identificador de servicio SSID (Service Set Identifier) o nombre de red programado. Cámbielo de inmediato con un nombre alfanumérico ya que cada casa comercial preconfigura el suyo en sus dispositivos, por ello es muy fácil descubrirlo. Debemos cambiarlo por uno lo suficientemente grande y difícil como para que nadie lo adivine. Así mismo debemos modificar a la baja la frecuencia de broadcast del SSID, deteniendo su difusión de ser posible. Si su organización puede absorber la tarea administrativa, cambie regularmente este SSID y no cometa el error equivalente a caminar con el nombre de su red escrito en su frente, desactive la función de anuncio automático del SSID.

6) Cambie el password que viene por "default" en el punto de acceso o ruteador inalámbrico.

7) La WEP es un excelente protocolo de seguridad. La WEP (Wired Equivalent Privacy) es el protocolo de seguridad inalámbrica estándar 802.11b. Está diseñada para ofrecer protección similar a la de redes por cables, a través de la encriptación de datos mientras transmite información. En pocas palabras: Póngalo en función e inmediatamente cambie la clave WEP que viene programada. Lo ideal es programar el sistema para que genere automáticamente las claves WEP cuando algún usuario ingrese, haciendo que el acceso inalámbrico a los datos sea un blanco movedizo para los "hackers". Las claves WEP basadas en sesiones y en usuarios ofrecen la mejor protección y añaden un nivel adicional de prevención. Debemos seleccionar una clave de cifrado para el WEP lo suficientemente difícil como para que nadie sea capaz de adivinarla. No debemos usar fechas de cumpleaños ni números de teléfono, o bien hacerlo cambiando (por ejemplo) los ceros por o's, etc. Cambie las claves periódicamente.

8) Pero el protocolo WEP no es infalible. No ponga la encriptación de todos sus datos en WEP, ya que éste es un nivel de seguridad más entre muchos otros y no se debe contar con él como su única medida de protección.

9) La VPN es uno de los mejores mecanismos de seguridad que existe. Si cada opción de seguridad funciona como una puerta cerrada bajo llave que los "hackers" tienen que penetrar cambiando SSIDs, programando filtración de direcciones MAC y utilizando una generación dinámica de claves WEP, entonces una Red Virtual Privada (VPN - Virtual Private Network) es la puerta de la bóveda de un banco. Las VPNs ofrecen niveles más altos de seguridad (Capa 3) que la WEP y permiten un túnel seguro de extremo a extremo entre el usuario y la red.

10) Aprovéchese de los servidores RADIUS existentes.

11) Compartir sólo lo necesario. Limitar los directorios compartidos a aquéllos a los que realmente queremos compartir y no a todo el disco duro. Y proteger éstos con claves fuertes.

12) Asegurar la entrada al punto de acceso. Establecer claves de entrada para poder tener derecho a las propiedades administrativas del equipo.

13) Deshabilitar la administración remota de los puntos de acceso.

14) Aislar el segmento de red formado por los dispositivos inalámbricos de nuestra red convencional. Es aconsejable montar un firewall (cortafuegos) que filtre el tráfico entre los dos segmentos de red.

15) No usar TCP/IP para compartir el sistema de ficheros o las impresoras. Normalmente los puntos de acceso están instalados detrás de los routers y cortafuegos; de esta forma al utilizar los clientes TCP/IP para acceder al sistema les estamos denegando automáticamente el acceso a nuestro sistema de ficheros e impresoras al estar éstos compartidos por otro protocolo.

16) Usar el OSA[5]. Esto es debido a que en la autenticación mediante el SKA[6], se puede comprometer la clave WEP que nos expondría a mayores amenazas. Además el uso del SKA nos obliga a acceder físicamente a los dispositivos para poder introducir en su configuración la clave. Es bastante molesto en instalaciones grandes, pero es mucho mejor que difundir a los cuatro vientos la clave. Algunos dispositivos OSA permiten el cambiar la clave cada cierto tiempo de forma automática, lo cual añade un extra de seguridad pues no da tiempo a los posibles intrusos a recoger la suficiente información de la clave como para exponer la seguridad del sistema.

[5] OSA (Open System Authentication, Autenticación Abierta), cualquier interlocutor es válido para establecer una comunicación con el Punto de Acceso.

[6] SKA (Shared Key Authentication, Autenticación mediante Clave Compartida) es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación, entonces, el dispositivo receptor pide al Punto de Acceso autenticarse. El Punto de Acceso le envía una trama al receptor, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.

17) Desactivar el DHCP[7] y activar el ACL[8]. Debemos asignar las direcciones IP manualmente y sólo a las direcciones MAC conocidas. De esta forma no permitiremos que se incluyan nuevos dispositivos a nuestra red. En cualquier caso existen técnicas de sniffing de las direcciones MAC que podrían permitir a alguien el descubrir direcciones MAC válidas si estuviese el suficiente tiempo escuchando las transmisiones.

18) Utilice herramientas avanzadas si lo requiere. Por ejemplo, la mejor forma para impedir los accesos no autorizados es utilizar un mecanismo de autentificación fuerte protegido mediante encriptación como: Transport Layer Security (TLS), Protected EAP (PEAP) o unneled TLS (TTLS). Para evitar el análisis no autorizado de tráfico es recomendable emplear protocolos seguros como el SSH, SSL o IPSec.

19) Simplifique su seguridad. Integre políticas inalámbricas y de cables. La seguridad inalámbrica no es una infraestructura de red por separado que requiere de procedimientos y protocolos diferentes. Desarrolle una política de seguridad que combine una seguridad por cable e inalámbrica para aprovecharse de las ventajas de administración y costos. Por ejemplo, integre una sola identificación de usuario y requerimiento de contraseña para cada usuario cada vez que éste(a) entre a la red por medio de cualquiera de las dos infraestructuras.

20) No todas las WLANs fueron creadas iguales. Aunque el 802.11b es un protocolo estándar y todos los equipos que llevan la marca WiFi operarán con la misma funcionalidad base, no todos los equipos inalámbricos son iguales en términos de seguridad. Aunque el Wi-Fi asegura interoperabilidad, los equipos de muchos fabricantes no incluyen funciones mejoradas de seguridad.

21) No permita que se creen redes no autorizadas. Hoy en día, la instalación de una WLAN es lo suficientemente simple como para que algún miembro del personal sin conocimientos técnicos instale sus propios "routers" o puntos de acceso inalámbricos en los departamentos de sus oficinas, con poca conciencia de seguridad. Vigile con regularidad su red con herramientas de detección de intrusos para deshacerse de redes no autorizadas que proveen puntos de entrada susceptibles a los "hackers". Asegúrese de tener una política que restrinja la creación de WLANs sin sistemas de administración formales e implementaciones aprobadas. Monitoree frecuentemente su red para detectar intrusos.

22) Recuerde que los "hackers" están siempre buscando como obtener información fácilmente y las redes inalámbricas están siendo actualmente su mejor opción. Esté pendiente de nuevas tecnologías de protección que salen al mercado.

---

[7] DHCP (Dinamic Host Configuration Protocol, Protocolo de Configuración de Host Dinámico). Función que permite a los ordenadores que se conectan a la red identificarse entre sí, garantizando de esta manera que los datos se transfieran correctamente entre ellos.

[8] ACL (Access Control List, Lista de Control de Acceso), y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

3.4. PRUEBAS CON EQUIPO INALÁMBRICO

3.4.1. Características del equipo utilizado

A lo largo de este trabajo hemos analizado las características del sistema y hemos encontrado que una solución de tipo inalámbrica será la más conveniente para resolver el problema.

La principal dificultad que existe al implementar un proyecto es el contar con los medios económicos para adquirir los diferentes dispositivos que lo conforman. En el caso de nuestro trabajo una implementación de la solución propuesta resultaría en una gran inversión que solamente puede ser absorbida por el cliente a quien pertenece el proyecto. Nuestro trabajo fue desarrollado con la expectativa de implementar físicamente nuestra propuesta; sin embargo, en el momento de escribir este trabajo aún no se contaba con los medios para desarrollarlo con los dispositivos recomendados en nuestro diseño. A pesar de estas dificultades el interés de validar nuestra propuesta nos orilló a desarrollar pruebas con otros dispositivos que, aunque no son los ideales, sí nos permitieran tener una expectativa de la respuesta que encontraríamos en una implementación con equipo inalámbrico.

Estas pruebas se enfocaron en los dispositivos inalámbricos que nos permitieran una interconexión entre edificios, por ello utilizamos dos "Access Point" – "Bridge" (punto de acceso – puente) con las siguientes características (las figuras corresponden a su configuración en pantalla).

Características técnicas del equipo:

Figura 3.3 Aironet AP 630-2400.

Nombre: Ethernet Access Point.

Modelo: 630-2400 (1996).

Compañía: Aironet Wireless Communications Inc.

Frecuencia de transmisión: 2.4 Ghz.

Tasa máxima de transmisión: 2 Mbps.

Alcance:

- De 38 a 61 metros con antena estándar en una oficina vacía.
- De 23 a 38 metros con antena estándar en una oficina concurrida.
- De 45 a 91 metros en una oficina vacía con la antena estándar elevada a 1.8 metros.
- De 30 a 45 metros en una oficina concurrida con la antena estándar elevada a 1.8 metros.
- Aproximadamente 300 metros con una antena estándar en exteriores.
- Más de 9 kilómetros con una antena opcional tipo yagi en exteriores.

Alimentación: 120 ó 240 volts - corriente alterna.

Antena:

- Estándar Dipolo a 2 dB (incluida).
- Omnidireccional a 3 dB (opcional).
- Tipo reflector a 6 dB (opcional).
- Tipo yagi a 13.5 dB.

Conexiones: 10BaseT (Par trenzado Ethernet), 10Base5 (Puerto AUI), 10Base2 (Conector BNC), Puerto RS-485, Puerto RS-232 (DB-9 hembra).

Medio de Configuración: Mediante un programa emulador de terminal (para nuestras pruebas se utilizó Microsoft Windows Hyperterminal).

Características funcionales del equipo:

Los equipos pueden ser configurados para funcionar como:

- Punto de acceso en oficina.
- Repetidor (repeater).
- Ruteador (router).
- Puente.

Para nuestro proyecto nos interesa la modalidad de Puente (Figura 3.4). Esta modalidad se puede implementar en modo Unicast (transmisión de uno a uno) y Multicast (uno a muchos). En nuestro proyecto se requeriría una transmisión Multicast (uno a dos). A pesar de que sólo contamos con dos equipos para transmitir, es posible realizar las pruebas en esta modalidad.

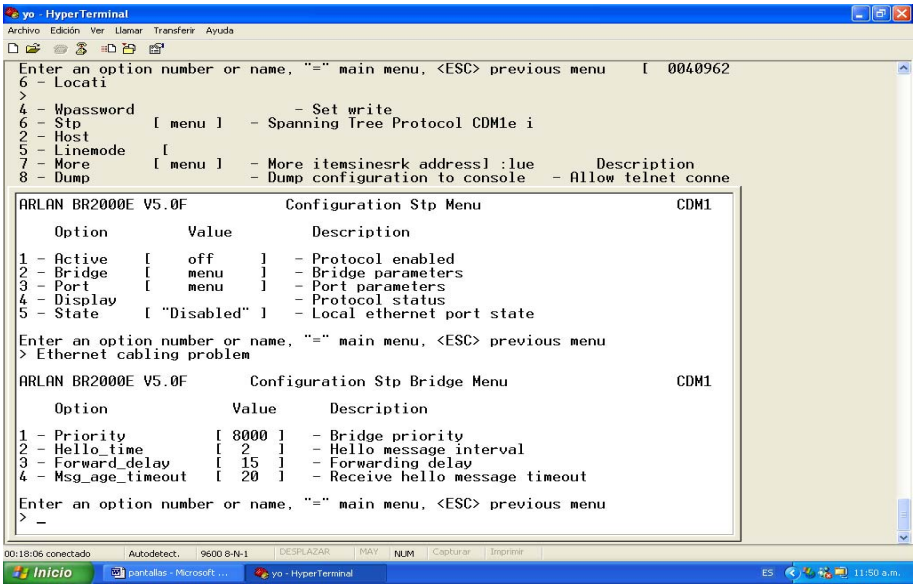


Figura 3.4. Modo Bridge.

Estos dispositivos manejan los siguientes protocolos: Novell Netware, NDIS LAN, Microsoft LAN Manager, PC LAN, SNMP, IPx, Ethertalk, TCP/IP y los protocolos basados en él.

Características de seguridad del equipo:

Algunas de las opciones de seguridad son las siguientes:

Modo escritura y/o lectura. Mediante la creación de una contraseña es posible bloquear la lectura de la configuración del equipo o limitarlo a solo lectura sin que se pueda modificar. (Figura 3.5).

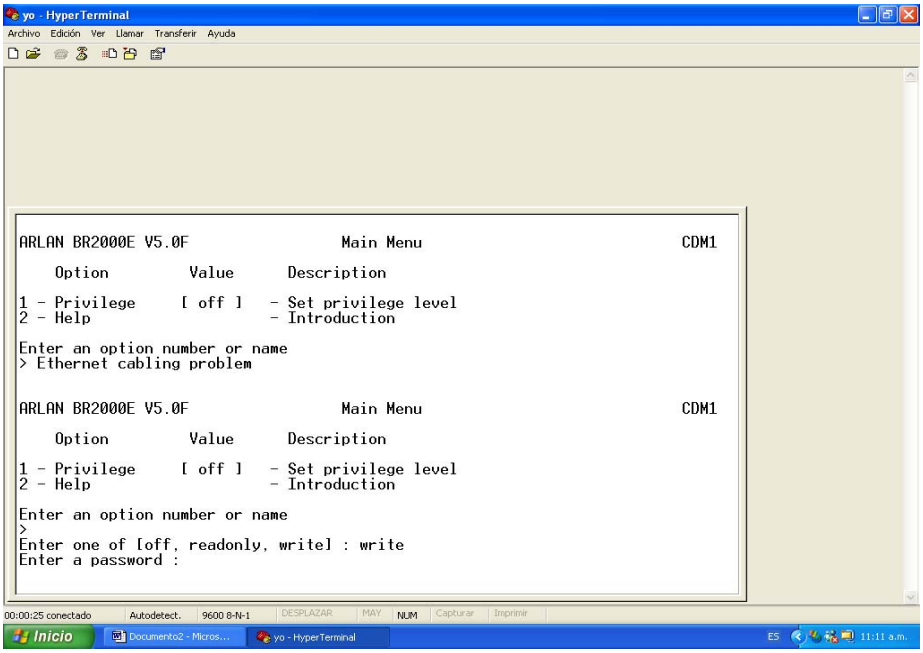


Figura 3.5. Modo escritura y/o lectura

SID. Establece un identificador codificado para cada equipo, lo que permite limitar la conexión a solo los equipos definidos estableciendo límites en la red (Figura 3.6).

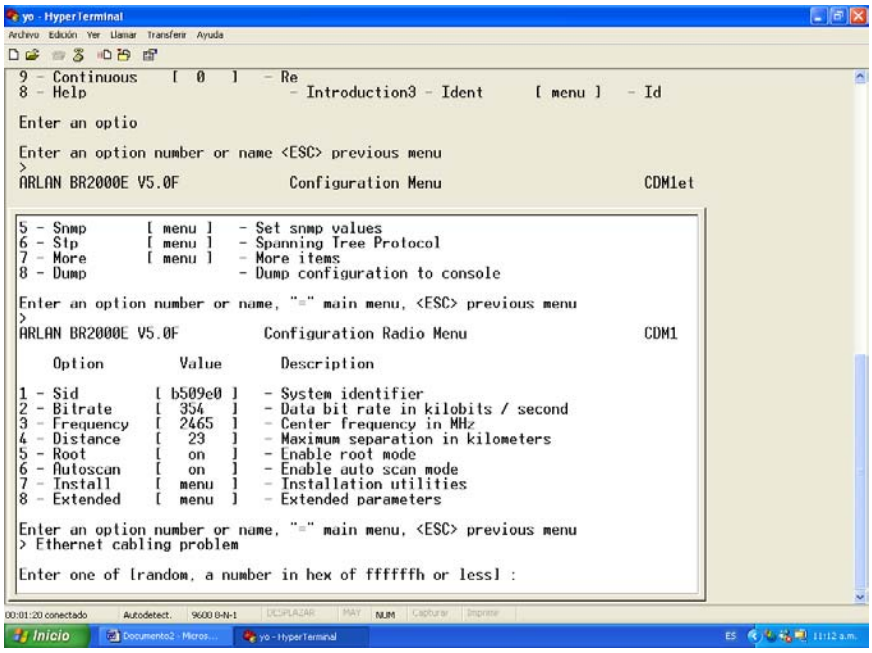


Figura 3.6. SID

Frequency (Frecuencia). Se puede definir una frecuencia más específica para limitar la transmisión o mejorar su calidad (Figura 3.7).

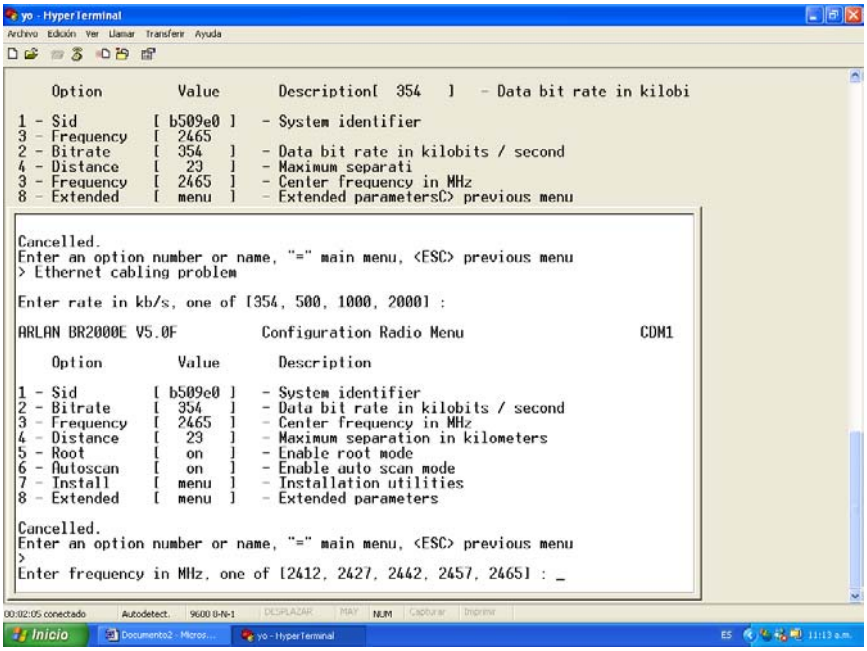


Figura 3.7. Frecuencia

Distance (Distancia). Podemos limitar la distancia de transmisión a exteriores (Figura 3.8).

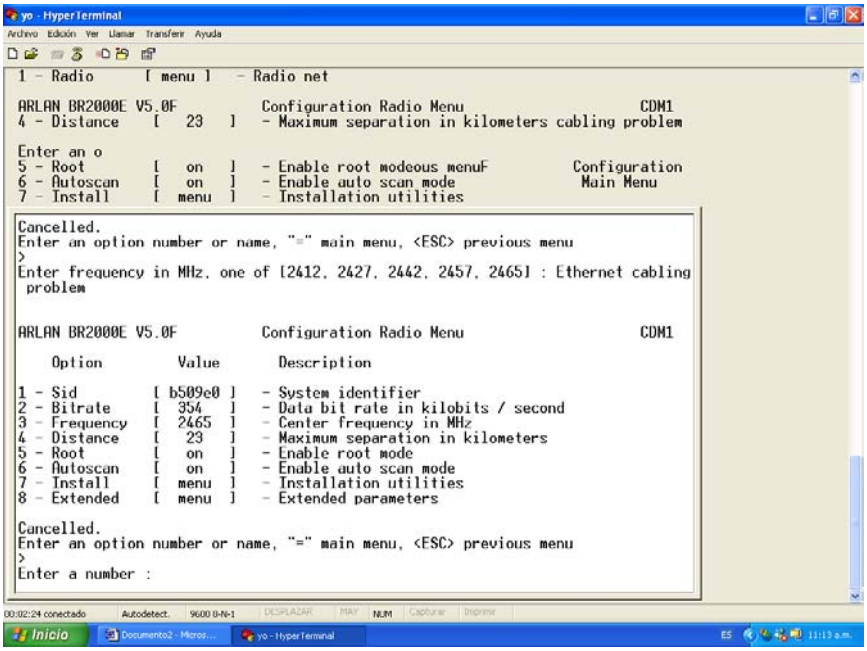


Figura 3.8. Distancia

Root (Ruteo)**.** La opción root nos permite establecer rutas de entrega de paquetes y bien manejada es una opción tanto de orden como de seguridad (Figura 3.9).

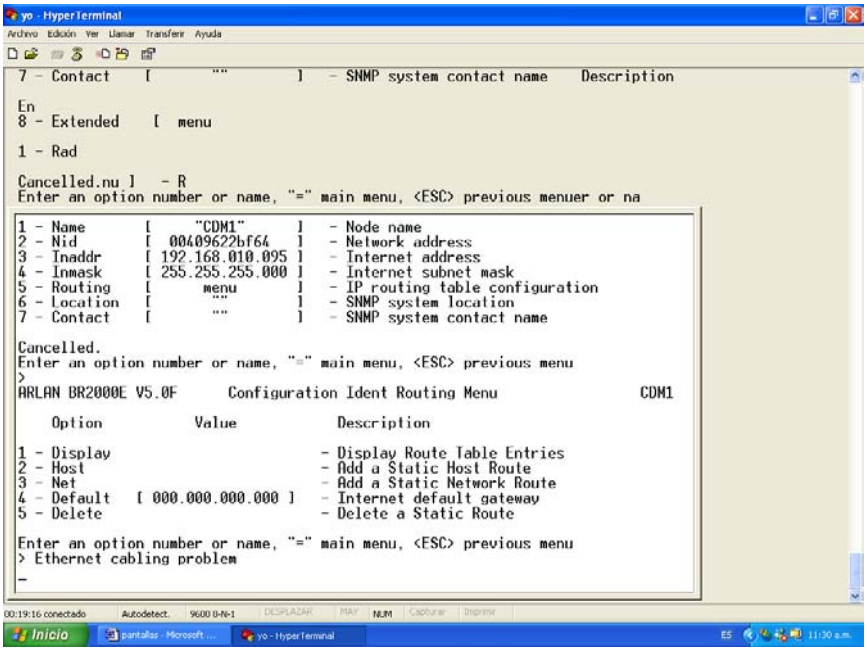


Figura 3.9. Ruteo

Ethernet. Nos permite configurar parámetros como *Active* (Activo) para habilitar o no el funcionamiento del dispositivo en una red; "*Size"* (Tamaño) para establecer la máxima longitud de trama y "*Port"* para designar el puerto por donde se comunicará. Esto resulta en una mejor administración y por ello en una ayuda extra a la seguridad (Figura 3.10).

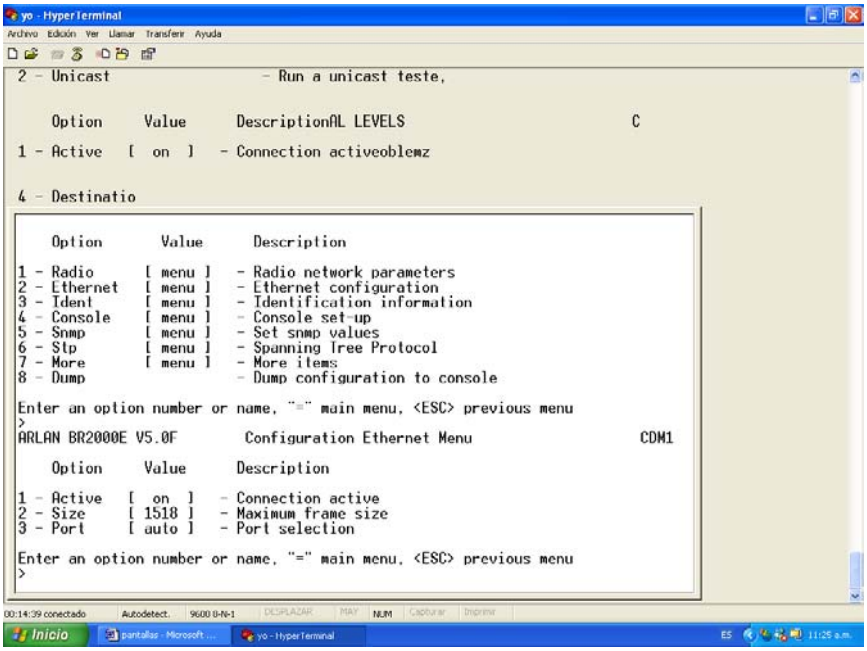


Figura 3.10. Ethernet

Ident. Este menú permite identificar con claridad al dispositivo dentro de la red al asignarle un nombre, una clave de identificación en la red *(Nid),* dirección IP, máscara de red, ruteo y localización SNMP (Figura 3.11).

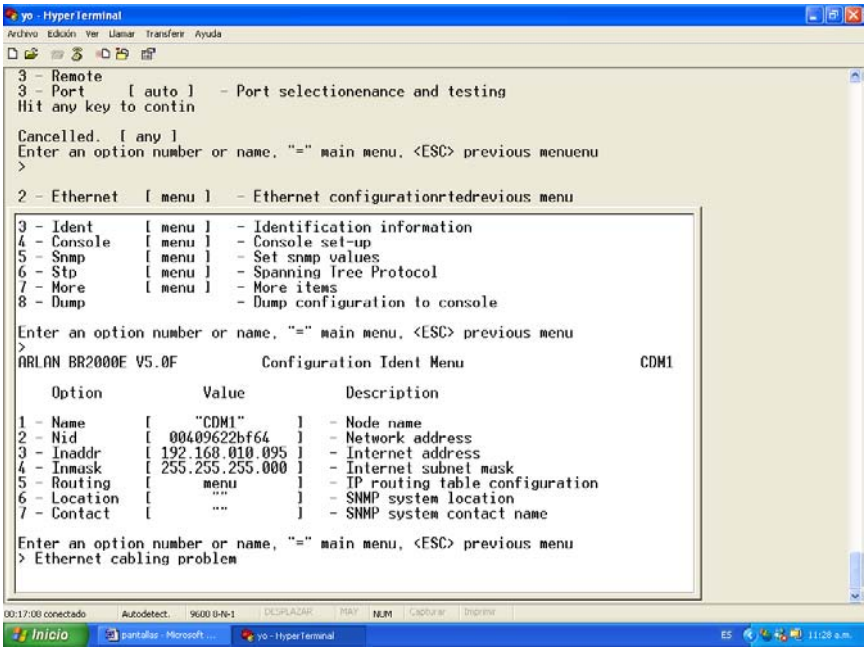


Figura 3.11. Identificador

Filter (Filtro). Se puede establecer un filtro para aceptar la transmisión sólo con equipos o configuraciones designadas. Este filtro se puede establecer por dirección de red, por nodo y por protocolos (Figura 3.12).

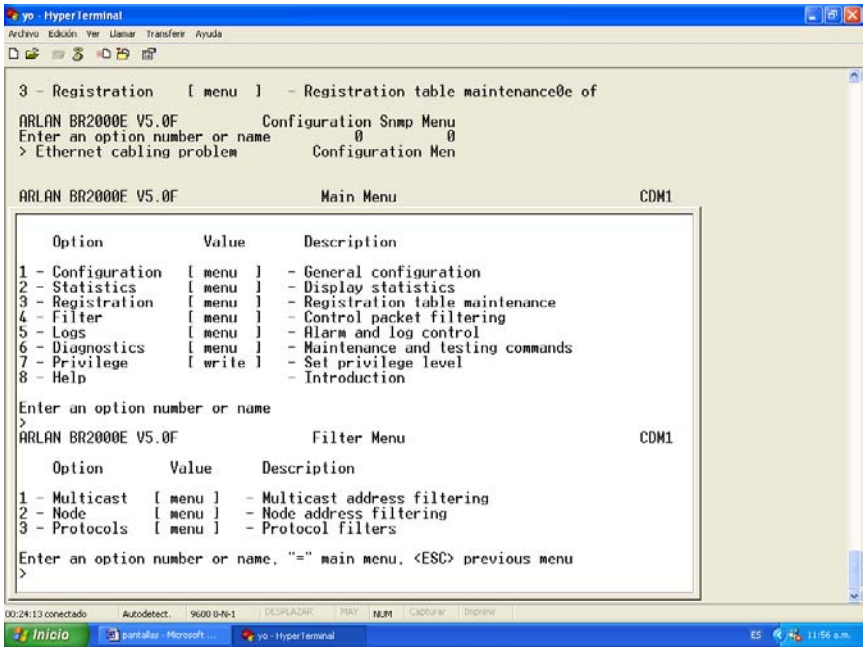


Figura 3.12. Filtro

Éstas son algunas de las opciones que se encuentran disponibles para otorgar un poco de seguridad a los dispositivos; solamente las hemos descrito de manera breve ya que una configuración formal requiere más tiempo; sin embargo, el conocimiento y utilización detallada de todas las opciones (primarias y secundarias) proveen de una mejor organización y protección de la red.

Características de las pruebas.

Nuestro mayor interés respecto a los equipos es el establecer una buena calidad en la transmisión a distancia y saber si la tecnología inalámbrica nos permitirá realizar los enlaces pretendidos en nuestro sistema. La seguridad será un aspecto secundario en las pruebas ya que la implementación de medios que hagan seguras nuestras transmisiones se considerará solamente en el desarrollo del sistema completo (pueden ser medios de configuración como WEP o externos como firewalls, VPN, etc.) además, los equipos que utilizamos son antiguos y no poseen muchas herramientas actuales para reforzar la seguridad de este tipo de enlaces.

Por estas razones nuestras pruebas se enfocarán en medir las distancias a las cuales podemos transmitir y el porcentaje de datos correctos que se reciben al otro lado del enlace. Realizaremos una tabla en la que relacionaremos las distancias con el porcentaje de datos recibidos correctamente.

Las pruebas se realizarán bajo las siguientes condiciones:

- Una tasa de transmisión media: 1 Mbps. (la mínima es 860 Kbps y la máxima es 2 Mbps).
- El primer grupo de pruebas consistirá en transmisiones realizadas en una oficina medianamente concurrida con los equipos mencionados con la antena estándar.
- El segundo grupo de pruebas implicará un enlace a distancia en un área con distintos edificios de pequeña altura y una población mediana de árboles; se utilizará una antena externa tipo yagi.
- Se realizarán cinco transmisiones en cada punto (distancia) por medio de la opción LINKTEST de los equipos.

3.4.2. LINKTEST

Los equipos utilizados para realizar las pruebas cuentan con una opción llamada LINKTEST (prueba de conexión) que sirve para evaluar la calidad de la transmisión entre unidades, ya sea en modo punto de acceso, repetidor, ruteador o puente.

La prueba tiene el siguiente desarrollo en los equipos:

- Uno de los equipos manda una secuencia de paquetes de datos de control especiales, especificando el destino a donde deben llegar.
- Los nodos que reciben estos paquetes realizan una acción de "eco" regresándolos a su nodo de origen.
- Cada paquete de datos de control contiene un número que lo identifica dentro de la secuencia, lo que permite saber qué paquetes se perdieron en el camino desde la fuente hasta su destino o en el viaje de regreso de los nodos a su origen.

Como se mencionó anteriormente, estas pruebas se pueden realizar de modo Unicast, es decir de uno a uno, o Multicast de uno a varios o mediante la dirección de los nodos dentro de la red (Figura 3.13).

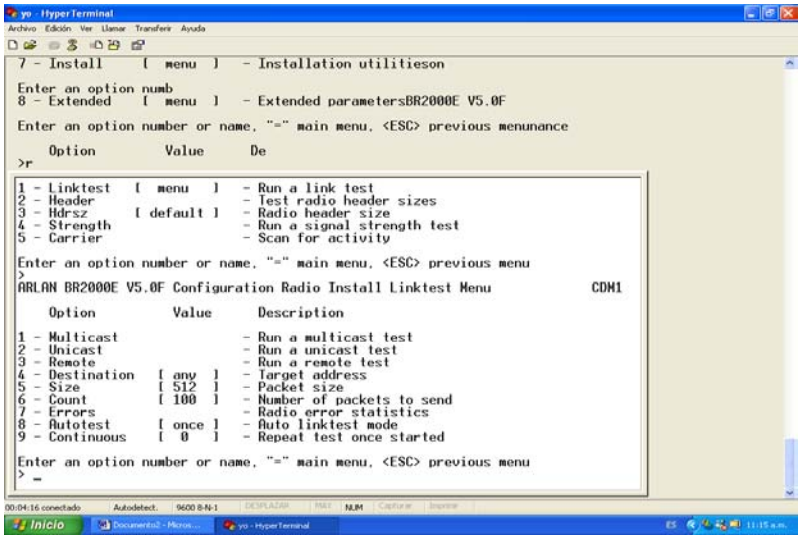


Figura 3.13. Unicast y Multicast

Además, se puede especificar el tamaño (entre 24 y 1000 bytes) y número de paquetes (entre 1 y 999). Por defecto se envían 100 paquetes de 512 bytes; éste será el estándar que se utilizará para nuestras pruebas (Figura 3.14).

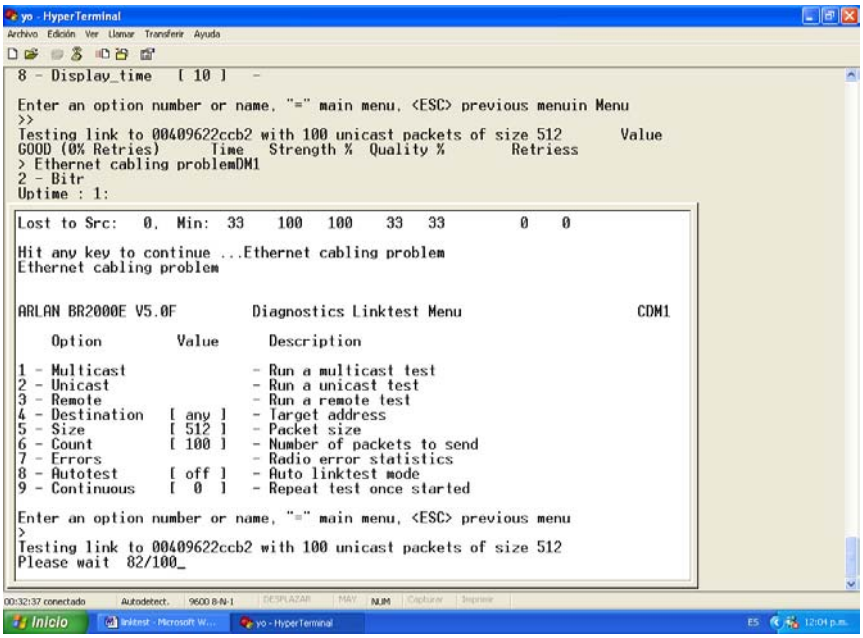


Figura 3.14. Tamaño y número de paquetes

La siguiente es la pantalla que presenta el resultado de la prueba y el porcentaje de datos perdidos (por lo cual podemos calcular el porcentaje de datos transmitidos correctamente).

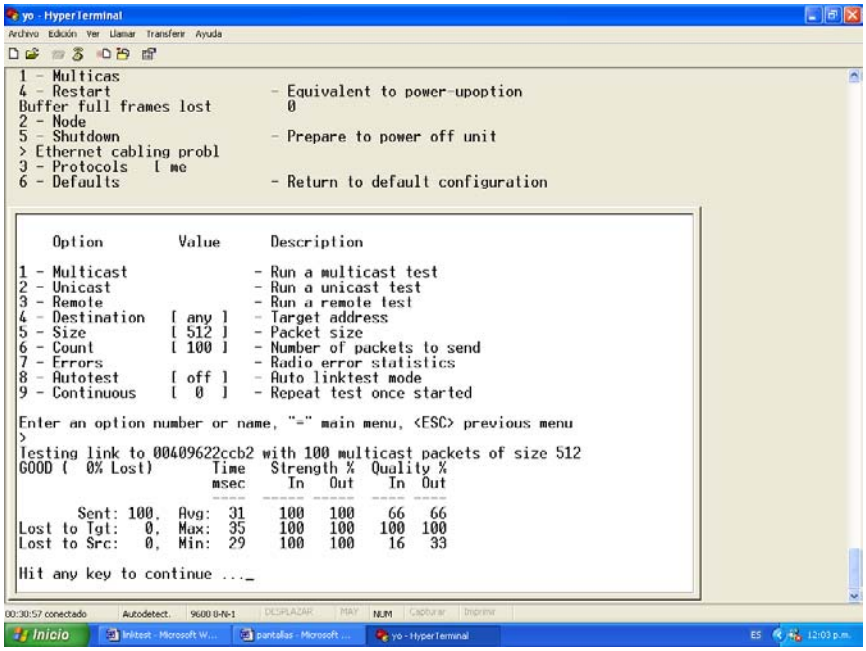


Figura 3.15. Resultados de pruebas y porcentajes de datos perdidos

Los equipos presentan la posibilidad de saber más acerca de los errores de transmisión (como estadísticas de recepción (Figura 3.16), de errores (Figura 3.17), de conexión Ethernet (Figura 3.18), historial gráfico (Figura 3.19), condiciones generales de conexión (Figura 3.20), etc.) sin embargo, por el significado de estas pruebas no entraremos en más detalles que el porcentaje de datos transmitidos correctamente.

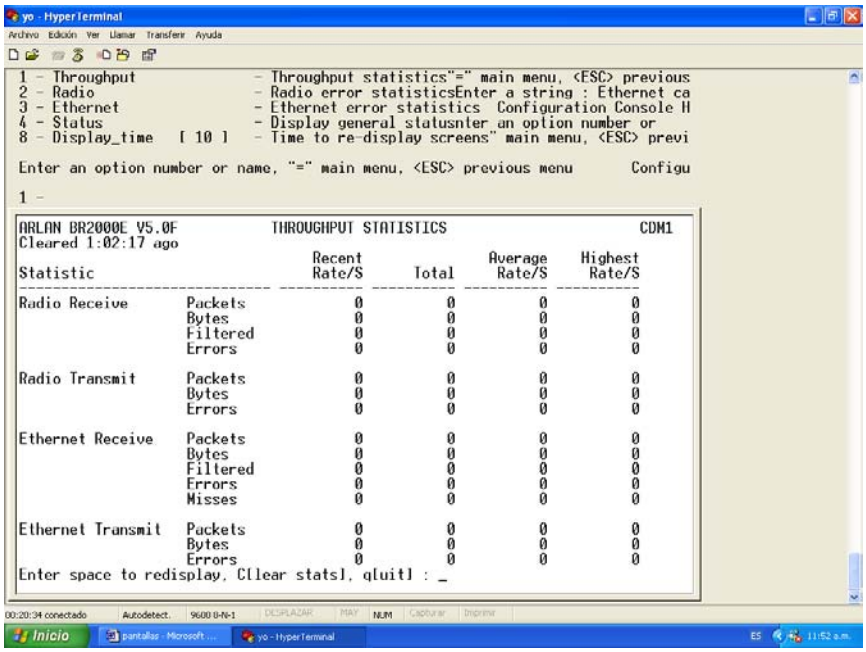


Figura 3.16. Estadística de recepción

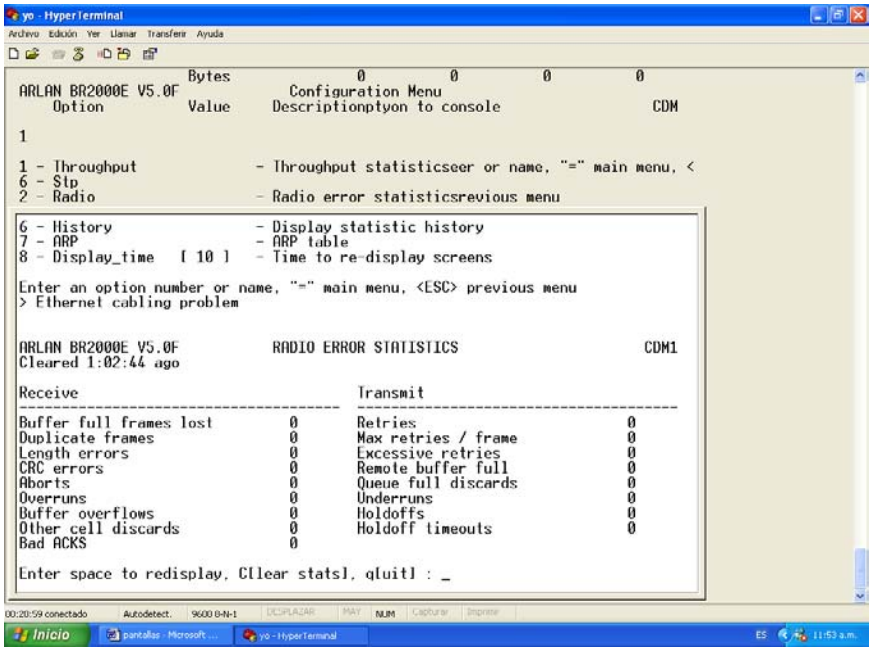


Figura 3.17. Estadística de errores

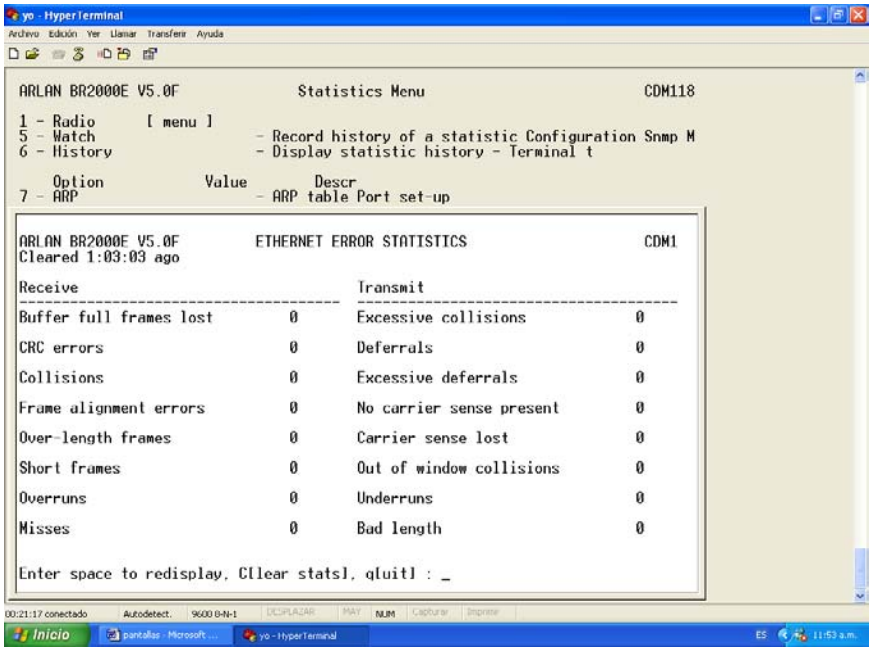


Figura 3.18. Estadística de conexión Ethernet

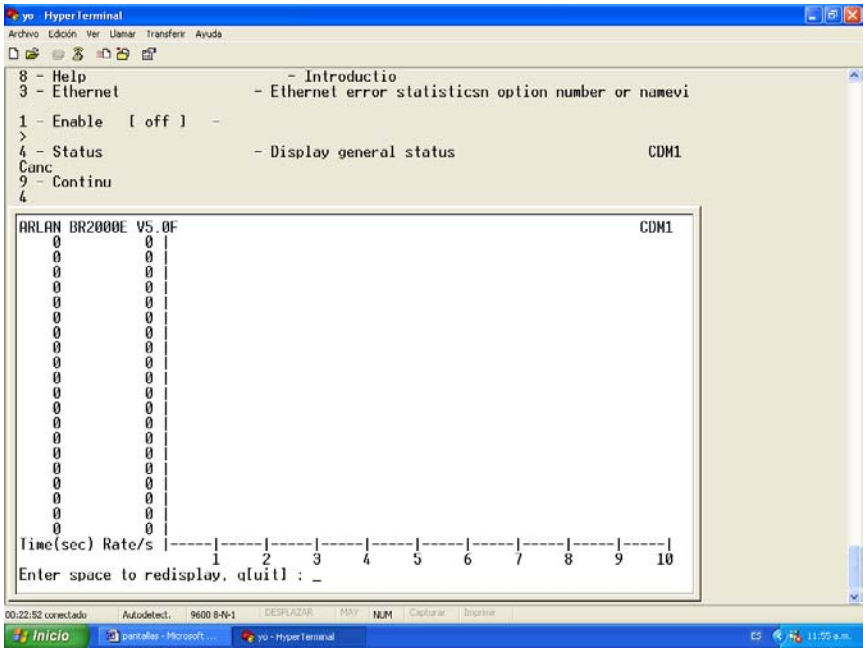


Figura 3.19. Historial Gráfico

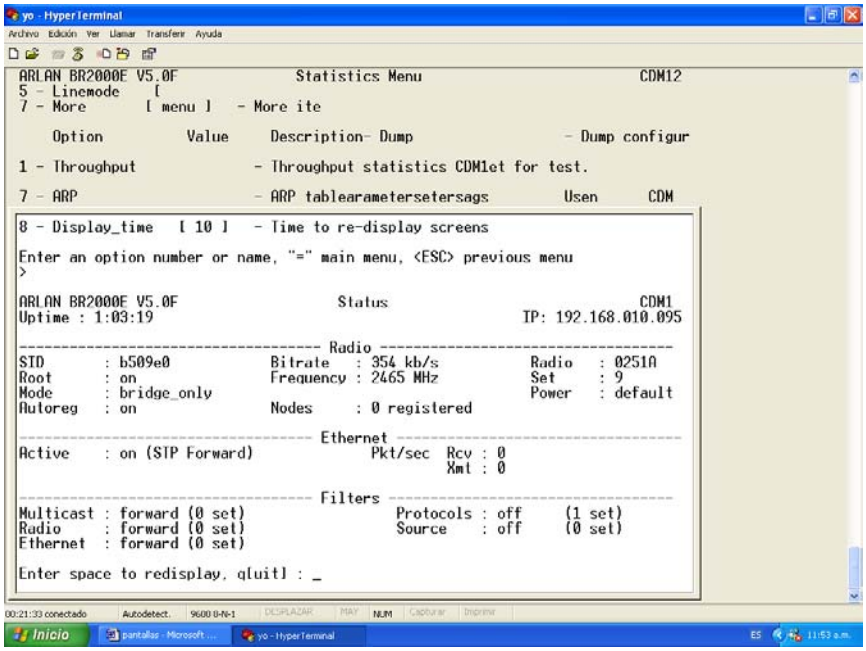


Figura 3.20. Condiciones generales de conexión

3.4.3. Resultados de las pruebas.

GRUPO DE PRUEBAS 1.

Estas pruebas se realizaron dentro de un edificio con paredes cada 10 metros construidas de tabique con un grosor de aproximadamente 15 centímetros. Las condiciones ambientales eran normales. Los equipos se encuentran directamente conectados a la PC por medio de la entrada 10BaseT (Par trenzado Ethernet) aunque dicha conexión no influye en las pruebas. La antena es la estándar conectada directamente a los equipos (sin elevar). Los resultados son los siguientes:

DISTANCIA	PRUEBA 1	PRUEBA 2	PRUEBA 3	PRUEBA 4	PRUEBA 5	PROMEDIO
2 metros	100%	100%	100%	100%	100%	100%
10 metros	100%	100%	100%	100%	100%	100%
20 metros	100%	100%	100%	100%	100%	100%
30 metros	100%	100%	100%	99%	100%	99.8%
40 metros	100%	99%	100%	100%	100%	99.8%
50 metros	100%	100%	98%	100%	100%	99.6%
60 metros	100%	99%	100%	100%	99%	99.6%

PROMEDIO TOTAL =	99.57%

GRUPO DE PRUEBAS 2.

Estas pruebas se realizaron conectando una antena yagi a cada uno de los equipos y colocándolas en la azotea de los edificios (estos edificios tienen alturas similares y se encuentran en una superficie más o menos uniforme: CU). Se tomó siempre un edificio como punto fijo en donde se ubicó una de las antenas a aproximadamente 12 metros de altura. Las antenas se orientaron lo mejor posible. Los resultados son los siguientes:

DISTANCIA / ALTURA	PRUEBA 1	PRUEBA 2	PRUEBA 3	PRUEBA 4	PRUEBA 5	PROMEDIO
100 metros / 6 m	100%	100%	100%	100%	100%	100%
200 metros / 12 m	100%	100%	100%	100%	100%	100%
500 metros / 10 m	99%	100%	98%	100%	99%	99.2%
700 metros / 17 m	100%	99%	100%	100%	99%	99.6%
1000 metros / 18 m	100%	100%	99%	100%	100%	99.8%
1500 metros / 15 m	100%	99%	100%	99%	100%	99.6%
2000 metros / 20 m	100%	100%	100%	99%	100%	99.80%

PROMEDIO TOTAL =	99.71%

3.5. ADMINISTRACIÓN DE LA RED INALÁMBRICA

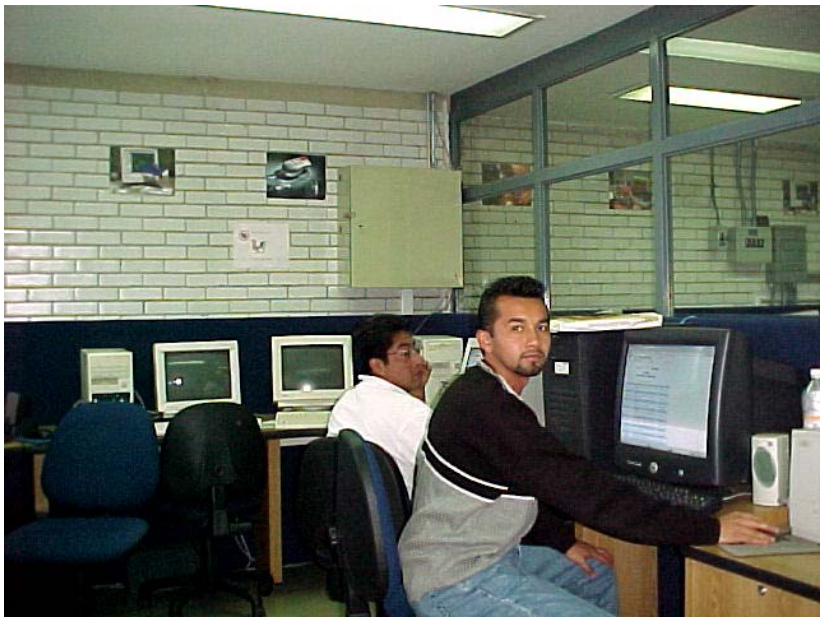


Figura 3.21. Administración de la red

En esta fase se realiza la definición de estándares, herramientas y procedimientos que aseguren una correcta utilización y mantenimiento de la red.

El objetivo es proporcionar herramientas que permitan tener todos los elementos de la red inalámbrica bajo control.

La administración de la red se puede definir como el conjunto de actividades requeridas para planear, instalar, supervisar y mantener todos los componentes de la red con el fin de lograr niveles de servicio requeridos de manera confiable, a un costo aceptable.

Las funciones del administrador de la red pueden dividirse en dos grupos:

3.5.1. Funciones Diarias. Están relacionadas con el control diario de la red, incluyendo:

- Supervisión y mantenimiento del nivel de servicio.
- Manejo de fallas: identificación, diagnóstico y reparación de las fallas en los componentes de la red.
- Administración de los cambios de la red inalámbrica: esta actividad incluye la administración de inventarios de todos los componentes de la red como por ejemplo: Computadoras, servidores, interuptores, puntos de acceso, antenas, impresoras, etc. También el control de las ediciones, movimientos y otros cambios en los sistemas de los usuarios.
- Supervisión en el desempeño de la red: esta función está relacionada con la supervisión y el mantenimiento del nivel de servicio y con la planeación del crecimiento de la red inalámbrica.
- Soporte a los usuarios: incluye entrenamiento de los usuarios y soporte en todos los aspectos relacionados con el acceso y uso de los servicios y facilidades de la red.
- Seguridad: es necesaria para garantizar que el acceso a los servicios de la red sea realizado únicamente por usuarios autorizados y que se encuentra bajo control muy estricto.

3.5.2. Funciones de Planeación. Cubren las actividades de largo plazo que se encuentran relacionadas con la operación de la red en el futuro. Estas actividades incluyen las siguientes:

- Planeación y Diseño: es la planeación que asegurará que la red será capaz de responder al crecimiento en el tráfico y será capaz de soportar la implementación de nuevas aplicaciones.

- Relaciones con los proveedores: el objetivo de esta función es supervisar las políticas de los proveedores, en aspectos como son las políticas de ventas y las políticas de mantenimiento.

Figura 3.22. Administración del servidor

Capítulo VI

MANTENIMIENTO DE LA RED

4.1. MANTENIMIENTO PREVENTIVO Y CORRECTIVO PARA EL HARDWARE Y SOFTWARE

Ya que está terminada la instalación de la red inalámbrica y que ya está funcionando correctamente hay que tomar en cuenta que el equipo tiene un período de vida útil, por lo que hay que adecuarse a las necesidades de la empresa, es por eso que hay que organizar una agenda de mantenimiento de la red.

Como la red está compuesta tanto de elementos de hardware como de software, el mantenimiento se debe realizar a ambos.

El mantenimiento del hardware.

Consiste en que se deben revisar periódicamente las computadoras y todo el equipo con el que se cuenta ya que se le deben realizar ajustes de limpieza interna y externa. Además de las computadoras, el medio de comunicación se debe revisar si hay continuidad en los puntos de acceso, evitar ruidos ocasionados por balastras, líneas eléctricas, etc. Se debe supervisar que los elementos de concentración tengan la adecuada instalación eléctrica, ya que cualquier elemento de la red híbrida es indispensable para su completa operación.

El mantenimiento del software.

Consiste en revisar los parámetros de seguridad de la red, esto quiere decir; revisar los privilegios de los usuarios y grupos de usuarios, los mecanismos de entrada a la red, respaldar la información, actualizar las aplicaciones.

Una gran cantidad de fallas que se presentan en la operación de las redes se deben a la falta de mantenimiento, por lo que no se debe perder de vista que es indispensable el que éstas se revisen para mantenerlas en óptimas condiciones de operación más aún cuando nuestra red dependerá de la poca interferencia de ondas en la antena.

Se recomienda que toda empresa que utiliza computadoras, lleve una bitácora del sistema. Éste es un diario en el que se anotan el hardware, el software con el que cuentan, ¿quién lo instaló?, ¿cuándo? y ¿dónde?, ¿qué configuración se le dio?, ¿cuándo se hicieron los respaldos y las restauraciones? y cualquier otra cosa que sea pertinente para describir y documentar el sistema.

4.2. CARACTERÍSTICAS

Es más fácil resolver los problemas si se sabe la configuración del equipo. Por lo tanto, es conveniente saber los siguientes puntos acerca de cada una de las PC´s de la red:

Hardware general:

- Los fabricantes que proporcionaron los componentes del sistema.
- Tipo de Procesador.
- Memoria.
- Su velocidad.
- ¿Qué tipo y tamaño es el disco duro?
- ¿Qué tarjetas tienen instaladas?
- ¿Qué direcciones de interrupciones y de Entrada/Salida son empleadas por las tarjetas instaladas?

Hardware de la red:

- El tipo de tarjeta de interfaz de red que tiene.
- ¿Que "bridge" se instalará?
- El tipo de "switch" se empleará.
- Tipo de antena que se ocupa.
- ¿Qué opciones están activadas?

Sistema operativo de la PC:

- Versión del sistema operativo que está cargado.
- ¿Qué opciones están instaladas?
- ¿Qué configuraciones han sido seleccionadas?

Programas residentes en memoria:

- ¿Qué programas de permanencia y residencia además del software de red se emplean?
- Éstos incluyen controladores para sistemas de almacenamiento en Cd´s y tarjetas de comunicación.

Datos de configuración:

Windows 2000 Server tiene dos archivos adicionales: WIN.INI y SYSTEM.INI. Las aplicaciones ya sea de DOS o Windows con frecuencia crean sus propios archivos de configuración. Es conveniente guardar una copia de estos archivos en discos flexible o Cd´s, para ahorrarse tiempo cuando se necesite consultar la configuración de un sistema que no esté funcionando.

Cable de red:

- El tipo de cable que se utiliza.
- Verificar que el cable que conecta a las PC´s sea el mismo para todas.

Software de red:

- Verificar qué versión tiene cada componente del software de la red.
- ¿Cuál es el tamaño de los archivos y las fechas de creación de cada componente? de manera que si se dañan de alguna manera se pueda saber si el archivo está intacto.
- ¿Qué interrupciones se utilizan?
- ¿Cuánta memoria disponible había después de cargar el software?

4.3. CAPACITACIÓN

Aunque la red deberá ser transparente, es decir, que los usuarios no se den cuenta de los procesos que se ejecutan al entrar a la red. Los usuarios necesitarán capacitación sobre los servicios que podrán controlar. En el nivel más básico los usuarios deberán estar al tanto de la red. Esto es importante para poder cimentar la confianza en el sistema.

En la empresa la capacitación la van a recibir todos los gerentes y personal de confianza de cada restaurante y uno de ellos se asignará para ser el supervisor de la misma y es el que va poder asignar los privilegios a los demás empleados.

4.4. ALCANCE TECNOLÓGICO EN UN FUTURO

Las redes se han convertido en el foco de nuestros recursos de computación, se están convirtiendo en un arma estratégica de negocios que es crucial para el éxito comercial de la misma, como tener teléfonos, fax, luz, etc. Las redes se convierten en el sistema nervioso de las corporaciones, llegan a encarnar la inteligencia de la organización ya que si el sistema se cae, no hay acceso a las bases de datos y no se puede tener acceso a información importante.
La última tendencia es que las compañías están empezando a hacer negocios en la red más grande del mundo Internet por el cual las redes inalámbricas sobresalen en la actualidad a la luz pública ya que es una manera de avanzar en cuestión tecnológica como los teléfonos celulares el cual ha surgido desde los 80 y actualmente se envía o recibe información de manera practica y sencilla, esto nos lleva a que las redes inalámbricas serán la gran base para nuestro siglo y los siguientes. Por el cual, la vía de transmisión por ondas en el aire será lo mejor en cuanto a transmisión y recepción de datos muy importantes que se pueden efectuar, para el año 2010 se estima que este hardware y el Internet dará un servicio a mucho más de mil millones de personas en todo el mundo por lo cual no será un lujo sino una necesidad en cuestión de la comunicación.

Glosario

ACL. Access Control List (Lista de Control de Acceso). Es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

ADSL. (Línea Asimétrica de Abonado Digital). Línea telefónica con tasas de transmisión diferentes en ambos sentidos.

Ancho de banda (Bandwidth). Expresa la cantidad de información que puede ser enviada a través de una comunicación y se mide en bits por segundos (Bps).

Banda ISM. La Comisión Federal de Comunicaciones y sus contra partes fuera de los Estados Unidos tienen separadas un conjunto de anchos de bandas para uso no regulado, en la llamada Banda ISM (Industrial, Scientific and Medical; Industrial, Científica y Medica) el espectro de operación se encuentra cerca de los 2.4GHz. En particular, está comenzando a ser disponible en todo el mundo; esto representa una oportunidad verdaderamente revolucionaria para ubicar convenientes capacidades de redes inalámbricas a altas velocidades en las manos de los usuarios alrededor del globo.

Bridge. (Puente). Dispositivo que permite la interconexión de redes de un mismo tipo.

Cifrado. Técnicas utilizadas para hacer inaccesible la información a personas no autorizadas. Se suele basar en una clave, sin la cual la información no puede ser descifrada.

Client (Cliente). Esta denominación se usa para representar el programa usado para contactar y obtener datos desde un software servidor que se encuentra generalmente en otro computador. En la arquitectura cliente-servidor, existe un software cliente corriendo en un computador y un software servidor corriendo en otro computador que interactúan entre ellos y ejecutan alguna tarea específica.

CNAC. Closed Network Access Control (Control de Acceso Red Cerrada). Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.

DHCP. Dinamic Host Configuration Protocol (Protocolo de Configuración de Host Dinámico). Función que permite a los ordenadores que se conectan a la red identificarse entre sí, garantizando de esta manera que los datos se transfieran correctamente entre ellos. La ventaja del protocolo DHCP es que las redes son eficientes al no malgastar el espacio de direcciones IP y, por lo tanto, los administradores informáticos no tienen la carga de trabajo adicional de estar pendientes de las direcciones IP.

DSSS. (Espectro Amplio de Secuencia Directa). DSSS es la tecnología de transmisión por radio utilizada por los dispositivos inalámbricos 802.11b. Técnica utilizada para transmitir datos por el espectro de frecuencias. En ella se expande el espectro de onda sobre un ancho de banda, para ello se envían varios bits por cada bit de información original.

Espejo (Mirror)**.** Término usado en Internet para hacer referencia a un servidor FTP, página Web o cualquier otro recurso que es espejo de otro. Estos mirrors se realizan automáticamente y en una frecuencia determinada, y pretenden tener una copia exacta del lugar del que hacen mirror.

Ethernet /Fast Ethernet (10BaseT/ 100BaseTX). Ethernet y Fast Ethernet son estándares internacionales en el sector de las redes. Ethernet, también conocido como 10BaseT, funciona a velocidades de hasta 10 Mbps. Fast Ethernet, también conocido como 100BaseTX, es capaz, en teoría, de funcionar a velocidades hasta 10 veces más rápidas, hasta 100 Mbps. Normalmente, el cableado CAT5 se utiliza para conectar cada ordenador de la red a redes Ethernet/Fast Ethernet.

Firewall. (Cortafuegos). Es una combinación de hardware y software que separa una red de área local (LAN) en dos o más partes con propósitos de seguridad.

FTP. File Transfer Protocol (Protocolo de Transferencia de Archivos). Protocolo de Internet que se utiliza para mover archivos de un sitio de Internet a otro. Los servidores públicos de FTP permiten la carga y descarga de archivos. Así se crean repositorios de tipo público.

GPS. Global Positioning System (Sistema de Pocisionamiento Global). Sistema de navegación que utiliza las señales de tres satélites para, a través de una antena, captar los datos y, por medio de una aplicación matemática, posicionar el vehículo reconociendo las coordenadas.

Hacker. Persona que tiene un conocimiento profundo acerca del funcionamiento de redes y 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. Computadora a la que tenemos acceso de diversas formas (telnet, ftp, world wide web, etc). Es el servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente.

HTTP. HyperText Transmission Protocol (Protocolo de Transmisión de Hipertexto). Protocolo usado para la transferencia de documentos.

Hub. (Concentrador). Dispositivo que permite conectar computadoras en red bajo una configuración de bus. El ancho de banda del hub se divide entre el número de dispositivos conectados.

ID. (Nombre de usuario). Corresponde al nombre de usuario o identificación de la persona que tiene permiso para accesar algún servicio en particular.

IEEE. Institute of Electrical and Electronic Engineers (Instituto de Ingeniería Eléctrica y Electrónica). Fundado en 1963 para difundir, investigar y regular normativas en los campos de la electrónica y de la electricidad.

IEEE 802.X. Conjunto de especificaciones de la redes LAN dictadas por el IEEE (the Institute of Electrical and Electronic Engineers). La mayor parte de las redes cableadas cumplen la norma 802.3, especificación para las redes Ethernet basadas en CSMA/CD, o la norma 802.5, especificación para las redes Token Ring. Existe un comité 802.11 trabajando en una normativa para redes inalámbricas de 1 y 2 Mbps. La norma tendrá una única capa MAC para las siguientes tecnologías: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) e infrarrojos. Se están desarrollando borradores de las normas.

Intranet. Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.
IP (Número IP). Este número esta dividido en cuatro partes separadas por puntos 206.137.97.254. Esto permite a un paquete de datos viajar a través de múltiples redes hasta alcanzar su destino. Cada computador está conectado a Internet y tiene su propio número IP y es único en todo el mundo.

ISDN. Integrated Services Digital Network (Red Digital de Servicios Integrados). En el servicio de ISDN las líneas telefónicas transportan señales digitales en lugar de señales analógicas, lo que aumenta considerablemente la velocidad de transferencia de datos a la computadora. Si se cuenta con el equipo y el software necesarios y si la central telefónica local ofrece ISDN y el proveedor de servicios lo soporta, el ISDN es posible utilizarlo. La velocidad de transferencia que puede alcanzar ISDN y el proveedor es de 128,000 Bps, aunque en la práctica las velocidades comunes son de 56,000 ó 64,000.

LAN. Local Area Network (Red de Área Local). Red de datos para dar servicio a un área geográfica máxima de unos pocos kilómetros cuadrados, por lo cual pueden optimizarse los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100Mbps (100 megabits por segundo).

MAC. Media Access Control (Controlador de Acceso a Medios)**.** El acrónimo MAC se suele utilizar para describir el uso de direcciones MAC. Todos los dispositivos de red tienen asignado un número exclusivo por el fabricante, similar a un número de serie exclusivo. Cada número se registra en FCC para poder tener constancia de la identidad del fabricante, convirtiéndolos así en una parte permanente del dispositivo de red. Estos números exclusivos, o direcciones MAC, se utilizan a veces para filtrar o restringir el acceso a la red.

Modelo Cliente-Servidor. El modelo cliente-servidor se apoya en terminales (clientes) conectadas a una computadora que los provee de un recurso (servidor). De esta manera los clientes son los elementos que necesitan servicios del recurso y el servidor es la entidad que poseen recursos. Los clientes sin embargo no dependen totalmente del servidor. Ellos pueden realizar los procesamientos para desplegar la información (por ejemplo en forma gráfica). El servidor los provee únicamente de la información sin hacerse cargo de otros procesos. El tráfico en la red de esta forma se ve aligerado y las comunicaciones entre las computadoras se realizan más rápido.

Network. (Red). Una red de computadoras es un sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en diferentes lugares. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

NIC. Network Interface Card (Placa de Interfaz de Red). Placa de interfaz que conecta la computadora a los cables de una red.

Nodo. Computadora conectada a una red de área local por un medio físico. Un nodo inalámbrico es, por ejemplo, una computadora de usuario con una tarjeta de red inalámbrica (adaptador), un Punto de Acceso, etc.

OSA. Open System Authentication (Autentificación Sistema Abierto). Cualquier interlocutor es válido para establecer una comunicación con el Punto de Acceso.

OSI. Open System Interconect (Interconexión de Sistemas Abiertos). 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.

Paquete (Packet). La unidad de datos que se envía a través de una red. Un paquete se compone de un conjunto de bits que viajan juntos.

PCMCIA (Asociación Internacional de Tarjetas de Memoria para Computadoras Personales). PCMCIA es realmente una asociación internacional de normalización: Con el tiempo, el acrónimo PCMCIA ha venido a indicar el formato utilizado para las tarjetas de red inalámbrica en computadoras portátiles. Normalmente, las tarjetas PCMCIA son aproximadamente del mismo tamaño y la misma forma que una tarjeta de crédito y se conectan a la computadora portátil a través de un conector PCMCIA en la parte posterior o lateral de la computadora.

Protocolo. Un conjunto de normas reguladas, las cuales especifican cómo debe realizarse el intercambio de datos en la red.

Puente (Bridge). Los puentes son dispositivos que tienen usos definidos. Primero, pueden interconectar segmentos de red a través de medios físicos diferentes, por ejemplo, no es poco común ver puentes entre cable coaxial y de fibra óptica. Además, pueden adaptar diferentes protocolos de bajo nivel (capa de enlace de datos y física de modelo OSI).

Punto de Acceso. Dispositivo que sirve como medio de interconexión entre una red inalámbrica y una cableada o como un punto de unión para varios dispositivos.

Red inalámbrica. Red que no utiliza como medio físico el cableado sino el aire, utilizando generalmente microondas, o rayos infrarrojos.

Redes inalámbricas. El término "red inalámbrica" se utiliza para describir situaciones en las cuales dos o más computadoras pueden comunicarse entre sí, compartir archivos, impresoras y otros dispositivos sin estar conectados entre sí con cables. Las redes inalámbricas suelen comunicarse por ondas de radio.

Router. (Encaminador). Equipo informático conectado a una red con el fin de “encaminar” o dirigir los mensajes a una u otra red, aunque estas sean diferentes. De esta forma permite la interconexión de varias redes de comunicaciones. Se utiliza para establecer determinadas medidas de seguridad, de forma que se permita o impida el acceso a ciertas redes, o se limite su acceso.

SKA. Shared Key Authentication (Clave de Autentificación Compartida) es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación, entonces, el dispositivo TR pide al AP autenticarse. El AP le envía una trama al TR, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.

SMTP. Simple Mail Transfer Protocol (Protocolo Simple para la Transferencia de Correo). Protocolo de TCP/IP utilizado para transmitir e-mail en una red o para direccionar e-mail en Internet.

Switch. Equipo utilizado para conectar segmentos de redes locales, análogo a un puente con múltiples puertos, sin embargo, al contrario de los puentes que usan bus interno compartido, los switches permiten que las estaciones, en segmentos separados, transmitan simultáneamente.

Sniffer. Es un programa que monitoriza los paquetes de datos que circulan por una red. Más claramente, todo lo que circula por la red va en "paquetes de datos" que el sniffer chequea en busca de información referente a unas cadenas prefijadas por el que ha instalado el programa.

SNMP. Simple Network Management Protocol (Protocolo Simple de Administración de Red). Protocolo que se utiliza para administrar y monitorear dispositivos conectados a una red.

SSID. Service Set Identifier (Identificador de Conjunto de Servicio). Es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica. Los nodos y terminales deben conocer el nombre de la red para poder unirse a ella.

SSL. .Secure Sockets Layer (Capa de conexiones Seguras). Utiliza una llave de 40 bits para encriptar la información proporcionada de manera confidencial, ya sea a un proveedor, una base de datos, etc.

TCP/IP. Tranmission Control Protocol/ Internet Protocol (Protocolo de Control de Transmisión / Protocolo Internet). Sistema de protocolos, definidos en RFC 793, en los que se basa buena parte de Internet. El primero se encarga de dividir la información en paquetes en origen, para luego recomponerla en destino, mientras que el segundo se responsabiliza de dirigirla adecuadamente a través de la red.

Telnet. Protocolo de emulación de terminal que permite establecer una sesión remota a otra computadora en Internet.

Token Passing. (Paso de Ficha). Protocolo que se utiliza en redes Arcnet y Token Ring, y que se basa en un esquema libre de colisiones, dado que el permiso para transmitir (token) se pasa de un nodo o estación al siguiente nodo. Con esto se garantiza que todas las estaciones tendrán la misma oportunidad de transmitir y que un sólo paquete viajará a la vez en la red.

Token Ring. Red local desarrollada por IBM que utiliza el protocolo de acceso Token Passing y que utiliza un ancho de banda de 4 y 16 Mbps. Utiliza la topología de anillo.

Topología de Anillo. Topología en donde las estaciones de trabajo se conectan físicamente en un anillo, terminando el cable en la misma estación de donde se originó.

Topología de Bus. Topología en donde todas las estaciones se conectan a un cable central llamado "bus". Este tipo de topología es fácil de instalar y requiere menos cable que la topología de estrella.

Topología de Estrella. Topología donde cada estación se conecta con su propio cable a un dispositivo de conexión central, bien sea un servidor de archivo o un concentrador o repetidor.

Topología de Red. Se refiere a cómo se establece y se cablea físicamente una red. La elección de la topología afectará la facilidad de la instalación, el costo del cable y la confiabilidad de la red. Tres de las topologías principales de red son la topología de BUS de ESTRELLA y de ANILLO.

UIT. (Unión Internacional de Telecomunicaciones). Organismo internacional, con sede en Ginebra, cuya misión es definir estándares para las redes de comunicación.

VPN. Virtual Private Network (Red Privada Virtual). Una VPN es una red privada, construida sobre la infraestructura de una red pública (recurso público, sin control sobre el acceso de los datos), normalmente Internet. Es decir, en vez de utilizarse enlaces dedicados (como el X.25 y

Frame Relay) para conectar redes remotas, se utiliza la infraestructura de Internet; una vez que las redes están conectadas es transparente para los usuarios. A través de VPN, los accesos a los datos entre redes de la empresa y entre usuarios y la empresa son codificados, ofreciendo total seguridad a los usuarios y a la red de acceso. La principal motivación para la implantación de las VPNs es la financiera: los enlaces dedicados son demasiados caros, principalmente cuando las distancias son largas. Por otro lado existe Internet, que por ser una red de alcance mundial, tiene puntos de presencia diseminados por el mundo. Las conexiones con Internet tienen un coste mas bajo que los enlaces dedicados, principalmente cuando las distancias son largas.

WAN. World Area Network (Red de Área Mundial). Red de datos con un gran número de equipos que puede extenderse a una gran región geográfica, como todo un país o a muchos a través del mundo.

Warchalking. Es un lenguaje de símbolos normalmente escritos con tiza en las paredes que informa a los posibles interesados de la existencia de una red inalámbrica en ese punto.

WECA. Wireless Ethernet Compatibility Alliance (Alianza de Compatibilidad Ethernet Inalámbrica). Alianza para la compatibilidad de los dispositivos inalámbricos para crear una red Ethernet. Este grupo certifica la compatibilidad entre los productos para que sean compatibles con las normas descritas en 802.11.

WEP. Wired Equivalet Privacy (Confidencialidad Equivalente al Cable) .Clave introducida para intentar asegurar la autenticación, protección de las tramas y confidencialidad en la comunicación entre los dispositivos inalámbricos. Puede ser WEP64 (40 bits reales) WEP128 (104 bits reales) y algunas marcas están introduciendo el WEP256. Cuando se comunican dos dispositivos con cifrado WEP, establecen una "clave" compartida para la comunicación. Tanto si la clave se genera automáticamente o se asigna específicamente, los dispositivos deben utilizar la clave para identificarse con el fin de que se les permita la comunicación.

WLAN (Wireless Local Area Network). Red inalámbrica de área local. Son redes de área local que no utilizan cables para establecer la conexión ente los diversos dispositivos que las componen. Para comunicarse utilizan ondas de radio. En ellas sus miembros comparten recursos (periféricos, datos y aplicaciones).

WPAN (Wireless Personal Area Network). Red inalámbrica de área personal. Se trata de un tipo de red de muy limitada cobertura (generalmente usa Bluetooth) y que se limita a comunicar dispositivos como teléfono móvil, computadora portátil, etc.

Conclusiones

La propuesta que se desarrolló obtuvo las conclusiones siguientes:

- Las redes inalámbricas pueden tener mucho auge en nuestro país debido a la necesidad de movimiento que se requiere en la industria, para lo cual esta nueva tecnología inalámbrica abre un campo muy grande para las pequeñas y grandes empresas; el cual descubre un mundo de posibilidades de conexión sin la utilización de cableado clásico, proporcionando una flexibilidad y comodidad sin precedentes en la conectividad entre computadoras.

- Además es relativamente fácil el crear una red híbrida, con la cual se tuvo un seguimiento teniendo las ventajas de la velocidad que nos brinda la parte cableada y extenderíamos las posibilidades con la parte inalámbrica. Una red híbrida Ethernet, se puede considerar como una de las redes a la que se ha dado mayor uso actualmente en el mundo.

- El estándar IEEE 802.11, tiene un brillante futuro por delante. Va a ser el líder en comunicaciones empresariales y lo tiene todo para ser el Ethernet inalámbrico. Con la facilidad de instalación y sus considerables velocidades será el que comunique nuestras computadoras, no sólo portátiles, tanto en la oficina como en nuestras casas. Y eso sin olvidarnos de las otras tecnologías que, cada una por un lado, en nichos de mercado distintos van a salir igual de triunfadores, además de que serán más bien complementarios y no tanto competidores.

- Los logros de las pruebas y los resultados del proyecto son bastante satisfactorios, incluso en grandes distancias. A pesar de que se trata de equipos y marcas que resultan nuevos en el mercado y llegan a ser no muy compatibles, pudimos comprobar que funcionan bastante bien en cuanto a la calidad de transmisión.

- Los errores que se presentaron no fueron realmente muchos, considerando que las características del medio eran bastante diversas, ya que algunas de las pruebas fueron realizadas en condiciones de clima normal y otras en lluvia. Además, podemos ver que la distancia no es un verdadero problema puesto que con la ayuda de la antena externa se obtuvieron transmisiones de casi la misma calidad que en distancias cortas y bajo techo.

- Para completar nuestras pruebas realizamos conexiones a distancias en las que no solo transmitíamos datos de prueba sino aplicaciones más comunes. Uno de los puntos de acceso estaba conectado a una línea de conexión a Internet y el otro estaba conectado al módem de una computadora. Desplegamos distintas páginas y no encontramos problema alguno para ello, incluso quisimos medir el tiempo de retardo existente pero no fue posible ya que prácticamente no existió.

- Por estas razones, podemos decir que los errores son compensados por los protocolos de transmisión de paquetes de datos (como TCP/IP) que se aseguran de que los datos extraviados sean retransmitidos con la única dificultad de que se presenta un retardo de fracciones de segundo.

- Concluimos que toda la información y la nueva tecnología cumplen con el objetivo propuesto en esta tesis. Así como los equipos actuales que cuentan con mejores prestaciones técnicas (ancho de banda, velocidad, protocolos, etc.) y más y mejores herramientas de seguridad, permitirán un buen funcionamiento de nuestra red inalámbrica para empresas a larga distancia y ésta será una opción muy ventajosa respecto a métodos de transmisión más comunes como la fibra óptica o el cable de par trenzado o coaxial.

Figura C.1. Estructura de equipos

Es evidente que estas distintas etapas tuvieron que ser revisadas y corregidas para obtener un mejor resultado y podemos decir que, como en cualquier proyecto, el nuestro debe de ser constantemente revisado y actualizado si es que queremos que funcione de manera óptima.

Toda la información recabada a lo largo de este trabajo y todo el conocimiento adquirido y la información proporcionada en nuestras asignaturas fueron la guía de nuestra propuesta, por lo cual podemos decir que cumplimos con el objetivo de aplicar estos conocimientos teóricos en la solución de un caso práctico. Esperamos que este trabajo también sirva como guía para futuros proyectos y que toda la información que se concentró en nuestro trabajo pueda servir de ayuda a aquellas personas que la consulten, de la misma manera en que nosotros encontramos guía de los materiales consultados.

Figura C.2. Estructura de cada computadora con "Access Point"

Nos encontramos muy agradecidos con nuestra facultad por todas las facilidades que se nos otorgaron para la utilización de equipo, no sólo para la realización de esta propuesta, sino durante toda nuestra trayectoria académica. Obviamente nuestra facultad nos ha dado los medios para enfrentar problemas como el descrito en este trabajo y esperamos hacer honor a su nombre al abordar nuevos problemas en nuestra futura vida profesional.

Bibliografía

TANENBAUM Andrew S.; "Redes de computadoras"; Editorial Prentice Hall; New Jersey, Estados Unidos de Norteamérica; 1989; pp. 658.

MADRON Thomas W.; "Redes de Área Local. La siguiente generación"; Editorial Megabyte-Noriega Editores; México, D.F.; 1993; pp. 305.

RAPPAPORT Teodore S.; "Wireless Communications"; Editorial Prentice Hall; New Jersey, Estados Unidos de Norteamérica; 1996; pp. 641.

BLACK Ulises; "Redes de Computadoras"; Editorial Microbit Editores; México, D.F.; 1990; pp.421.

FUENTES DE INFORMACIÓN EN INTERNET

http://www.geocities.com/elplanetamx/tecnologiaslan.htm

http://elqui.dcsc.utfsm.cl/apuntes/redes/2001/pdf/0-4-Modelo-TCPIP-Diversas- Arquitecturas.pdf

http://medusa.unimet.edu.ve/electrica/fpie43/links.htm

http://pagina.de/inforedes

http://www.seguridadenlared.org/programs/SeguridadWireless.pdf

http://spain.micronet.info/Download/catalog/catalog.asp

http://www.netstumbler.com

http://www.infoworld.com/articles/hn/xml/01/08/24/010824hnfreewireless.xml

http://www.madridwireless.com

http://www.computienda.com.mx/inalambricas.asp

http://madridwireless.net

http://www.newswireless.net

http://www.communitywireless.org

http://www.wi-fi.com

http://www.linksys.com

http://www.cisco.com

http://www.3com.com

http://www.trendnet.com

http://www.micronet.com