PONTIFICA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TITULO DE

INGENIERO EN SISTEMAS

"ESTUDIO TÉCNICO COMPARATIVO DE REDES LAN ALAMBRICAS E INALÁMBRICAS"

AUTOR:
GABRIEL SEBASTIAN PROAÑO BRAGANZA

DIRECTORA: ING. BEATRIZ CAMPOS

QUITO NOVIEMBRE, 2009

ÍNDICE DE CONTENIDOS

LISTADO DE FIGURAS

LISTADO DE TABLAS

LISTADO DE ANEXOS

INTRODUCCIÓN

La globalización y automatización de la información en conjunto con los avances tecnológicos que esto supone nos ponen ante la imprescindible necesidad de conocer los diferentes parámetros que diferencian a las redes LAN Y WLAN con lo cual se tendrá una idea mucho mas clara y concisa de cuando utilizar cada una de las 2 tecnologías de redes o las 2 fusionadas de así requerirlo esto traería como consecuencia una solución al problema que a menudo se les presenta a los usuarios de redes informáticas al no saber cuando aplicar redes del tipo LAN y cuando podrían ser mas funcionales redes del tipo Wlan o viceversa.

Se podrían enumerar infinidad de ejemplos de cómo se instalan y configuran de manera inapropiada las redes LAN y WLAN y por consecuente el uso inadecuado que se les da a las mismas en los diferentes ámbitos de las organizaciones en donde son implementadas.

Muchas veces el ignorar el uso de redes informáticas deriva en el uso excesivo de recursos en periféricos que perfectamente podrían ser utilizados por varias estaciones de trabajo aprovechando así de forma más eficiente dicho hardware lo cual representaría a la empresa un ahorro sustancial en el presupuesto que tiene designado para dicho rubro.

Otro punto primordial por el cual se promueve este estudio comparativo es administrar de mejor forma aquel recurso intangible pero de alto valor para las organizaciones: la información, el cual viene de la mano con las redes informáticas en muchas ocasiones al no configurarla bien se pierde tiempo valioso al no estar actualizada la información entre los distintos usuarios, así como el ingreso de usuarios no deseados a dicha información.

El saber utilizar redes informáticas y aplicar correctamente sus servicios es sin duda un talón de Aquiles en el desarrollo de pequeñas, medianas y grandes organizaciones.

CAPITULO I

INTRODUCCIÓN

1.1 Redes Informáticas

Una red informática es un sistema de comunicación que enlaza computadores y otros equipos informáticos entre sí, con el fin de compartir información y recursos.

Cuando la información y los recursos de una red son compartidos, los usuarios de los sistemas informáticos de una organización pueden hacer un mejor uso de los mismos, optimizando de este modo el beneficio y/o rendimiento global de la organización.

Entre las ventajas que se pueden mencionar al tener instalada una red, están las siguientes:

- Mayor facilidad en la comunicación entre usuarios.
- Reducción en el presupuesto para software.[1]
- Posibilidad de organizar grupos de trabajo.
- Mejoras en la administración de los equipos y programas.
- Mayor seguridad para acceder a la información.
- Reducción en el presupuesto para hardware.[2]
- Seguridad en la administración de datos así como en la integridad de los mismos.

Para obtener todas las ventajas que supone el uso de una red informática, se deben tener instalados una serie de servicios de red, como son:

Acceso.- Los servicios de acceso se encargan tanto de comprobar la identidad del usuario (para asegurar que sólo pueda acceder a los recursos para los que tiene permiso) como de permitir la conexión de usuarios a la red desde zonas remotas.

1.- Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

2.- Conjunto de los componentes que integran la parte material de una computadora.

Ficheros.- El servicio de ficheros consiste en ofrecer a la red grandes capacidades de almacenamiento para descargar o eliminar los discos de las estaciones. Esto permite almacenar tanto aplicaciones como datos en el servidor, reduciendo los requerimientos de las estaciones. Los ficheros deben ser cargados en las estaciones para su uso.

Impresión.-Permite compartir impresoras entre varios ordenadores de la red, lo cual evitará la necesidad de tener una impresora para cada equipo, con la consiguiente reducción en los costes. Las impresoras de red pueden ser conectadas a un servidor de impresión, que se encargará de gestionar la impresión de trabajos para los usuarios de la red, almacenando trabajos en espera (cola de impresión), asignando prioridades a los mismos, etc.

Información.-Los servidores de información pueden almacenar bases de datos para su consulta por los usuarios de la red u otro tipo de información, como por ejemplo documentos de hipertexto.[3]

Otros.-En el campo de la comunicación entre usuarios existen una serie de servicios que merece la pena comentar. El más antiguo y popular es el correo electrónico (e-mail) que permite la comunicación entre los usuarios a través de mensajes escritos. Los mensajes se enviarán y se recuperarán usando un equipo servidor de correo. Resulta mucho más barato, económico y fiable que el correo convencional. Además, existen los servicios de conferencia (tanto escrita, como por voz y vídeo) que permitirán a dos o más usuarios de la red comunicarse directamente (en línea).

1.2 Historia de las redes

Hasta hace no mas de 4 décadas las redes informáticas estaban muy poco desarrolladas y su uso estaba limitado a ámbitos no muy cotidianos, sino mas bien de inteligencia militar, pero esto dio un gran giro a partir del “invento” del Internet, la llamada ahora red de redes, es por esto que no hay mejor forma de reflejar la historia de las redes que mirar hacia ella, a continuación una reseña breve pero completa de la red de redes.

3.- Texto que contiene elementos a partir de los cuales se puede acceder a otra información.

La idea de una red de computadoras diseñada para permitir la comunicación general entre usuarios de varios ordenadores se remonta al temprano desarrollo de las redes de comunicación.

Las más antiguas versiones de estas ideas aparecieron a finales de los años 50. Implementaciones prácticas de estos conceptos empezaron a finales de los 60 y a lo largo de los 70. En la década de 1980, tecnologías que reconoceríamos como las bases de la moderna Internet, empezaron a expandirse por todo el mundo. En los 90 se introdujo la World Wide Web, que se hizo común.

Un método de conectar computadoras, prevalente sobre los demás, se basaba en el método de la computadora central o unidad principal, que simplemente consistía en permitir a sus terminales conectarse a través de largas líneas alquiladas. Este método se usaba en los años 50 por el Proyecto RAND para apoyar a investigadores como Herbert Simon, en Pittsburgh (Pensilvania), cuando colaboraba a través de todo el continente con otros investigadores de Santa Mónica (California) trabajando en demostraciones de teoremas automatizadas e inteligencia artificial.

Un pionero fundamental en lo que se refiere a una red de comunicación mundial, fue J.C.R. Licklider, que comprendió la necesidad de una red mundial, según consta en su documento de enero, 1960, Man-Computer Symbiosis (Simbiosis Hombre-Computadora).

En octubre de 1962, Licklider fue nombrado jefe de la oficina de procesado de información DARPA, y empezó a formar un grupo informal dentro del DARPA del Departamento de Defensa de los Estados Unidos para investigaciones sobre ordenadores más avanzadas. Como parte del papel de la oficina de procesado de información, se instalaron tres terminales de redes: una para la System Development Corporation en Santa Monica, otra para el Proyecto Genie en la Universidad de California (Berkeley) y otra para el proyecto Multics en el Instituto Tecnológico de Massachusetts. La necesidad de Licklider de redes se haría evidente por los problemas que esto causó.

Como principal problema en lo que se refiere a las interconexiones estaba el conectar diferentes redes físicas para formar una sola red lógica. Durante los años 60, varios grupos trabajaron en el concepto de la conmutación de paquetes.

Normalmente se considera que Donald Davies (National Physical Laboratory), Paul Baran (Rand Corporation) y Leonard Kleinrock (MIT) lo han inventado simultáneamente.

Internet fue creada a partir de un proyecto del Departamento de Defensa de los Estados Unidos llamado ARPANET (Advanced Research Project Network según su sigla en ingles) fue iniciado en 1969 y cuyo principal propósito era la investigación y desarrollo de protocolos de comunicación para redes de área amplia, para ligar redes de transmisión de información de diferentes tipos; capaces de resistir las condiciones de operación más difíciles y continuar funcionando aún con la pérdida de una parte de la red.

Estas investigaciones dieron como resultado el protocolo TCP/IP (Transmission Control Protocol/Internet Protocol) un sistema de comunicaciones muy sólido y robusto bajo el cual se integran todas las redes que conforman lo que se conoce actualmente como Internet.

Durante el desarrollo de este protocolo se incrementó notablemente el número de redes locales de agencias gubernamentales y de universidades que participaban en el proyecto, dando origen así a la red de redes más grande del mundo, las funciones militares se separaron y se permitió el acceso a la red a todo aquel que lo requiriera sin importar de que país provenía la solicitud siempre y cuando fuera para fines académicos o de investigación (y por supuesto que pagara sus propios gastos de conexión), los usuarios pronto encontraron que la información que había en la red era por demás útil y si cada quien aportaba algo se enriquecería aún más el cúmulo de información existente.

Después de que las funciones militares de la red se separaron en una sub-red de Internet (llamada MILNET), la tarea de coordinar el desarrollo de la red recayó en varios grupos, uno de ellos, la National Science Foundation promovió el uso de la red ya que se encargo de conectar cinco centros de contención de información a los que se accedía desde cualquier nodo de la red. Debido a que el trafico de datos superó las cargas de información que se podía soportar, se dio la concesión a Merit Network Inc., para que administrara y actualizara la red, se mejoraron las líneas de comunicación dando un servicio mucho más rápido, pero este proceso de mejora nunca termina debido a la creciente demanda de los servicios que se encuentran en la red.

El enorme crecimiento de Internet se debe en parte a que es una red basada en fondos gubernamentales de cada país que forma parte de Internet lo que proporciona un servicio prácticamente gratuito. A principios de 1994 comenzó a darse un crecimiento explosivo de las compañías con propósitos comerciales en Internet, dando así origen a una nueva etapa en el desarrollo de la red.

La infraestructura de Internet se esparció por el mundo, para crear la moderna red mundial de computadoras que hoy conocemos. Atravesó los países occidentales e intentó una penetración en los países en desarrollo, creando un acceso mundial a información y comunicación sin precedentes, pero también una brecha digital en el acceso a esta nueva infraestructura. Internet también alteró la economía del mundo entero, incluyendo las implicaciones económicas de la burbuja de las .com. [4]

1.3 Evolución de las redes Informáticas

El desarrollo de las redes informáticas ha sido muy vertiginoso tomando en cuenta el relativo poco tiempo que estas han sido puestas a la disposición de la humanidad.

Las redes han evolucionado desde su creación y seguirán evolucionando a medida que la tecnología de conectividad que las soporte, siga evolucionando.

Esta evolución se ha llevado a cabo en los últimos 15 años y corresponde en mucho, al desarrollo de nuevas corrientes en la gestión de los Servicios Informáticos, el surgimiento de nuevos productos y tecnologías y a las nuevas utilidades que la computación y las redes presentan a la comunidad, las empresas y las instituciones en general.

En la actualidad se puede distinguir hasta tres tipos de generaciones en el desarrollo de las redes informáticas.

4.- Se utiliza para designar los nombres de dominio propios de entidades comerciales o empresariales.

1.3.1 Redes de Primera Generación

La primera generación de redes, se caracterizaba por utilizar tecnología propietaria del proveedor de los equipos. Se basaban en la tecnología de Barra o Bus (salvo en el caso de IBM, que proveía la tecnología de anillo o Token Ring), la cobertura era departamental y se administraba en forma local.

1.3.2 Redes de Segunda Generación

En esta segunda generación, las redes informáticas, se basan en estándares de tecnología, usando una topología estrella, soportadas en concentradores o Hub. Su área de influencia es empresarial, disponen en algunos casos de un ruteador central y se dispone de una capacidad de administración por segmentos.

1.3.3 Redes de Tercera Generación

La Tercera generación está sustentada en principios de:

Escalabilidad. Entendida por el crecimiento en el servicio a usuarios dentro de la institución (desde 5 usuarios a 50, luego a 100, para llegar a 1000 o más), así como la capacidad de implantar componentes complejos que permitan tal crecimiento.

Flexibilidad. Para adaptarse a la infraestructura civil de los locales y ambientes de la empresa y/o institución.

Seguridad. En la infraestructura de red y de sus componentes dentro de los ambientes e instalaciones.

Operabilidad. Soportada sobre principio de fácil instalación y manipulación de los componentes de la red informática.

Estas características podemos centrarlas en:

* Gran ancho de banda escalable
Servidores Centralizados
* Distribución switchada
* Cableado estructurado

1.4 Clasificación redes informáticas

La clasificación de las redes es muy amplia y se la puede hacer bajo diversos parámetros a continuación se tratara de abarcar la mayoría de ellas:

1.4.1 Red pública.

Una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.

1.4.2 Red privada.

Una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.

1.4.3 Red de área Personal (PAN): (Personal Area Network)

Es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora (teléfonos incluyendo las ayudantes digitales personales) cerca de una persona. Los dispositivos pueden o no pueden pertenecer a la persona en cuestión. El alcance de una PAN es típicamente algunos metros. Las PAN se pueden utilizar para la comunicación entre los dispositivos personales de ellos mismos (comunicación del intrapersonal), o para conectar con una red de alto nivel y el Internet (un up link). Las redes personales del área se pueden conectar con cables con los buses de la computadora tales como USB y FireWire. Una red personal sin hilos del área (WPAN) se puede también hacer posible con tecnologías de red tales como IrDA y Bluetooth.

1.4.4 Redes de Área Local (LAN)

Una LAN (Local Area Network) es un sistema de interconexión de equipos informáticos basado en líneas de alta velocidad (decenas o cientos de megabits por segundo).

Las principales tecnologías usadas en una LAN son: Ethernet, Token ring, ARCNET y FDDI

Un caso típico de este tipo de redes esta configurado con un equipo servidor de LAN desde el que los usuarios cargan las aplicaciones que se ejecutarán en sus estaciones de trabajo. Los usuarios pueden también solicitar tareas de impresión y otros servicios que están disponibles mediante aplicaciones que se ejecutan en el servidor.

Además pueden compartir ficheros con otros usuarios en el servidor. Los accesos a estos ficheros están controlados por un administrador de la LAN.

Su extensión esta limitada físicamente a un edificio o a un entorno de 200 metros pero con repetidores se podría llegar a la distancia de un kilómetro. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

Las estaciones de trabajo y los ordenadores personales en oficinas normalmente están conectados en una red LAN, lo que permite que los usuarios envíen o reciban archivos y compartan el acceso a los datos. Cada ordenador conectado a una LAN se llama un nodo.

Cada nodo (ordenador individual) en una LAN tiene su propia CPU con la cual ejecuta programas, pero también puede tener acceso a los datos y a los dispositivos en cualquier parte en la LAN. Esto significa que muchos usuarios pueden compartir dispositivos costosos, como impresoras láser, así como datos. Los usuarios logran también manejar la LAN para comunicarse entre ellos, enviando E-mail o chateando.

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

1.4.5 Redes Wlan

Es un sistema de comunicación de datos inalámbrico dúctil, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Manipula tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van logrando jerarquía en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central. También son muy populares en los hogares para compartir el acceso a Internet entre diversos ordenadores.

Existen dos tipos de redes inalámbricas: la "Ad-Hoc" y la "Infraestructure".

La primera es una conexión de tipo "punto a punto" en la que los clientes se enlazan directamente unos con otros simplemente envían los paquetes de información "al aire", con la expectativa de que estos lleguen al destinatario que al que originalmente fueron enviados.
En la red "Infraestructure" se utiliza un dispositivo llamado punto de acceso, que funciona como el switch tradicional. Envía directamente los paquetes de información a cada ordenador de la red. El switch incrementa la velocidad y eficiencia de la red.

1.4.6 Red del área del campus (CAN).

Se deriva a una red que conecta dos o más LANs los cuales deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.

1.4.7 Red de área metropolitana (MAN)

Una red que conecta dos o más redes locales pero no extiende más allá de los límites de la ciudad inmediata, o del área metropolitana. Las rebajadoras (routers) múltiples, los interruptores (switch) y los cubos están conectados para crear a una MAN.

1.4.8 Red interna

Dos o más redes o segmentos de la red conectados con los dispositivos que funcionan en la capa 3 (la capa de la "red") del modelo de la referencia básica de la OSI[5], tal como un router, el modelo OSI se estudiará mas adelante en este mismo capitulo en el punto 1.6 con mayor detalle.

Cualquier interconexión entre las redes del público, privadas, comerciales, industriales, o gubernamentales se puede también definir como red interna.

1.4.9 Internet

Una red interna específica, consiste en una interconexión mundial de las redes gubernamentales, académicas, públicas, y privadas basadas sobre el Advanced Research Projects Agency Network (ARPANET) desarrollado por WARRA del departamento de los EE.UU. de la defensa también a casa al World Wide Web (WWW) y designado el "Internet" con un capital "I" para distinguirlo de otros Internet Works genéricos.

1.4.10 Intranet

Una red interna que se limitan en alcance a una sola organización o entidad y que utilicen el TCP/IP Protocol Suite, el HTTP[6], el FTP[7], y los otros protocolos y software de red de uso general en el Internet. Intranets se puede también categorizar como el LAN, CAN, MAN, WAN

1.4.11 Extranet

Una red interna que se limitan en alcance a una sola organización o entidad pero que también han limitado conexiones a las redes de una o más generalmente, pero no necesariamente, organizaciones confiadas o entidades.

5.- Organización Internacional de Normalización/Interconexión de Sistemas Abiertos.
6.- Acrónimo de HyperText Transfer Protocol, protocolo de transferencia de hipertexto. Se utiliza en las transferencias de información de páginas en Internet, de tal forma que puedan ser visualizadas en un navegador o explorador
7.- Acrónimo de File Transfer Protocol, protocolo de transferencia de archivos que se utiliza en Internet y otras redes para transmitir archivos entre servidores o entre un usuario y un servidor.

Un extranet se puede también categorizar como CAN, MAN, WAN, u otro tipo de red, aunque, por la definición, un extranet no puede consistir en un solo LAN, porque un extranet debe tener por lo menos una conexión con una red exterior. Intranets y los extranets pueden o no pueden tener conexiones al Internet. Si está conectado con el Internet, el Intranet o el extranet se protege normalmente contra ser alcanzado del Internet sin la autorización apropiada. El Internet en sí mismo no se considera ser una parte del Intranet o del extranet, aunque el Internet puede servir como portal para el acceso a las porciones de un extranet.

1.4.12 Red de área amplia (WAN)

Es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, tales como compañías del teléfono.

Las tecnologías WAN funcionan generalmente en las tres capas más bajas del Modelo de referencia OSI: la capa física, la capa de transmisión de datos, y la capa de red.

1.4.2 Tipos de redes informáticas según su topología

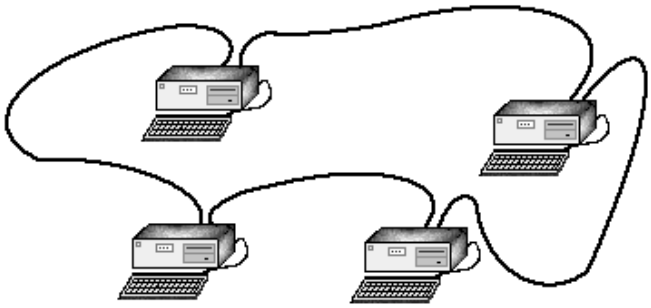
La topología se refiere a la forma en que están interconectados los distintos equipos (nodos) de una red. Un nodo es un dispositivo activo conectado a la red, como un ordenador o una impresora. Un nodo también puede ser dispositivo o equipo de la red como un concentrador, conmutador o un router.

Las topologías más usadas son:

1.4.2.1 Anillo

Tipo de LAN en la que los ordenadores o nodos están enlazados formando un círculo a través de un mismo cable. Las señales circulan en un solo sentido por el círculo, regenerándose en cada nodo. En la práctica, la mayoría de las topologías lógicas en anillo son en realidad una topología física en estrella.

Figura 1.1 Topología de red tipo Anillo

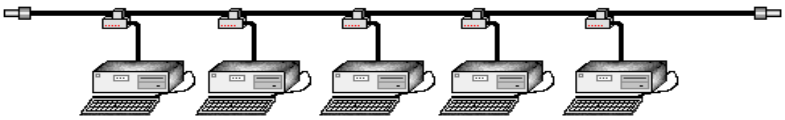


Fuente: http://www.gobiernodecanarias.org/educacion

1.4.2.2 Bus

Una topología de bus consiste en que los nodos se unen en serie con cada nodo conectado a un cable largo o bus, formando un único segmento A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo. Una rotura en cualquier parte del cable causará, normalmente, que el segmento entero pase a ser inoperable hasta que la rotura sea reparada.

Figura 1.2 Topología de red tipo Bus



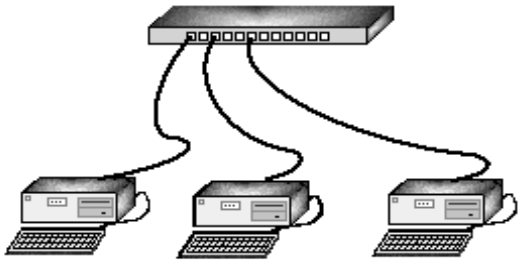
Fuente: http://www.gobiernodecanarias.org/educacion

1.4.2.3 Estrella

Esta topología es la más utilizada, la cual tiene en un extremo del segmento un nodo y al otro extremo un concentrador. La principal ventaja de este tipo de red es la fiabilidad, dado que si uno de los segmentos tiene una rotura, afectará sólo al nodo conectado en él.

Otros usuarios de los ordenadores de la red continuarán operando como si ese segmento no existiera. 10BASE-T Ethernet[8] y Fast Ethernet son ejemplos de esta topología.

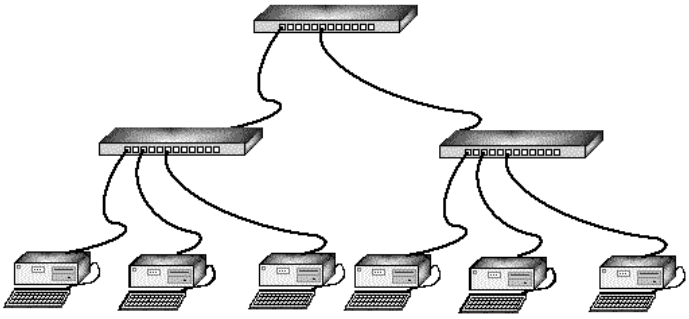
Figura 1.3 Topología de red tipo Estrella



Fuente: http://www.gobiernodecanarias.org/educacion

A la interconexión de varias subredes en estrella se le conoce con el nombre de topología en árbol.

Figura 1.4 Interconexión de varias subredes en estrella



Fuente: http://www.gobiernodecanarias.org/educacion

8.-Especificación de red de área local (LAN) desarrollada en 1976 por Xerox, en cooperación con DEC e Intel, originalmente para conectar los mini ordenadores del Palo Alto Research Center (EE.UU.).

1.4.3 Tipos de redes informáticas según su protocolo de bajo nivel

Se podría definir protocolo como el conjunto de normas que regulan la comunicación entre los distintos dispositivos de una red. Es como el lenguaje común que deben de usar todos los componentes para entenderse entre ellos. Los protocolos se clasifican en dos grupos: protocolos de bajo nivel que son los que se encargan de gestionar el tráfico de información por el cable, o sea a nivel físico, fundamentalmente definen las normas a nivel de software por las que se van a comunicar los distintos dispositivos de la red. Existen bastantes protocolos de bajo nivel como pueden ser Ethernet, Token Ring, FDDI, ATM, LocalTalk, etc. Aunque los más usados para implementaciones similares a la que nos ocupa en este estudio comparativo son los dos primeros:

1.4.3.1 Ethernet

Es el método de conexión más extendido porque permite un buen equilibrio entre velocidad, costo y facilidad de instalación. Todo esto combinado con su buena aceptación en el mercado y la facilidad de soportar prácticamente todos los protocolos de red, convierten a Ethernet en la tecnología ideal para la mayoría de las instalaciones de LAN.

Consigue velocidades de conexión de 10 Mbits/s aunque existen especificaciones de velocidades superiores como es el caso de Fast Ethernet que llega a conseguir hasta 100 Mbits/s.

1.4.3.2 Token Ring

Es un sistema bastante usado aunque mucho menos que Ethernet. Llega a conseguir velocidades de hasta 16 Mbits/s aunque también existen especificaciones para velocidades superiores. La topología lógica que usa es en anillo aunque en la práctica se conecta en una topología física en estrella, a través de concentradores llamados MAU (Multistation Access Unit). Es más fácil de detectar errores que en Ethernet. Cada nodo reconoce al anterior y al posterior. Se comunican cada cierto tiempo. Si existe un corte, el nodo posterior no recibe información del nodo cortado e informa a los demás de cual es el nodo inactivo.

1.4.3.3 IPX/SPX

IPX (*Internetwork Packet Exchange*) es un protocolo de Novell que interconecta redes que usan clientes y servidores Novell Netware. Es un protocolo orientado a paquetes y no orientado a conexión (esto es, no requiere que se establezca una conexión antes de que los paquetes se envíen a su destino). Otro protocolo, el SPX (*Sequenced Packet eXchange*), actúa sobre IPX para asegurar la entrega de los paquetes.

1.4.3.4 NetBIOS

NetBIOS (*Network Basic Input/Output System*) es un programa que permite que se comuniquen aplicaciones en diferentes ordenadores dentro de una LAN. Desarrollado originalmente para las redes de ordenadores personales IBM, fue adoptado posteriormente por Microsoft. NetBIOS se usa en redes con topologías Ethernet y token ring. No permite por si mismo un mecanismo de enrutamiento por lo que no es adecuado para redes de área extensa (MAN), en las que se deberá usar otro protocolo para el transporte de los datos, Ej. TCP.
Puede actuar como protocolo orientado a conexión o no (en sus modos respectivos *sesión* y *data grama*). En el modo sesión dos ordenadores establecen una conexión para establecer una conversación entre los mismos, mientras que en el modo data grama cada mensaje se envía de forma independiente.

Una de las desventajas de NetBIOS es que no proporciona un marco estándar o formato de datos para la transmisión.

1.4.3.5 NetBEUI

NetBIOS Extended User Interface o *Interfaz de Usuario para NetBIOS* es una versión mejorada de NetBIOS que sí permite el formato o arreglo de la información en una transmisión de datos. También desarrollado por IBM y adoptado después por Microsoft, es actualmente el protocolo predominante en las redes Windows NT, LAN Manager y Windows para Trabajo en Grupo.

Aunque NetBEUI es la mejor elección como protocolo para la comunicación dentro de una LAN, el problema es que no soporta el enrutamiento de mensajes hacia otras redes, que deberá hacerse a través de otros protocolos (por ejemplo, IPX o TCP/IP). Un método usual es instalar tanto NetBEUI como TCP/IP en cada estación de trabajo y configurar el servidor para usar NetBEUI para la comunicación dentro de la LAN y TCP/IP para la comunicación hacia afuera de la LAN.

1.4.3.6 AppleTalk

Es el protocolo de comunicación para ordenadores Apple Macintosh y viene incluido en su sistema operativo, de tal forma que el usuario no necesita configurarlo. Existen tres variantes de este protocolo:

LocalTalk. La comunicación se realiza a través de los puertos serie de las estaciones. La velocidad de transmisión es pequeña pero sirve por ejemplo para compartir impresoras.

Ethertalk. Es la versión para Ethernet. Esto aumenta la velocidad y facilita aplicaciones como por ejemplo la transferencia de archivos.

Tokentalk. Es la versión de Appletalk para redes Tokenring.

1.5 TCP/IP

Las siglas TCP/IP se refieren a dos protocolos de red, que son Transmission Control Protocol (Protocolo de Control de Transmisión) e Internet Protocol (Protocolo de Internet) respectivamente.
Estos protocolos pertenecen a un conjunto mayor de protocolos. Dicho conjunto se denomina suite TCP/IP.
Los diferentes protocolos de la suite TCP/IP trabajan conjuntamente para proporcionar el transporte de datos dentro de Internet (o Intranet). En otras palabras, hacen posible que accedamos a los distintos servicios de la Red. Estos servicios incluyen, transmisión de correo electrónico, transferencia de ficheros, grupos de noticias, acceso a la World Wide Web, etc.

Hay dos clases de protocolos dentro de la suite TCP/IP que son: protocolos a nivel de red y protocolos a nivel de aplicación.

1.5.1 TCP.

Controla la división de la información en unidades individuales de datos (llamadas paquetes) para que estos paquetes sean encaminados de la forma más eficiente hacia su punto de destino. En dicho punto, TCP se encargará de reensamblar dichos paquetes para reconstruir el fichero o mensaje que se envió. Por ejemplo, cuando se nos envía un fichero HTML desde un servidor Web, el protocolo de control de transmisión en ese servidor divide el fichero en uno o más paquetes, numera dichos paquetes y se los pasa al protocolo IP. Aunque cada paquete tenga la misma dirección IP de destino, puede seguir una ruta diferente a través de la red. Del otro lado el programa cliente en el computador, TCP reconstruye los paquetes individuales y espera hasta que hayan llegado todos para presentárnoslos como un solo fichero.

1.5.2 IP.

Se encarga de repartir los paquetes de información enviados entre el ordenador local y los ordenadores remotos.

Esto lo hace etiquetando los paquetes con una serie de información, entre la que cabe destacar las direcciones IP de los dos ordenadores. Basándose en esta información, IP garantiza que los datos se encaminarán al destino correcto. Los paquetes recorrerán la red hasta su destino (que puede estar en el otro extremo del planeta) por el camino más corto posible gracias a unos dispositivos denominados encaminadores o routers.

1.5.3 Breve Historia del Protocolo TCP/IP

A principios de los años 60, varios investigadores intentaban encontrar una forma de compartir recursos informáticos de una forma más eficiente. En 1961, Leonard Klienrock introduce el concepto de *Conmutación de Paquetes* (*Packet Switching*, en inglés). La idea era que la comunicación entre ordenadores fuese dividida en *paquetes*.

Cada paquete debería contener la dirección de destino y podría encontrar su propio camino a través de la red.

En 1969 la Agencia de Proyectos de Investigación Avanzada (Defense Advanced Research Projects Agency o DARPA) del Ejército de los EE.UU. desarrolla la ARPAnet. La finalidad principal de esta red era la capacidad de resistir un ataque nuclear de la URSS para lo que se pensó en una administración descentralizada.

De este modo, si algunos ordenadores eran destruidos, la red seguiría funcionando. Aunque dicha red funcionaba bien, estaba sujeta a algunas caídas periódicas del sistema. De este modo, la expansión a largo plazo de esta red podría resultar difícil y costosa. Se inició entonces una búsqueda de un conjunto de protocolos más fiables para la misma.

Dicha búsqueda finalizó, a mediados de los 70, con el desarrollo de TCP/IP. TCP/IP tenia (y tiene) ventajas significativas respecto a otros protocolos. Por ejemplo, consume pocos recursos de red. Además, podía ser implementado a un coste mucho menor que otras opciones disponibles entonces.

Gracias a estos aspectos, TCP/IP comenzó a hacerse popular. En 1983, TCP/IP se integró en la versión 4.2 del sistema operativo UNIX de Berkeley y la integración en versiones comerciales de UNIX vino pronto. Así es como TCP/IP se convirtió en el estándar de Internet.

En la actualidad, TCP/IP se usa para muchos propósitos, no solo en Internet. Por ejemplo, a menudo se diseñan *intranets* usando TCP/IP. En tales entornos, TCP/IP ofrece ventajas significativas sobre otros protocolos de red. Una de tales ventajas es que trabaja sobre una gran variedad de hardware y sistemas operativos. De este modo puede crearse fácilmente una red heterogénea usando este protocolo. Dicha red puede contener estaciones Mac, PC compatibles, estaciones Sun, servidores Novell, etc. Todos estos elementos pueden comunicarse usando la misma suite de protocolos TCP/IP.

1.5.4 Cómo Trabaja TCP/IP

TCP/IP opera a través del uso de una pila. Dicha pila es la suma total de todos los protocolos necesarios para completar una transferencia de datos entre dos máquinas (así como el camino que siguen los datos para dejar una máquina o entrar en la otra). La pila está dividida en capas, como se ilustra en la siguiente figura:

Tabla 1.1 Equipo Servidor o Cliente

Capa de Aplicaciones	Cuando un usuario inicia una transferencia de datos, esta capa pasa la solicitud a la Capa de Transporte.
Capa de Transporte	La Capa de Transporte añade una cabecera y pasa los datos a la Capa de Red.
Capa de Red	En la Capa de Red, se añaden las direcciones IP de origen y destino para el enrutamiento de datos
Capa de Enlace de Datos	Ejecuta un control de errores sobre el flujo de datos entre los protocolos anteriores y la Capa Física
Capa Física	Ingresan o salen los datos a través del medio físico, que puede ser Ethernet vía coaxial, PPP vía módem, etc.

Autor: Gabriel Sebastián Proaño B.

Después de que los datos han pasado a través del proceso ilustrado en la tabla 1.1, viajan a su destino en otra máquina de la red.

Allí, el proceso se ejecuta al revés (los datos entran por la capa física y recorren la pila hacia arriba). Cada capa de la pila puede enviar y recibir datos desde la capa adyacente. Cada capa está también asociada con múltiples protocolos que trabajan sobre los datos.

Protocolos a Nivel de Aplicación

Aquí se encuentran los protocolos asociados a los distintos servicios de Internet, como FTP, Telnet, Gopher, HTTP, etc. Estos protocolos son visibles para el usuario en alguna medida. Por ejemplo, el protocolo FTP (File Transfer Protocol) es visible para el usuario. El usuario solicita una conexión a otro ordenador para transferir un fichero, la conexión se establece, y comienza la transferencia. Durante dicha transferencia, es visible parte del intercambio entre la máquina del usuario y la máquina remota (mensajes de error y de estado de la transferencia, como por ejemplo cuantos bytes del fichero se han transferido en un momento dado).

1.5.5 DNS

El DNS (Domain Name System, o Sistema de Nombres de Dominio) es un sistema hace corresponder a la dirección IP de cada host de Internet un único nombre de dominio, para que podamos acceder a dicho host con mayor facilidad.

1.5.6 Dominio.

Representa el primer nivel en la estructura de nombres de dominio. Existen dos tipos de dominios: territoriales y genéricos. Un dominio territorial normalmente indica el país donde está situado el ordenador (por ejemplo **es** se refiere a España), mientras que uno genérico alude a la clase de organización a la que pertenece (por ejemplo, **com.** nos informa de que el ordenador pertenece a una institución comercial).

Las dos tablas que figuran a continuación ofrecen un listado de los dominios territoriales y genéricos más usuales:

Tabla 1.2. Dominios territoriales y genéricos más usuales

Dominio Territorial	**País**	**Dominios Genéricos**	**Institución**
de	Alemania	com	Comercial
uk	Reino unido	net	Recursos de red
se	Suecia	org	Otras organizaciones
dk	Dinamarca	edu	Académica
au	Australia	gov	Gubernamental (no militar)
nl	Países Bajos	mil	Militar
jp	Japón		
ch	Suiza		
ar	Argentina		
it	Italia		
br	Brasil		
nz	Nueva Zelanda		
za	Sudáfrica		
at	Austria		
fr	Francia		
ec	Ecuador		

Fuente: http://www.gobiernodecanarias.org/educacion

Una observación: no se suele utilizar el dominio territorial **us**, esto es porque los ordenadores de los Estados Unidos de América pertenecen normalmente a un dominio genérico.

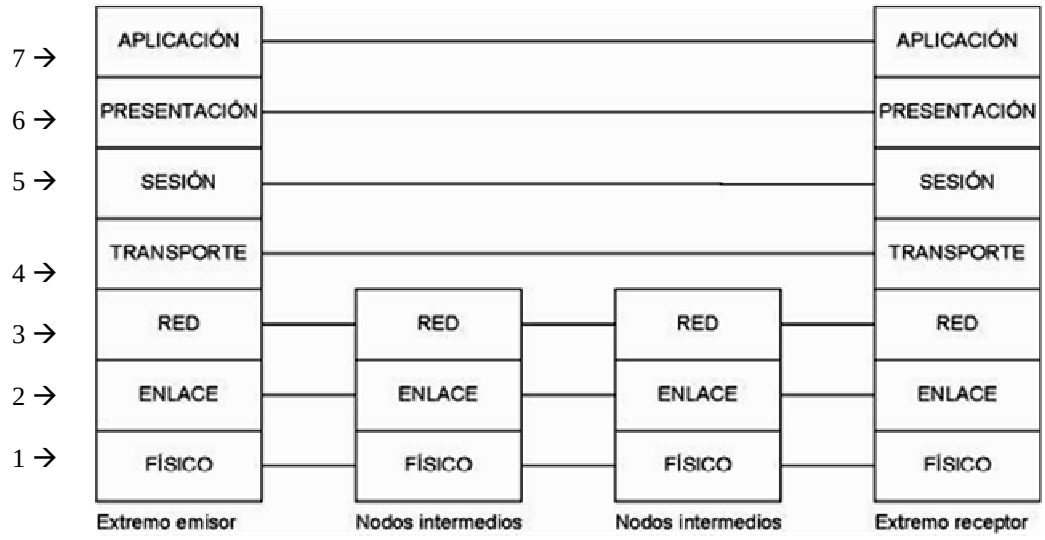
1.6 Arquitectura redes informáticas

El modelo OSI (Open Systems Interconnection) es la propuesta que hizo la Organización Internacional para la Estandarización (ISO) con el fin de estandarizar la interconexión de sistemas abiertos.

Un sistema abierto se refiere a que es independiente de una arquitectura específica. Se compone el modelo, por tanto, de un conjunto de estándares ISO relativos a las comunicaciones de datos.

El modelo en sí mismo no puede ser considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, sino que suele hablarse de modelo de referencia. Por tanto, al hablar de Arquitectura de Redes hablaremos del conjunto de Arquitecturas definibles según el modelo estándar OSI. Este modelo está dividido en siete capas:

Figura 1.5. Modelo OSI



Fuente: http://es.wikipedia.org

A continuación se presenta una descripción de cada una de las capas las cuales han sido divididas de la siguiente manera:

1 Capa Física
1.1 Codificación de la señal
1.2 Topología y medios compartidos
1.3 Equipos adicionales
2 Capa de enlace de datos
3 Capa de red
4 Capa de transporte
5 Capa de sesión
6 Capa de presentación
7 Capa de aplicación

1.6.1 Capa Física

La Capa Física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio (cable conductor, fibra óptica o inalámbrico); características del medio (tipo de cable o calidad del mismo); tipo de conectores normalizados o en su caso tipo de antena; etc.; como a la forma en la que se transmite la información (codificación de señal, niveles de tensión/corriente eléctrica, modulación, tasa binaria, etc.)
Envía los bits de información a través del medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si esta es uni o bidireccional (simplex, duplex o full-duplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas.

También se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable); o electromagnéticos.

Estos últimos, dependiendo de la frecuencia /longitud de onda de la señal pueden ser ópticos, de micro-ondas o de radio.
Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados, coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

1.6.1.1 Codificación de la señal

El nivel físico recibe una trama binaria que debe convertir a una señal electro magnética, de tal forma que a pesar de la degradación que pueda sufrir en el medio de transmisión vuelva a ser interpretable correctamente en el receptor.

En el caso más sencillo el medio es directamente digital, como en el caso de las fibras ópticas, dado que por ellas se transmiten pulsos de luz.

Cuando el medio no es digital hay que codificar la señal, en los casos más sencillos la codificación puede ser por pulsos de tensión (PCM o Pulse Code Modulatión) (por ejemplo 5 voltios para los "unos" y 0 voltios para los "ceros"), es lo que se llaman codificación unipolar NRZ. Otros medios se codifican mediante presencia o ausencia de corriente. En

general estas codificaciones son muy simples y no apuran bien la capacidad de medio. Cuando se quiere sacar más partido al medio se usan técnicas de modulación más complejas, y suelen ser muy dependientes de las características del medio concreto.

En los casos más complejos, como suelen ser las comunicaciones inalámbricas, se pueden dar modulaciones muy sofisticadas, este es el caso de los estándares Wi-Fi, con técnicas de modulación complejas de espectro ensanchado.

1.6.1.2 Topología y medios compartidos

Indirectamente el tipo de conexión que se haga en la capa física puede influir en el diseño de la capa de Enlace. Atendiendo al número de equipos que comparten un medio hay dos posibilidades:

Conexiones punto a punto: que se establecen entre dos equipos y que no admiten ser compartidas por terceros
Conexiones multipunto: en las que dos o más equipos pueden usar el medio.
Así por ejemplo la fibra óptica no permite fácilmente conexiones multipunto y por el contrario las conexiones inalámbricas son inherentemente multipunto. Hay topologías como el anillo, que permiten conectar muchas máquinas a partir de una serie de conexiones punto a punto.

La técnica utilizada para lograr que los nodos sobre la red, accedan el cable ó medio de comunicación y evitar que dos o más estaciones intenten transmitir simultáneamente es trabajo del nivel 2, la capa de enlace.

1.6.1.3 Equipos adicionales

A la hora de diseñar una red hay equipos adicionales que pueden funcionar a nivel físico: los repetidores amplifican la señal, pudiendo también regenerarla. En las redes Ethernet con la opción de cableado de par trenzado (la más común hoy por hoy) se emplean unos equipos de interconexión llamados hubs que convierten una topología física en estrella en

un bus lógico y que actúan exclusivamente a nivel físico, a diferencia de los conmutadores (switches) que actúan a nivel de enlace.

1.6.2 Capa de enlace de datos

A partir de cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También debe incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.

Ejemplos: Ethernet, Token Ring, ATM.

1.6.3 Capa de red

El cometido de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Es decir que se encarga de encontrar un camino manteniendo una tabla de enrutamiento y atravesando los equipos que sea necesario, para hacer llegar los datos al destino. Los equipos encargados de realizar este encaminamiento se denominan en castellano encaminadores, aunque es más frecuente encontrar el nombre inglés routers y, en ocasiones enrutadores.
Adicionalmente la capa de red debe gestionar la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red (similar a un atasco en un cruce importante en una ciudad).

1.6.4 Capa de transporte

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas unidades si es necesario, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación.

Otra característica a destacar es que debe aislar a las capas superiores de las distintas posibles implementaciones de tecnologías de red en las capas inferiores, lo que la convierte en el corazón de la comunicación.

En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes. Estos servicios estarán asociados al tipo de comunicación empleada, la cual puede ser diferente según el requerimiento que se le haga a la capa de transporte. Por ejemplo, la comunicación puede ser manejada para que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío. Una de las dos modalidades debe establecerse antes de comenzar la comunicación para que una sesión determinada envíe paquetes, y ése será el tipo de servicio brindado por la capa de transporte hasta que la sesión finalice.

De la explicación del funcionamiento de esta capa se desprende que no está tan encadenada a capas inferiores como en el caso de las capas 1 a 3, sino que el servicio a prestar se determina cada vez que una sesión desea establecer una comunicación. Todo el servicio que presta la capa está gestionado por las cabeceras que agrega al paquete a transmitir.

Para finalizar, podemos definir a la capa de transporte como aquella capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la destino, independizándolo del tipo de red física que se esté utilizando.

1.6.5 Capa de sesión

Esta capa ofrece varios servicios que son cruciales para la comunicación, como son:

Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta).
Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo).

Mantener puntos de verificación (checkpoints), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio.
Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción.

1.6.6 Capa de presentación

Esta capa se encarga de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, unicode, EBCDIC), números (little-endian tipo intel, big-endian tipo motorola), sonido o imágenes; los datos lleguen de manera reconocible.

Para conseguir este objetivo se describió una posible notación de sintaxis abstracta (ASN.1), que en realidad se utiliza internamente en los MIB de SNMP (protocolo de gestión de red, para supervisar equipos de comunicaciones a distancia).

Esta capa es la primera en trabajar más el contenido de la comunicación que cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Son ejemplos claros datos transmitidos en ASCII a un receptor que utiliza EBCDIC, como en el caso de los mainframes de IBM, o la utilización de diferentes normas de punto flotante o aritméticas de complemento para representar los enteros.

Por lo tanto, se puede resumir a esta capa como la encargada de manejar las estructuras de datos abstractos y realizar las conversiones de representación de datos necesarios para la correcta interpretación de los mismos.

1.6.7 Capa de aplicación

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros. Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así por ejemplo un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en html, ni lee directamente el código html/xml.

Entre los protocolos más conocidos destacan:

- HTTP (HyperText Transfer Protocol) el protocolo bajo la WWW
- FTP (File Transfer Protocol) (FTAM, fuera de TCP-IP) transferencia de ficheros
- SMTP (Simple Mail Transfer Protocol) (X.400 fuera de tcp/ip) envío y distribución de correo electrónico
- POP (Post Office Protocol)/IMAP: reparto de correo al usuario final
- SSH (Secure SHell) principalmente terminal remoto, aunque en realidad cifra casi cualquier tipo de transmisión.
- Telnet otro terminal remoto, ha caído en desuso por su inseguridad intrínseca, ya que las claves viajan sin cifrar por la red.

Hay otros protocolos de nivel de aplicación que facilitan el uso y administración de la red:

- SNMP (Simple Network Management Protocol)
- DNS (Domain Name Server)

Casi todas las aplicaciones descritas comparten la arquitectura cliente-servidor, aunque hay otros paradigmas minoritarios como las redes P2P, los sistemas maestro-esclavo o el modelo RPC de Sun.

CAPITULO II

REDES LAN

2.1 Introducción redes Lan

LAN son las siglas de Local Area Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

Su extensión esta limitada físicamente a un edificio o a un entorno de 200 metros o con repetidores podríamos llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

Las estaciones de trabajo y los ordenadores personales en oficinas normalmente están conectados en una red LAN, lo que permite que los usuarios envíen o reciban archivos y compartan el acceso a los archivos y a los datos. Cada ordenador conectado a una LAN se llama un nodo.

Cada nodo (ordenador individual) en un LAN tiene su propia CPU con la cual ejecuta programas, pero también puede tener acceso a los datos y a los dispositivos en cualquier parte de la LAN. Esto significa que muchos usuarios pueden compartir dispositivos caros, como impresoras láser, así como datos. Los usuarios pueden también utilizar la LAN para comunicarse entre ellos, enviando E-mail o chateando.

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

2.2 Historia

Las primeras LAN fueron creadas a finales de los años 1970 y se solían crear líneas de alta velocidad para conectar grandes ordenadores centrales a un solo lugar. Muchos de los sistemas fiables creados en esta época, como Ethernet y ARCNET, fueron los más populares.

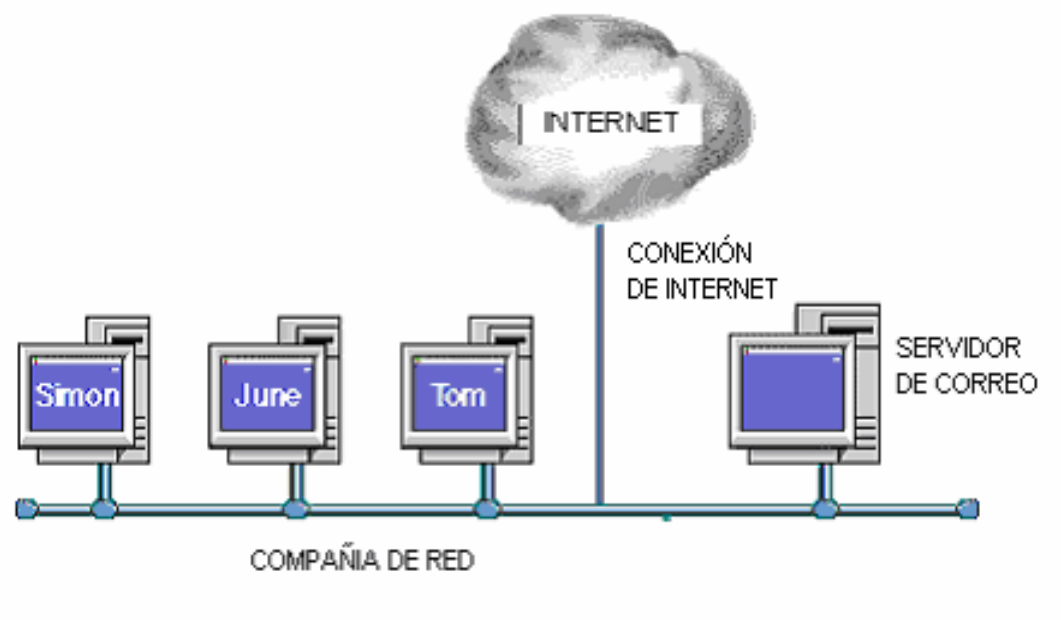
El crecimiento CP/M y DOS basados en el ordenador personal significaron que en un lugar físico existieran docenas o incluso cientos de ordenadores. La intención inicial de conectar estos ordenadores fue, generalmente, compartir espacio de disco e impresoras láser, pues eran muy caros en este tiempo. Había muchas expectativas en este tema desde 1983 y la industria informática declaró que el siguiente año sería “El año de las Lan”.

En realidad esta idea fracasó debido a la proliferación de incompatibilidades de la capa física y la implantación del protocolo de red, y la confusión sobre la mejor forma de compartir los recursos. Lo normal es que cada vendedor tuviera tarjeta de red, cableado, protocolo y sistema de operación de red. Con la aparición de Netware surgió una nueva solución, la cual ofrecía: soporte imparcial para los más de cuarenta tipos existentes de tarjetas, cables y sistemas operativos mucho más sofisticados que los que ofrecían la mayoría de los competidores. Netware dominaba el campo de las Lan de los ordenadores personales desde antes de su introducción en 1983 hasta mediados de los años 1990, cuando Microsoft introdujo Windows NT Advance Server y Windows for Workgroups.

De todos los competidores de Netware, sólo Banyan VINES tenía poder técnico comparable, pero Banyan ganó una base segura. Microsoft y 3Com trabajaron juntos para crear un sistema operativo de red simple el cual estaba formado por la base de 3Com's 3+Share, el Gestor de redes Lan de Microsoft y el Servidor del IBM. Ninguno de estos proyectos fue muy satisfactorio.

2.3 Diseño

Figura 2.1.Diseño Red Lan



Fuente: http://www.monografias.com

2.3.1 Análisis para el Diseño de una Red de Área Local

Topología:

Las topologías describen la red físicamente y también nos dan información acerca de el método de acceso que se usa (Ethernet, Token Ring, etc.).

Perdida de las Datos:

La pérdida de datos es producida por algún virus o por otro tipo de incidencia, los mas comunes son mal manejo por parte del usuario o personas inescrupulosas que acceden al sistema o mediante Internet, estos incidentes pueden evitarse de tal manera que en las estaciones de trabajo se instalan códigos para que así tengan acceso solo personal autorizado, en cuanto a Internet hay muchos software en el mercado mejor conocidos como Muros de fuego, que sirve para detener a los intrusos.

Caídas Continuas de la Red:

La caída continua en una Red se debe en la mayoría de los casos a una mala conexión Servidor > Concentrador o la conexión existente con el proveedor de Internet.

En el procesamiento de la información es muy lento:

Cuando el procesamiento de información de una Red es muy lento tenemos que tomar en cuenta el tipo de Equipos que elegimos, (Servidor, Cableado, Concentrador, Estaciones de Trabajo y otros, ya que si tomamos una decisión errónea perderemos tanto tiempo como dinero.

2.3.2 Protocolos a usar

TCP/IP:

Se refiere a los dos protocolos que trabajan juntos para transmitir datos: el Protocolo de Control de Transmisión (TCP) y el Protocolo Internet (IP). Cuando se envía información a través de Intranet, los datos se fragmentan en pequeños paquetes. Los paquetes llegan a su destino, se vuelven a fusionar en su forma original. El Protocolo de Control de Transmisión divide los datos en paquetes y los reagrupa cuando se reciben. El Protocolo Internet maneja el encaminamiento de los datos y asegura que se envían al destino exacto.

Norma EIA/TIA 568:

ANSI/TIA/EIA-568-A (Alambrado de Telecomunicaciones para Edificios Comerciales)
Este estándar define un sistema genérico de alambrado de telecomunicaciones para edificios comerciales que puedan soportar un ambiente de productos y proveedores múltiples.
El propósito de este estándar es permitir el diseño e instalación del cableado de telecomunicaciones contando con poca información acerca de los productos de telecomunicaciones que posteriormente se instalarán. La instalación de los sistemas de cableado durante el proceso de instalación y/o remodelación son significativamente más baratos e implican menos interrupciones que después de ocupado el edificio.

El propósito de esta norma es permitir la planeación e instalación de cableado de edificios comerciales con muy poco conocimiento de los productos de telecomunicaciones que serán instalados con posterioridad. La instalación de sistemas de cableado durante la construcción o renovación de edificios es significativamente menos costosa y desorganizadora que cuando el edificio está ocupado.

Alcance

La norma EIA/TIA 568A específica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. Se hacen recomendaciones para:

- Las topología
- La distancia máxima de los cables
- El rendimiento de los componentes
- Las tomas y los conectores de telecomunicaciones

Se pretende que el cableado de telecomunicaciones especificado soporte varios tipos de edificios y aplicaciones de usuario. Se asume que los edificios tienen las siguientes características:

- Una distancia entre ellos de hasta 3 Km.
- Un espacio de oficinas de hasta 1,000,000 m2
- Una población de hasta 50,000 usuarios individuales

Las aplicaciones que emplean los sistemas de cableado de telecomunicaciones incluyen, pero no están limitadas a:

- Voz , Datos, Texto, video, Imágenes

La vida útil de los sistemas de cableado de telecomunicaciones especificados por esta norma debe ser mayor de 10 años.

Las normas EIA/TIA es una de las mejores Normas por sus Antecedentes que son: Voz, Dato, video, Control y CCTV

Entre las utilidades y funciones tenemos un sistema de cableado genérico de comunicaciones para edificios comerciales. Medios, topología, puntos de terminación y conexión, así como administración, bien definidos. Un soporte para entornos multi proveedor multi protocolo. Instrucciones para el diseño de productos de comunicaciones para empresas comerciales. Capacidad de planificación e instalación del cableado de comunicaciones para un edificio sin otro conocimiento previo que los productos que van a conectarse.

Beneficios:

Flexibilidad, Asegura compatibilidad de Tecnologías, Reduce Fallas, Traslado, adiciones y cambios rápidos

2.3.3 Plataforma a utilizar

Se usa Windows XP dada la compatibilidad entre aplicaciones y hardware la confiabilidad de dicho sistema y puesto que las actualizaciones mas recientes incluidas en este sistema operativo superan en largo a sistemas operativos anteriores a Windows XP.

2.3.4 Determinación de los Equipos a utilizar en una Red de Área Local.

- Estaciones de Trabajo:

Es un dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información. Estos permiten que los usuarios intercambien rápidamente información y en algunos casos, compartan una carga de trabajo.

Generalmente nos enfocamos en los ordenadores más costosos ya que poseen la última tecnología, pero para el diseño de una Red de Área Local solamente necesitamos unas estaciones que cumpla con los requerimientos exigidos, hay que tener cuidado de no equivocarse ya que si erramos comprando un computador que no cumpla los requerimientos perderemos tiempo y dinero.

- Switch o (HUB):

Es el dispositivo encargado de gestionar la distribución de la información del Servidor (HOST), a las Estaciones de Trabajo y/o viceversa. Las computadoras de la Red envían la dirección del receptor y los datos al HUB, que conecta directamente los ordenadores emisor y receptor. Hay que tener cuidado cuando se elige un tipo de concentrador (HUB), los mismos se clasifican en 3 categorías.

- Switch para Grupos de Trabajo:

Un Switch para grupo de trabajo conecta un grupo de equipos dentro de su entorno inmediato.

- Switchs Intermedios:

Se encuentra típicamente en el closet de comunicaciones de cada planta. Los cuales conectan los Concentradores de grupo de trabajo. (Ellos pueden ser Opcionales)

- Switch Corporativos:

Representa el punto de conexión central para los sistemas finales conectados los concentradores intermedios. (Concentradores de Tercera Generación).

- Tarjetas Ethernet (Red):

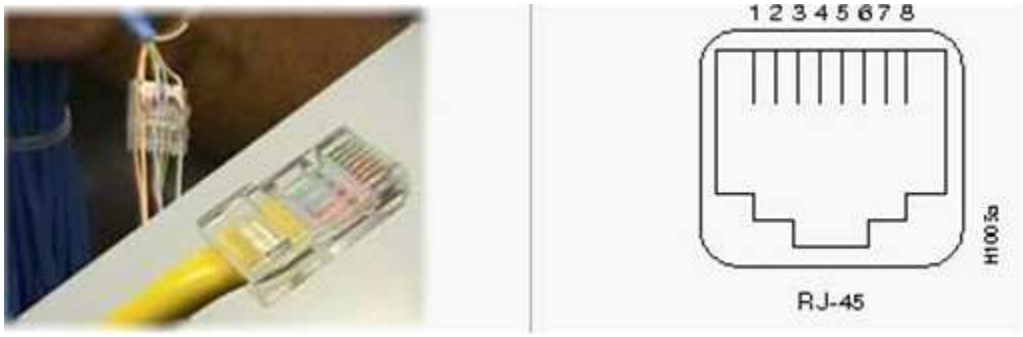
La tarjeta de Red es aquella que se encarga de interconecta las estaciones de trabajo con el concentrador y a su vez con el Servidor (HOST).

Otros:

- Conectores RJ45:

Es un acoplador utilizado para unir cables o para conectar un cable adecuado en este caso se Recomienda los conectores RJ45.

Figura 2.2. Conectores RJ45

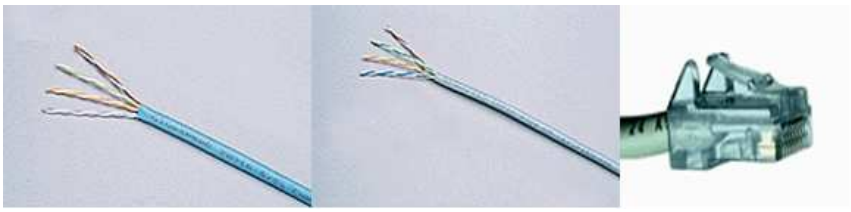


Fuente: http://www.monografias.com

- Cableado:

Es el medio empleado para trasmitir la información en la Red, es decir el medio de interconexión entre las estaciones de trabajo. Para el cableado es muy recomendado el Cable par trenzado Nivel Nº 5 sin apantallar.

Figura 2.3. Cable par trenzado Nivel Nº 5



Fuente: http://www.monografias.com

Figura 2.4. Nexxt Crimping Tool RJ45 o (Ponchador)

Fuente: http://www.monografias.com

2.3.5 Pasos a Seguir para la Construcción y Configuración de una Red

Los pasos que se han de seguir para la construcción de la Red son los aquí mencionados.

Diseñar la Red:

1. Dibujar un diagrama de la casa o la oficina donde se encuentra cada equipo e impresora. O bien, puede crear una tabla donde figure el hardware que hay en cada equipo.
2. Determinar que tipo de Hardware tiene cada equipo.

3. Junto a cada equipo, anotar el hardware, como módems y adaptadores de red, que tiene cada equipo.

4. Elegir el servidor determinado para la conexión con las estaciones de trabajo.

5. Determinar el tipo de adoptadores de red, que se necesita para la red domestica o de oficina.

6. Medición del espacio entre las estaciones de trabajo y el servidor:

En este espacio se medirá la distancia que existe entre las estaciones de trabajo y el servidor (host), con un metro, esto se hace para evitar excederse en los metros establecidos para dicha construcción.

7. Colocación de las canaletas plástica:

Para la colocación de las canaletas plástica simplemente tomaremos las medidas establecidas, cortaremos las canaletas, colocaremos los ramplus en la pared y atornillaremos las canaletas plásticas con los tornillos tira fondo.

8. Medición del cableado:

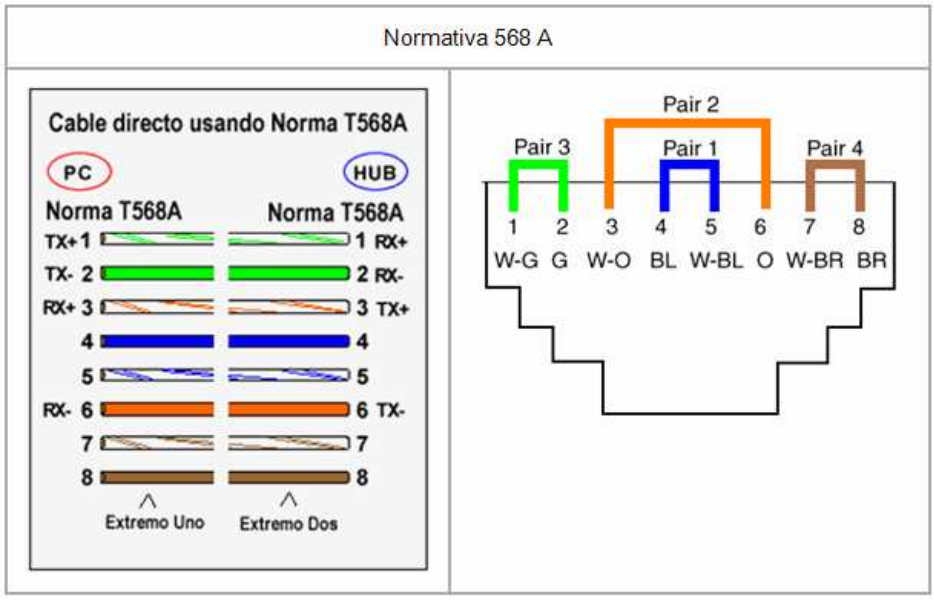
Se realiza el mismo procedimiento que con las canaletas, se toman las medidas del cableado para evitar el exceso de cables entre las estaciones de trabajo.

10. Conexión del cableado a los conectores:

En la conexión para los conectores necesitaremos: el cable conector, los conectores rj45 y un ponchador. El primer paso será tomar el cable colocarlo al final del ponchador, luego procederemos a desgarrarlo (pelarlo), el siguiente paso será cortarlo en línea recta es decir todos deben quedar parejos, ya que si esto no sucede tendremos una mala conexión y algunos contactos quedaran mas largos que otros. Bien proseguiremos a introducir el primer par de de cables

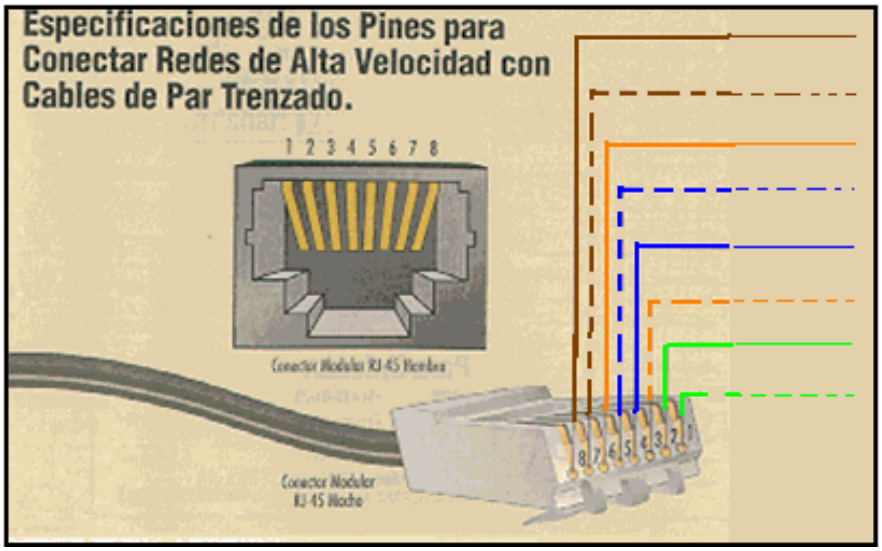
Primero se examinaran las normativas ya que esto es indispensable para el buen funcionamiento de la red.

Figura 2.5. Normativa 568 A



Fuente: http://www.monografias.com

Figura 2.6. Especificaciones de los pines para conectar redes de Alta Velocidad



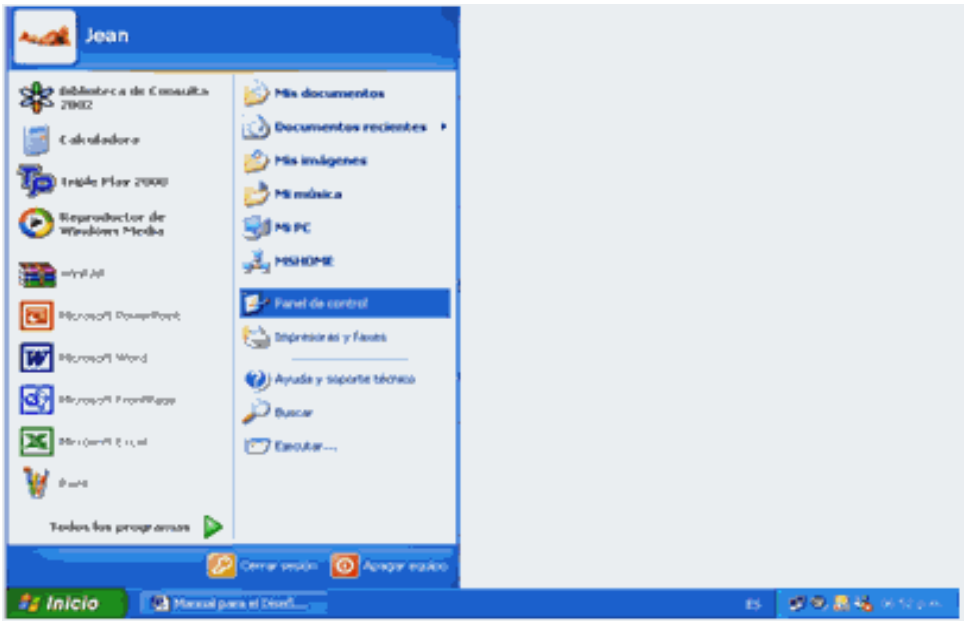
Fuente: http://www.monografias.com

Configuración de las Tarjetas de Red:

2.3.5.1 Pasos para la conexión de la tarjeta de red

Para la conexión de la tarjeta de Red, dar un click en la Barra del Menú de Inicio. Ubicar el puntero del mouse en la solapa de panel de control y hacer un click.

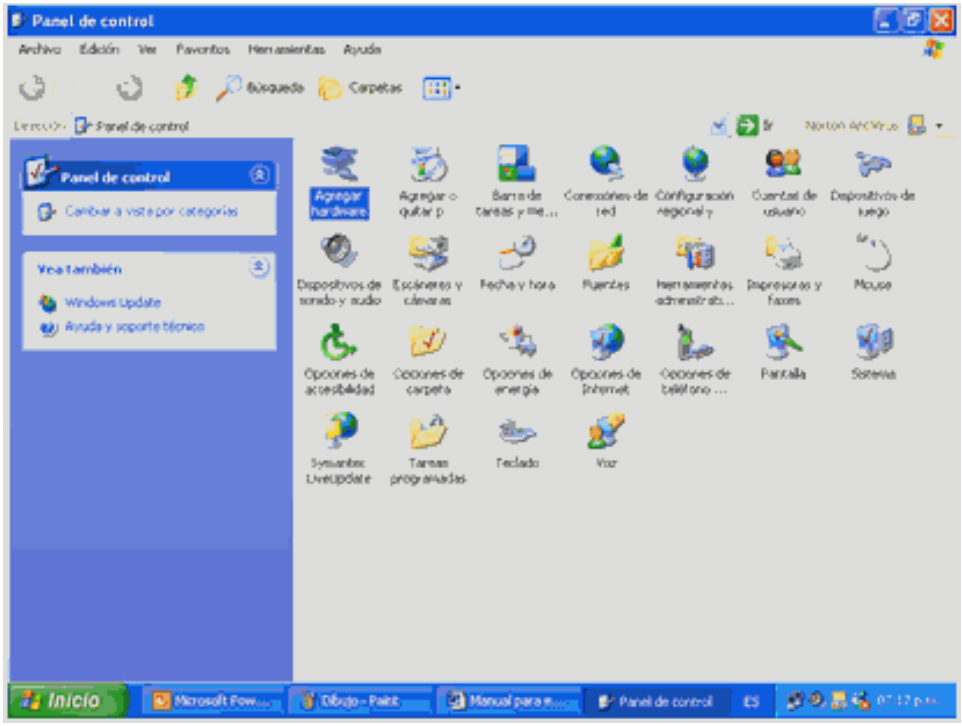
Figura 2.7. Solapa Panel de Control



Autor: Gabriel Sebastián Proaño B

A continuación ubicar el incono de agregar nuevo hardware, hacer un doble click para abrir el menú agregar nuevo hardware.

Figura 2.8. Selección icono agregar hardware



Autor: Gabriel Sebastián Proaño B

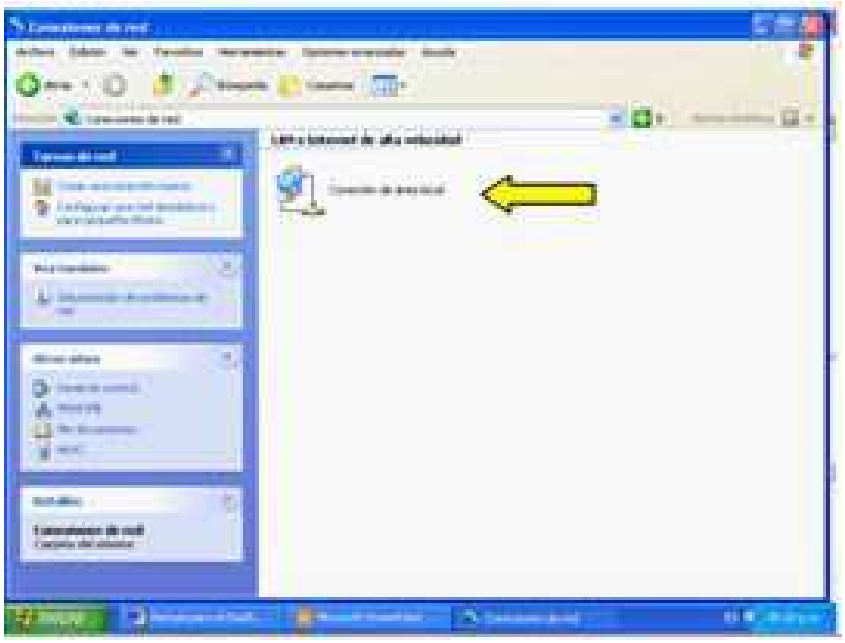
De allí en adelante seguir los procedimientos que indica el computador.

Actualmente las nuevas plataformas de Windows detectan automáticamente las tarjetas de red no hace falta configurarlas a menos que dicha plataforma no contenga el controlador requerido para dicha tarjeta.

Para la configuración del host se debe de proporcionar algunos protocolos que exige el ordenador para comenzar a programar el servidor así como las estaciones de trabajo. Hay que ser cuidadosos ya que un error traerá como resultado un gasto innecesario de tiempo y un mal funcionamiento en la red, podría traer consecuencias como un colapso.

Para la configuración de los protocolos (IP), la máscara de subred y la puerta de enlace, tendremos que abrir la ventana conexiones de red ubicada en el panel de control.

Figura 2.9. Ventana Conexiones de Red



Autor: Gabriel Sebastián Proaño B

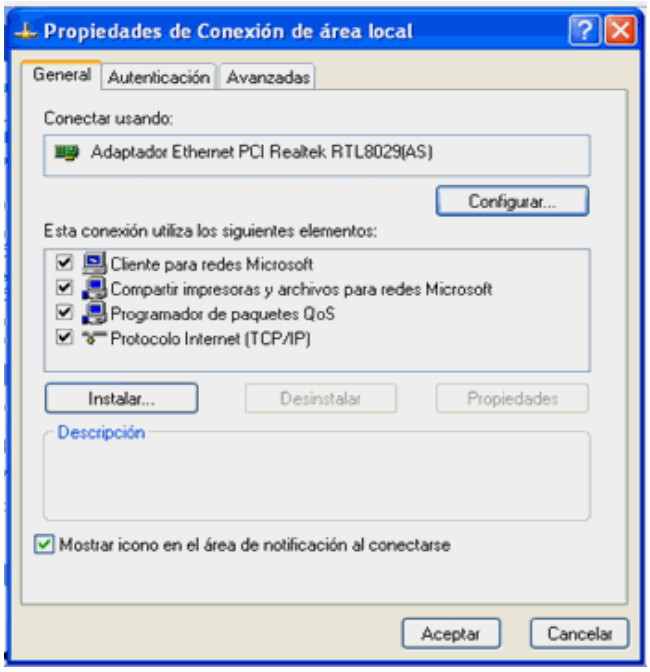
Dar un click con el botón derecho del mouse en el icono conexión de área local. Luego de haber hecho esto aparecerá una pequeña ventana, que dirá estado de conexión de área local.

Figura 2.10. Ventana Estado Conexión de área local

Autor: Gabriel Sebastián Proaño B

Luego que aparezca esta ventana, dar un click en el botón propiedades ubicado en la parte inferior izquierda de la ventana.

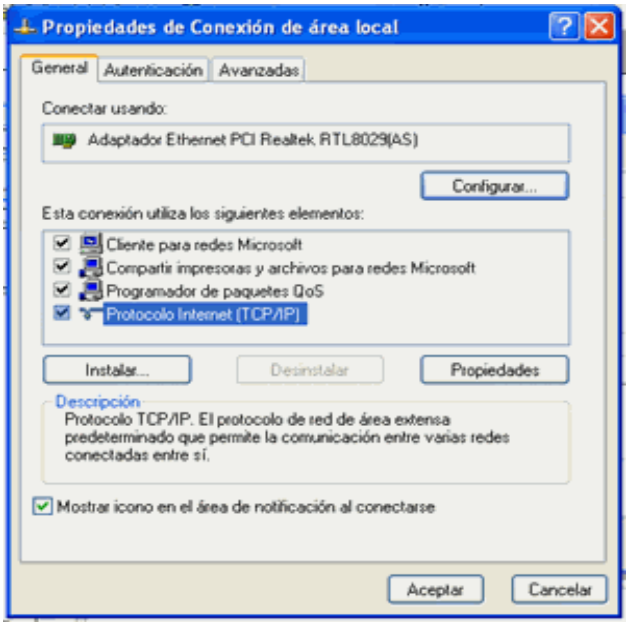
Figura 2.11. Ventana Propiedades de Conexión de área local



Autor: Gabriel Sebastián Proaño B

Luego que aparezca esta pantalla buscar la opción que dice: “Protocolo internet (TCP/IP)”. Ubicarse encima del mismo y a continuación dar doble click.

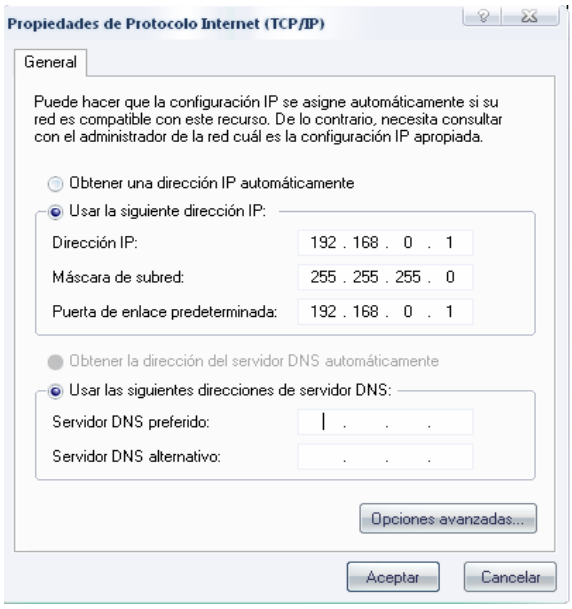
Figura 2.12. Ventana selección Protocolo Internet (TCP/IP)



Autor: Gabriel Sebastián Proaño B

Dentro de esta pantalla se tendrá la dirección IP, la máscara de subred y la puerta de enlace predeterminada. Dentro de estas opciones se realizará lo siguiente.

Figura 2.13 Ventana Propiedades de protocolo Internet (TCP/IP)



Autor: Gabriel Sebastián Proaño B.

Figura 2.14 Forma de configurar el protocolo (TCP/IP)

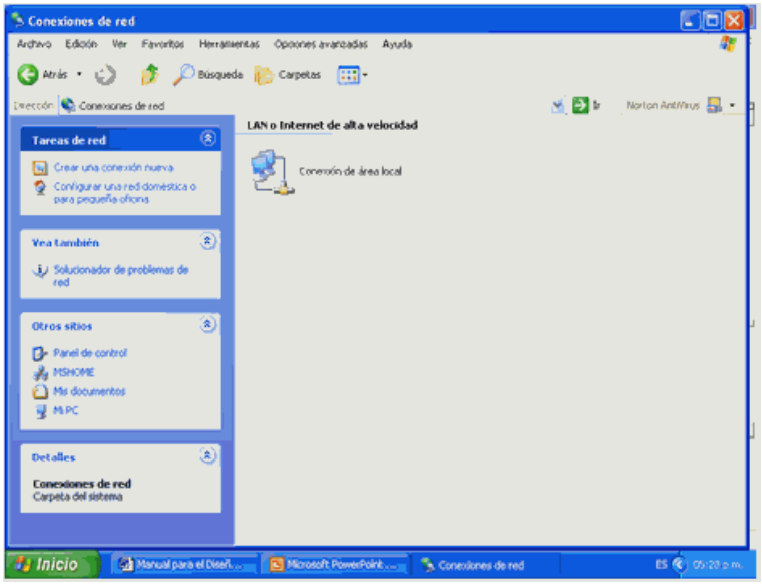
Autor: Gabriel Sebastián Proaño B

Una vez que se haya terminado de hacer esta operación podemos proseguir con la configuración de las Estaciones de Trabajo.

Configuración de las Estaciones:

Para la configuración de los protocolos (IP), la mascara de subred y la puerta de enlace de las estaciones de trabajo se tendrá que abrir la ventana conexiones de red ubicada en el panel de control.

Figura 2.15. Ventana Conexiones de Red Estación de Trabajo



Autor: Gabriel Sebastián Proaño B

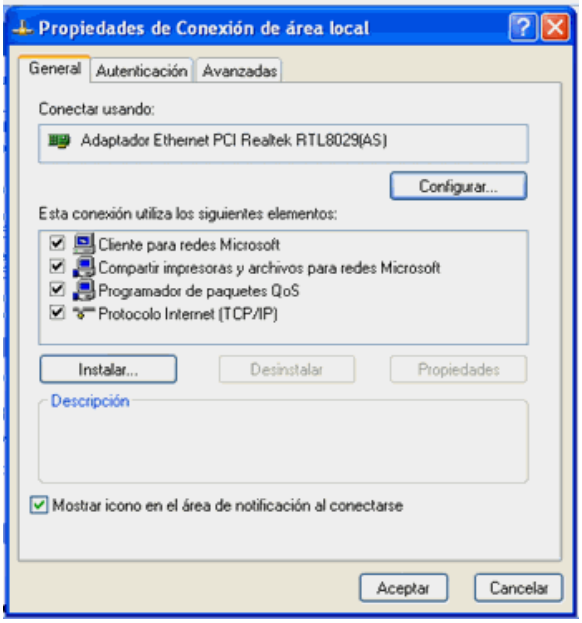
Dar un click con el botón derecho del mouse en el incono conexión de área local. Luego de haber hecho esta función aparecerá una pequeña ventana, que dirá. “Estado de conexión de área local.”

Figura 2.16. Ventana Estado Conexión de área local Estación de Trabajo

Autor: Gabriel Sebastián Proaño B

Luego que aparezca esta ventana, dar un click en el botón propiedades ubicado en la parte inferior izquierda de la ventana.

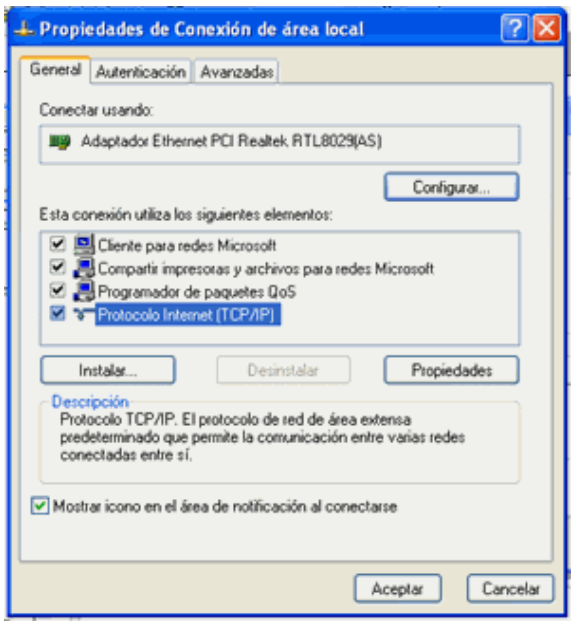
Figura 2.17. Ventana Propiedades de Conexión de área local Estación de Trabajo



Autor: Gabriel Sebastián Proaño B

Luego que aparezca esta pantalla buscar la opción que dice protocolo internet (TCP/IP) ubicarse encima del mismo y a continuación dar doble click.

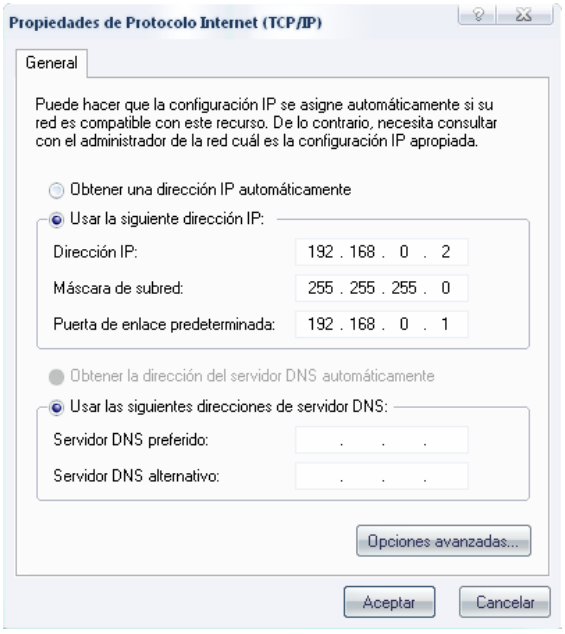
Figura 2.18. Ventana selección Protocolo Internet (TCP/IP) Estación de Trabajo



Autor: Gabriel Sebastián Proaño B

Una vez que se haya hecho esto se tendrá una pequeña pantalla que dirá. “Propiedades de Protocolo Internet (TCP/IP)”

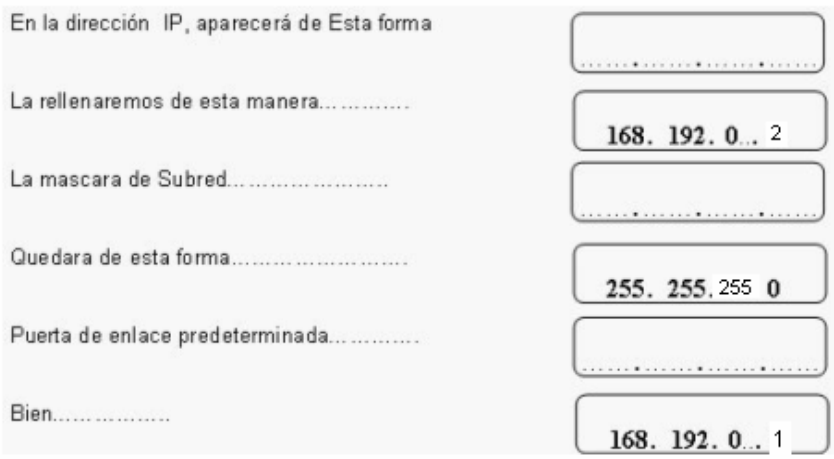
Figura 2.19 Ventana Propiedades de protocolo Internet (TCP/IP) Estación de Trabajo



Autor: Gabriel Sebastián Proaño B

Dentro de esta pantalla se tendrá la dirección IP, la mascara de subred y la puerta de enlace predeterminada. Dentro de estas opciones realizaremos lo siguiente:

Figura 2.20 Forma de configurar el protocolo (TCP/IP) Estación de Trabajo



Autor: Gabriel Sebastián Proaño B

INFORMACIÓN: La dirección IP cambiará en el ultimo digito mas para cada estación siendo este secuencial.

Ejemplo. En la primera estación tendremos la IP. 168.192.0.2, ¿Debido a que?; Es muy sencillo puesto que el primer digito (1) pertenece a el Servidor (HOST), A medida que se va avanzando de estaciones tendremos que añadir un digito mas como se menciono antes. Si la primera estación fue 168.192.0.2 la segunda Estación será 168.192.0.3 y así periódicamente. Por otra parte la Máscara de Subred será siempre 255.255.255.0 para todas las Estaciones. Con respecto a la puerta de Enlace siempre será 168.192.0.1, ¿Debido a que? la puerta de enlace será siempre la misma ya que el Protocolo o el IP del Servidor es 192.168.0.1 es decir es el código que nos permite acceder a Internet mediante el Servidor.

Conexión del Cableado al Switch:

En este se toman los Cables ya medidos con sus respectivos conectores RJ45 ya apantallados. El primer paso será tomar el Cable del Servidor y Conectarlo al Concentrador en el primer puerto luego se instalar todos los Equipos restantes en el orden requerido.

Figura 2.21 Switch de 8 Puertos

Fuente: http://www.solostocks.com

Comprobación de la Conexión:

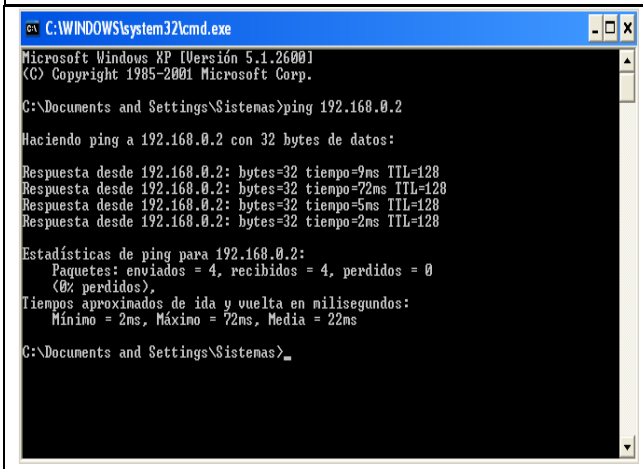
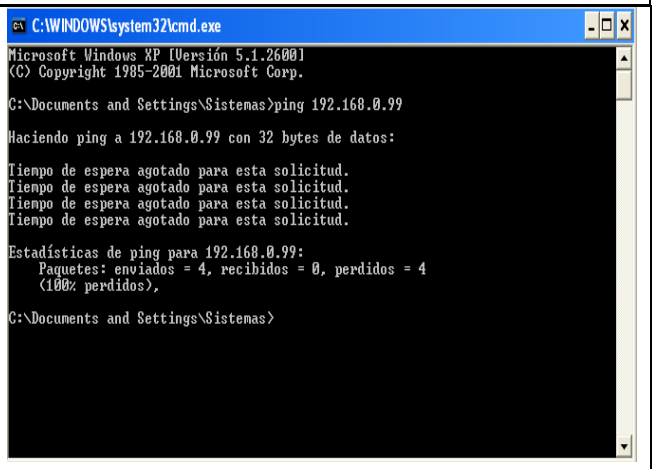
El primer paso será encender todas las estaciones impresoras y otros equipos instalados a la red, asegurarse de que el servidor esté conectado a Internet y que el concentrador este encendido y funcionando, otra forma de saber si las estaciones están conectadas con el servidor es abriendo el Panel de Control, dando doble Click sobre el Icono de Conexiones de Red. Una vez allí ubicar en el lado izquierdo una pequeña pantalla llamada Otros Sitios, dar un click sobre el nombre que se le dio a la red. Aparecerá otra pantalla en la parte superior izquierda de la pantalla, allí dar un Click en Ver Equipos de Red.

Siguiendo estos sencillos pasos habrá una vista completa de todos los Equipos conectados a la Red, de allí se podrá monitorearlos y acceder a ellos.

Si las estaciones no están dentro del mismo grupo de trabajo entonces estas no se podrán divisar, en este caso se procede con los siguientes pasos:

Vamos a inicio -> ejecutar -> escribimos cmd nos despliega la pantalla de comandos y allí ponemos “ping 192.168.0.2” en este caso para ve si el ordenador que tiene esta ip mantiene conexión con la red, en caso de desplegar un mensaje como “Respuesta desde 192.168.0.2” entonces la conexión existe pero el grupo de trabajo no esta bien asignado caso contrario saldrá algo como “No existe respuesta” o “Host de destino inaccesible” en este caso la conexión presenta algún tipo de falla de orden físico.

Figura 2.22 Pantallas al ejecutar ping en modo DOS

EXISTE RESPUESTA	NO EXISTE RESPUESTA
	

Autor: Gabriel Sebastián Proaño B

2.4 Arquitectura

- Servidor: el servidor es aquel o aquellos ordenadores que van a compartir sus recursos hardware y software con los demás equipos de la red. Sus características son potencia de cálculo, importancia de la información que almacena y conexión con recursos que se desean compartir.
- Estación de trabajo: los ordenadores que toman el papel de estaciones de trabajo aprovechan o tienen a su disposición los recursos que ofrece la red así como los servicios que proporcionan los Servidores a los cuales pueden acceder.
- Gateways o pasarelas: es un hardware y software que permite las comunicaciones entre la red local y grandes ordenadores (mainframes). El gateway adapta los protocolos de comunicación del mainframe (X25, SNA, etc.) a los de la red, y viceversa.
- Bridges o puentes: es un hardware y software que permite que se conecten dos redes locales entre sí. Un puente interno es el que se instala en un servidor de la red, y un puente externo es el que se hace sobre una estación de trabajo de la misma red. Los puentes también pueden ser locales o remotos. Los puentes locales son los que conectan a redes de un mismo edificio, usando tanto conexiones internas como externas. Los puentes remotos conectan redes distintas entre sí, llevando a cabo la conexión a través de redes públicas, como la red telefónica, RDSI o red de conmutación de paquetes.
- Tarjeta de red: también se denominan NIC (Network Interface Card). Básicamente realiza la función de intermediario entre el ordenador y la red de comunicación. En ella se encuentran grabados los protocolos de comunicación de la red.

  La comunicación con el ordenador se realiza normalmente a través de las ranuras de expansión que éste dispone, ya sea ISA, PCI o PCMCIA. Aunque algunos equipos disponen de este adaptador integrado directamente en la placa base.

- El medio: constituido por el cableado y los conectores que enlazan los componentes de la red. Los medios físicos más utilizados son el cable de par trenzado, par de cable, cable coaxial y la fibra óptica (cada vez en más uso esta última).

- Concentradores de cableado: una LAN en bus usa solamente tarjetas de red en las estaciones y cableado coaxial para interconectarlas, además de los conectores, sin embargo este método complica el mantenimiento de la red ya que si falla alguna conexión toda la red deja de funcionar. Para impedir estos problemas las redes de área local usan concentradores de cableado para realizar las conexiones de las estaciones, en vez de distribuir las conexiones el concentrador las centraliza en un único dispositivo manteniendo indicadores luminosos de su estado e impidiendo que una de ellas pueda hacer fallar toda la red.

  Existen dos tipos de concentradores de cableado:

  1. Concentradores pasivos: actúan como un simple concentrador cuya función principal consiste en interconectar toda la red.
  2. Concentradores activos: además de su función básica de concentrador también amplifican y regeneran las señales recibidas antes de ser enviadas.

  Los concentradores de cableado tienen dos tipos de conexiones: para las estaciones y para unirse a otros concentradores y así aumentar el tamaño de la red. Los concentradores de cableado se clasifican dependiendo de la manera en que internamente realizan las conexiones y distribuyen los mensajes. A esta característica se le llama topología lógica.

  Existen dos tipos principales:

  1. Concentradores con topología lógica en bus (HUB): estos dispositivos hacen que la red se comporte como un bus enviando las señales que les llegan por todas las salidas conectadas.
  2. Concentradores con topología lógica en anillo (MAU): se comportan como si la red fuera un anillo enviando la señal que les llega por un puerto al siguiente.

CAPITULO III

REDES WLAN

3.1 Introducción a Redes Wlan

Una WLAN es un sistema de comunicaciones de datos que transmite y recibe datos utilizando ondas electromagnéticas, en lugar del par trenzado, coaxial o fibra óptica utilizado en las LAN convencionales, y que proporciona conectividad inalámbrica de igual a igual (peer to peer), dentro de un edificio, de una pequeña área residencial/urbana o de un campus universitario. En EE.UU. proliferan estas redes para acceso a Internet, en donde hay más de 4.000 zonas de acceso, y en Europa es previsible que pronto se extiendan.
Las WLAN se encuadran dentro de los estándares desarrollados por el IEEE[9] (Instituto de Ingenieros Eléctricos y Electrónicos) para redes locales inalámbricas. Otras tecnologías como HyperLAN[10] apoyada por el ETSI[11], y el nuevo estándar HomeRF[12] para el hogar, también pretenden acercarnos a un mundo sin cables y, en algunos casos, son capaces de operar en conjunción y sin interferirse entre sí. Otro aspecto a destacar es la integración de las WLAN en entornos de redes móviles de 3G (UMTS) para cubrir las zonas de alta concentración de usuarios (los denominados hot spots), como solución de acceso público a la red de comunicaciones móviles.

Como todos los estándares 802 para redes locales del IEEE, en el caso de las WLAN, también se centran en los dos niveles inferiores del modelo OSI, el físico y el de enlace, por lo que es posible correr por encima cualquier protocolo (TCP/IP o cualquier otro) o aplicación, soportando los sistemas operativos de red habituales, lo que supone una gran ventaja para los usuarios que pueden seguir utilizando sus aplicaciones habituales, con independencia del medio empleado, sea por red de cable o por radio.

9.- Acrónimo de *Institute of Electric and Electronics Engineers, Inc.*, Instituto de Ingenieros Eléctricos y Electrónicos se encarga de definir estándares para las comunicaciones, la industria eléctrica, las aplicaciones biomédicas o la electrónica profesional y de consumo.
10.-HiperLAN (HIgh Performance Radio LAN) es un estándar de redes inalámbricas.
11.- Escuela Técnica Superior de Ingenieros European Telecommunications Standards Institute
12.- Estándar que pretendía diseñar un aparato central en cada casa que conectara los teléfonos y además proporcionar un ancho de banda de datos entre las computadoras.

Otra tecnología de acceso inalámbrico en áreas de pequeña extensión (WPAN/WLAN Personal Area Network) es la denominada Bluetooth, que aunque pueda parecer competencia directa de las WLAN, es más bien complementaria a ella.
Bluetooth pretende la eliminación de cables, como por ejemplo todos los que se utilizan para conectar el PC con sus periféricos, o proporcionar un medio de enlace entre dispositivos situados a muy pocos metros, sirviendo también como mando a distancia.

Las WLAN tienen su campo de aplicación específico, igual que Bluetooth, y ambas tecnologías pueden coexistir en un mismo entorno sin interferirse gracias a los métodos de salto de frecuencia que emplean, sus aplicaciones van en aumento y, conforme su precio se vaya reduciendo, serán más y más los usuarios que las utilicen, por las innegables ventajas que supone su rápida implantación y la libertad de movimientos que permiten.

En los últimos años las redes inalámbricas (WLAN, Wireless Local Area Network) han ganado muchos adeptos y popularidad en mercados verticales tales como hospitales, fabricas, bodegas, tiendas de autoservicio, tiendas departamentales, pequeños negocios y áreas académicas. Las redes inalámbricas permiten a los usuarios acceder información y recursos en tiempo real sin necesidad de estar físicamente en un sólo 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 video 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 PDAs (Personal Digital Assistants), 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 generalizada para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red.

3.2 Historia

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados por el IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema de espectro expandido (spread spectrum). En mayo de 1985, y tras cuatro años de estudios, la FCC (Federal Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz para uso en las redes inalámbricas basadas en Spread Spectrum (SS), con las opciones DS (Direct Sequence) y FH (Frequency Hopping). La técnica de espectro ensanchado es una técnica de modulación que resulta ideal para las comunicaciones de datos, ya que es muy poco susceptible al ruido y crea muy pocas interferencias. La asignación de esta banda de frecuencias propició una mayor actividad en el seno de la industria y ese respaldo hizo que las WLAN empezaran a dejar ya el entorno del laboratorio para iniciar el camino hacia el mercado.

Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbit/s, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN, con aplicación empresarial.

Las redes WLAN se componen fundamentalmente de dos tipos de elementos, los puntos de acceso y los dispositivos de cliente.

Los puntos de acceso actúan como un concentrador o hub que reciben y envían información vía radio a los dispositivos de clientes, que pueden ser de cualquier tipo, habitualmente, un PC o PDA con una tarjeta de red inalámbrica, con o sin antena, que se instala en uno de los slots libres o bien se enlazan a los puertos USB de los equipos.
La principal ventaja de este tipo de redes (WLAN), que no necesitan licencia para su instalación, es la libertad de movimientos que permite a sus usuarios, ya que la posibilidad de conexión sin hilos entre diferentes dispositivos elimina la necesidad de compartir un espacio físico común y soluciona las necesidades de los usuarios que requieren tener disponible la información en todos los lugares por donde puedan estar trabajando. Además, a esto se añade la ventaja de que son mucho más sencillas de instalar que las redes de cable y permiten la fácil reubicación de los terminales en caso necesario.
También, presentan alguna desventaja, o más bien inconveniente, que es el hecho de la "baja" velocidad que alcanzan, por lo que su éxito comercial es más bien escaso y, hasta que los nuevos estándares no permitan un incremento significativo, no es de prever su uso masivo, ya que por ahora no pueden competir con las LAN basadas en cable.
El uso más popular de las WLAN implica la utilización de tarjetas de red inalámbricas, cuya función es permitir al usuario conectarse a la LAN empresarial sin la necesidad de una interfaz física.

3.2.1 Normalización IEEE

La historia de las WLAN es bastante reciente, de poco más de una década. En 1989, en el seno de IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN, pero no es hasta 1994 cuando aparece el primer borrador, y habría que esperar hasta el año 1999 para dar por finalizada la norma.
En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (Personal Communications Systems).

En 1993 también se constituye la IrDA (Infrared Data Association) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos.

En 1996, finalmente, un grupo de empresas del sector de informática móvil (mobile computing) y de servicios forman el Wireless LAN Interoperability Forum (WLI Forum) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos.Por otra parte, WLANA (Wireless LAN Association) es una asociación de industrias y empresas cuya misión es ayudar y fomentar el crecimiento de la industria WLAN a través de la educación y promoción.

Actualmente son cuatro los estándares reconocidos dentro de esta familia; en concreto, la especificación 802.11 original; 802.11a (evolución a 802.11 e/h), que define una conexión de alta velocidad basada en ATM; 802.11b, el que goza de una más amplia aceptación y que aumenta la tasa de transmisión de datos propia de 802.11 original, y 802.11g, compatible con él, pero que proporciona aún mayores velocidades.

3.2.1.1 WLAN 802.11

En junio del año 1997 el IEEE ratificó el estándar para WLAN IEEE 802.11, que alcanzaba una velocidad de 2 Mbit/s, con una modulación de señal de espectro expandido por secuencia directa (DSSS), aunque también contempla la opción de espectro expandido por salto de frecuencia, FHSS en la banda de 2,4 GHz, y se definió el funcionamiento y la interoperabilidad entre redes inalámbricas.

El 802.11 es una red local inalámbrica que usa la transmisión por radio en la banda de 2.4 GHz, o infrarroja, con regímenes binarios de 1 a 2 Mbit/s. El método de acceso al medio MAC (Medium Access Mechanism) es mediante escucha pero sin detección de colisión, CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

La dificultad en detectar la portadora en el acceso WLAN consiste básicamente en que la tecnología utilizada es Spread-Spectrum y con acceso por división de código (CDMA), lo que conlleva a que el medio radioeléctrico es compartido, ya sea por secuencia directa DSSS o por saltos de frecuencia en FHSS. El acceso por código CDMA implica que pueden coexistir dos señales en el mismo espectro utilizando códigos diferentes, y eso para un receptor de radio implicara que detectaría la portadora inclusive con señales distintas de las de la propia red WLAN. Hay que mencionar que la banda de 2,4 GHz está reglamentada como banda de acceso pública y en ella funcionan gran cantidad de sistemas, entre los que se incluyen los teléfonos inalámbricos Bluetooth.

3.2.1.2 WLAN 802.11b (Wi-Fi)

Un poco más tarde, en el año 1999, se aprobó el estándar 802.11b, una extensión del 802.11 para WLAN empresariales, con una velocidad de 11 Mbit/s (otras velocidades normalizadas a nivel físico son: 5,5 - 2 y 1 Mbit/s) y un alcance de 100 metros, que al igual que Bluetooth y Home RF, también emplea la banda de ISM de 2,4 GHz, pero en lugar de una simple modulación de radio digital y salto de frecuencia (FH/Frequency Hopping), utiliza una la modulación linear compleja (DSSS). Permite mayor velocidad, pero presenta una menor seguridad, y el alcance puede llegar a los 100 metros, suficientes para un entorno de oficina o residencial.

3.2.1.3 WLAN 802.11g

El IEEE también aprobó en el año 2003 en el estándar 802.11g, compatible con el 802.11b, capaz de alcanzar una velocidad doble, es decir hasta 22 Mbit/s o llegar, incluso a 54 Mbit/s, para competir con los otros estándares que prometen velocidades mucho más elevadas pero que son incompatibles con los equipos 802.11b ya instalados, aunque pueden coexistir en el mismo entorno debido a que las bandas de frecuencias que emplean son distintas. Por extensión, también se le llama Wi-Fi.

3.3 Diseño

Las redes inalámbricas de área local (WLAN) son una realidad hoy en día y están teniendo un gran éxito entre la población en gran medida, gracias a que sus precios han disminuido considerablemente. Es posible conseguir un punto de acceso (AP, access point) o una tarjeta de red inalámbrica por menos de $100 dólares.

La tecnología Wi-Fi, cómo se le conoce comúnmente a las WLANs, utiliza frecuencias de radio (RF) para transmitir información en vez de utilizar los tradicionales cables para comunicación. Es claro que una de las principales ventajas de las redes sin alambres es la movilidad y la fácil integración con las redes cableadas existentes. Pero quizá su mayor ventaja con respecto a otras tecnologías inalámbricas, es que las frecuencias que utiliza son de uso libre.

Las WLAN han tenido mucha aceptación en oficinas, universidades, hogares, así como en áreas públicas como hoteles, aeropuertos, restaurantes. Ellos ven la tecnología inalámbrica una estrategia para atraer clientes al ofrecer Internet dentro de sus negocios.

Es muy común en este tipo de redes que los usuarios finales, entusiasmados por el boom que últimamente las WLANS han alcanzado, compren e instalen equipo sin una previa planeación y diseño. Trayendo como resultado un deficiente desempeño y en casos muy extremos, el robo de la información. La instalación y la configuración de una WLAN pueden ser un proceso muy sencillo, pero precisamente esto las hace ser un blanco fácil para ataques externos e internos a la organización. Recordemos que el medio por el cual se comunican dispositivos inalámbricos es el aire, y que cualquier espía con los dispositivos necesarios puede rastrear las señales y utilizar en su beneficio los recursos de la red. En este artículo describiremos como planear y diseñar una red WLAN, con la intención de optimizar su desempeño así como también de reducir el nivel de inseguridad que presentan este tipo de redes.

Factores que hay que tomar en consideración en el diseño y planeación de una red WLAN :

1. Ancho de banda/Velocidad de transmisión.
2. La frecuencia de operación.
3. Tipos de aplicaciones que van a correr en la WLAN.
4. Número máximo de usuarios.
5. área de cobertura.
6. Material con el que están construidos los edificios.
7. Conexión de la WLAN con la red cableada.
8. Disponibilidad de productos en el mercado.
9. Planeación y administración de las direcciones IP.
10. Los identificadores de la red (SSID)
11. Seguridad.

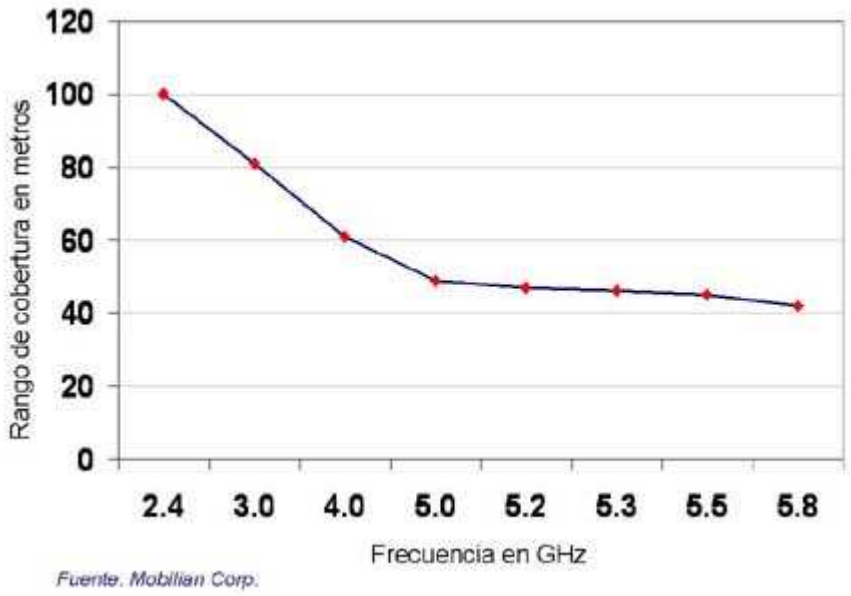
3.3.1 Ancho de banda/Velocidad de transmisión

Debemos tomar en cuenta el ancho de banda y la velocidad de transmisión que nos brinda las WLAN. Los estándares IEEE 802.11a y IEEE 802.11g, permiten velocidades de hasta 54 Mbps, por otro lado el estándar IEEE 802.11b permite velocidades de transmisión de hasta 11 Mbps. Este ancho de banda es mucho menor al de las redes cableadas, las cuales operan a 100 Mbps. El ancho de banda especificado por los estándares 802.11a/b/g es teórico y se cumple sólo en condiciones ideales. El máximo desempeño depende de muchos otros factores.

3.3.2 La frecuencia de operación

Cuando se diseña una WLAN generalmente causa confusión el hecho de seleccionar la frecuencia de operación que define el estándar que se va utilizar. Universalmente las WLAN utilizan las frecuencias de 2.4 GHz (802.11b) y 5 GHz (802.11a/g).
El hecho de utilizar una, tiene muchas implicaciones. Se han hecho diversos estudios sobre la propagación de las señales en estas dos frecuencias, dando como resultado que la frecuencia más baja (2.4 GHz) ofrece mejor propagación, extendiéndose más del doble de cobertura que la frecuencia de 5 GHz como se indica en la figura:

Figura 3.1 Rango de cobertura según la frecuencia



3.3.3 Tipos de aplicaciones

Es importante delimitar el tipo de aplicaciones que se van a correr en la red inalámbrica, tales como acceso a Internet, correo electrónico, consultas a base de datos y transferencia de archivos.

Dado el limitado ancho de banda, no es recomendable que se utilicen las WLAN para aplicaciones que consumen alto ancho de banda tales como transferencia de video e imágenes, videoconferencia, audio/video streaming.

Tabla 3.1. Comparación entre los estándares 802.11a, b y g

TABLA 3.1. COMPARACIÓN ENTRE LOS ESTÁNDARES 802.11A, B Y G			
PARÁMETRO	**IEEE 802.11A**	**IEEE 802.11B**	**IEEE 802.11G**
Frecuencia/Ancho de banda	5 GHz (300 MHz)	2.4 GHz (83.5 MHz)	2.4 GHz (83.5 MHz)
Modulación	OFDM	DSSS	OFDM
Ancho de banda por canal	20 MHz (6 canales utilizables)	22 MHz (3 canales)	22 MHz (3 canales)
Tasa de transmisión	54 Mbps	11 Mbps	54 Mbps
Cobertura interior/exterior	30/50 metros	50/150 metros	30/50 metros
Potencia máxima*	200 mW, 1 W, 4 W	1 mW/MHz	200 mW, 1 W, 4 W
Usuarios simultáneos	64	32	50

* Varía según la potencia de la antena y de la posición de ésta

Fuente: http://www.eveliux..com

3.3.4 Número máximo de usuarios

Uno de los factores más importantes cuando se diseña una WLAN es delimitar el número de usuarios que utilizará la red. Como se ve en la tabla 3.1, los estándares definen diferente número de usuarios conectados simultáneamente a un punto de acceso (AP).
Es obvio afirmar que a mayor número de usuarios conectados a una WLAN, menor será el desempeño de la misma. Hay que tener en cuenta el número máximo de usuarios que soporta cada estándar (ver tabla 3.1).

3.3.5 Área de cobertura:

Mientras la frecuencia aumenta, generalmente el rango de cobertura de la señal decrementa, de modo que la frecuencia de operación de 5 GHz generalmente tiene menor rango de cobertura que la de 2.4 GHz. De acuerdo con esto, si se utiliza el estándar 802.11a se requiere un número mayor de AP's para extender la cobertura, y esto implica un mayor presupuesto. Por otro lado el estándar 802.11b tiene una mayor cobertura aunque con un menor ancho de banda. También hay que tener en cuenta si el punto de acceso se va a instalar en exteriores o interiores. Dependiendo de ello, será el rango de cobertura. En cubículos cerrados la cobertura es de 20 metros, en cubículos abiertos de 30 metros. En pasillos y corredores de hasta 45 metros. En exteriores de hasta 150 metros. El uso de antenas con mayor ganancia aumentará considerablemente la cobertura.

3.3.6 Material con el que están construidos los edificios

La propagación de las ondas electromagnéticas (señales) se comportan de manera diferente en relación al material con el que estén construidos los edificios donde se instalará la WLAN. Hablamos entonces de diversos materiales tales como: madera, ladrillo, tabla roca. Ciertos materiales reflejan las señales sin problema como la madera y la tabla roca, lo cual puede extender la cobertura de la WLAN. Otros materiales (los duros) como el concreto con varilla, acero y cemento absorben o atenúan la potencia de la señal disminuyendo la cobertura.

3.3.7 Conexión de la WLAN

Con la red cableada: debemos tener en cuenta que los puntos de acceso necesitan electricidad para poder operar y además deben estar conectados a la red cableada. Se recomienda instalar los puntos de acceso en lugares estratégicos sin olvidarse de éstas dos conexiones. Existen puntos de acceso que proveen la electricidad al AP a través del cable par trenzado. Esta característica se le conoce como PoE (power over Ethernet).

3.3.8 Disponibilidad de productos en el mercado

Hay que estar concientes del mercado de punto de acceso. Si compramos un punto de acceso debemos de tomar en cuenta factores como el costo y el soporte técnico disponible. A veces lo barato puede salir caro.

3.3.9 Planeación y administración de las direcciones IP

Hay que tomar en cuenta que los dispositivos inalámbricos necesitan de una dirección IP para poder identificarse. Por lo que será necesario reservar direcciones IPs para los dispositivos inalámbricos que se quieran conectar a la red. En caso de no existan las suficientes, será necesario emplear enrutadores inalámbricos que puedan proporcionar direcciones IP privadas. También hay que considerar el uso servidores de DHCP para asignar direcciones dinámicamente; pero esto puede ser contraproducente. El administrador de la red deberá decidir si se utiliza ésta opción o asignar direcciones manualmente.

3.3.10 Los identificadores de la red (SSID)

Los SSIDs son los identificadores de los puntos de acceso. Se deben poner SSIDs adecuados y no muy obvios. La razón: estos identificadores son fácilmente rastréales por aplicaciones o por otros APs. Es muy común que al instalar un AP, no se cambie el nombre del SSID que trae de fábrica.

Esta mala práctica ocasiona que los usuarios maliciosos identifiquen claramente el nombre del fabricante del AP y puedan conocer la contraseña. Para después entrar al panel de administración de la configuración del AP y tomar el control total de la red.

3.3.11 Seguridad

La seguridad es quizás el factor menos tomado en cuenta al instalar una WLAN y resulta ser de lo más crítico. Las WLAN son más susceptibles a ataques debido a que los intrusos no requieren conexión física para acceder a la red.
En este punto hay que tener en cuenta cual será el nivel de seguridad que queramos para proteger nuestra red. Existen tres niveles de seguridad: el básico, intermedio y avanzado.

En el nivel básico existe ya por omisión un mecanismo de seguridad en el estándar 802.11x, conocido como WEP. Este mecanismo utiliza una llave o contraseña de 64 o 128 bits para acceder al AP. También existe en este nivel básico de seguridad el filtrado de direcciones MAC. Con este mecanismo se logra filtrar aquellas direcciones MAC que no pertenezcan a nuestra red. Se ha demostrado que es muy fácil corromper estos dos mecanismos, por lo cual no es muy recomendable si se desea un nivel de seguridad más sofisticado.

En el nivel intermedio de seguridad se encuentran los servidores de autentificación, tales como el RADIUS y el kerberos. Para ellos se requiere la instalación y configuración de un servidor de autentificación, el cual implica un gasto extra por la contratación de una persona calificada que lo instale, configure y administre. El acceso al AP se hace mediante un login y password más personalizado para cada usuario. El servidor de autentificación validará ésta información antes de darle acceso al AP. Una de las desventajas de los servidores de autentificación es que éstos pueden ser accesados maliciosamente por los hackers y obtener la lista completa de contraseñas y usuarios.

En el nivel avanzado de seguridad ya se hace uso de servidores de autentificación más sofisticados. En este nivel se pueden emplear protocolos de encriptación tales como IPSec, SSL o TLS. También pueden comprarse equipos VPN para crear túneles seguros entre los usuarios y los servidores de autentificación.

3.4 Arquitectura

Para la transmisión de la información en las redes Wlan se utilizan ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado. Al hablar de ondas de radio nos referimos normalmente a portadoras de radio, sobre las que va la información, ya que realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final.

A este proceso se le llama modulación de la portadora por la información que está siendo transmitida. Si las ondas son transmitidas a distintas frecuencias de radio, varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas. Para extraer los datos el receptor se sitúa en una determinada frecuencia, frecuencia portadora, ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena.
La naturaleza de la conexión sin cable es transparente a la capa del cliente.
Las configuraciones de red para radiofrecuencia pueden ser de muy diversos tipos y tan simples o complejas como sea necesario.

La más básica se da entre dos ordenadores equipados con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno.

Esto es llamado red de igual a igual (peer to peer). Cada cliente tendría únicamente acceso a los recursos del otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o preconfiguración.
Instalando un Punto de Acceso se puede doblar la distancia a la cuál los dispositivos pueden comunicarse, ya que estos 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 gestionan el tráfico de la red entre los terminales más próximos. Cada punto de acceso puede servir a varias máquinas, según el tipo y el número de transmisiones que tienen lugar. Existen muchas aplicaciones en el mundo real con un rango de 15 a 50 dispositivos cliente con un solo punto de acceso.

Los puntos de acceso tienen un alcance finito, del orden de 150 m en lugares u zonas abiertas. 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. iuparticulares de topologías, el diseñador de la red puede elegir usar un Punto de Extensión (EPs) 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 alcance 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.
Uno de los últimos componentes a considerar en el equipo de una WLAN es la antena direccional. Por ejemplo: si se quiere una Lan sin cable a otro edificio a 1 Km. de distancia. Una solución puede ser instalar una antena en cada edificio con línea de visión directa.

La antena del primer edificio está conectada a la red cableada mediante un punto de acceso. Igualmente en el segundo edificio se conecta un punto de acceso, lo cual permite una conexión sin cable en esta aplicación.

3.4.1Asignación de Canales

Los estándares 802.11b y 802.11g utilizan la banda de 2.4 – 2.5 Ghz. En esta banda, se definieron 11 canales utilizables por equipos WIFI, los que pueden configurarse de acuerdo a necesidades particulares. Sin embargo, los 11 canales no son completamente independientes (canales contiguos se superponen y se producen interferencias) y en la práctica sólo se pueden utilizar 3 canales en forma simultánea (1, 6 y 11).

Esto es correcto para USA y muchos países de América Latina, pues en Europa, el ETSI ha definido 13 canales. En este caso, por ejemplo en España, se pueden utilizar 4 canales no-adyacentes (1, 5, 9 y 13). Esta asignación de canales usualmente se hace sólo en el Punto de Acceso, pues los "clientes" automáticamente detectan el canal, salvo en los casos en que se forma una red ad hoc o punto a punto cuando no existe Punto de acceso.

3.5 Pasos para la instalación de la tarjeta de red inalámbrica externa

Para la conexión de la tarjeta de red inalámbrica se deben de seguir los siguientes pasos:

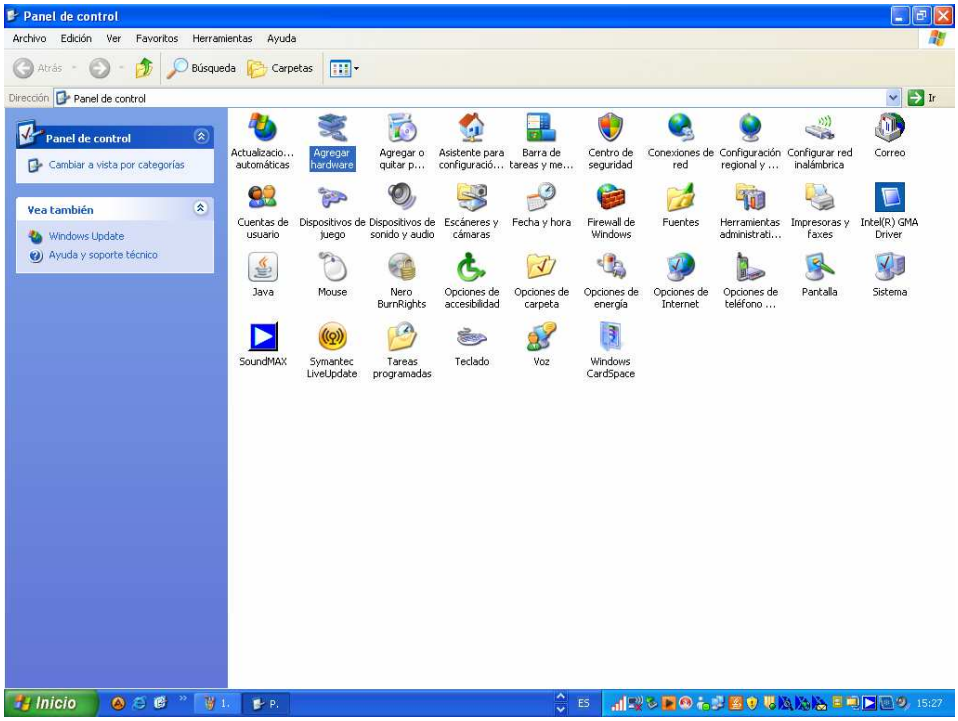
Dar un click en la barra del menú de inicio. Ubicar el puntero del mouse en la solapa de panel de control y hacer un click.

Figura 3.2Pantalla Panel de Control

Autor: Gabriel Sebastián Proaño B

A continuación ubicar el incono de agregar nuevo hardware, hacer un doble click para abrir el menú agregar nuevo hardware.

Figura 3.3. Ventana agregar hardware



Autor: Gabriel Sebastián Proaño B

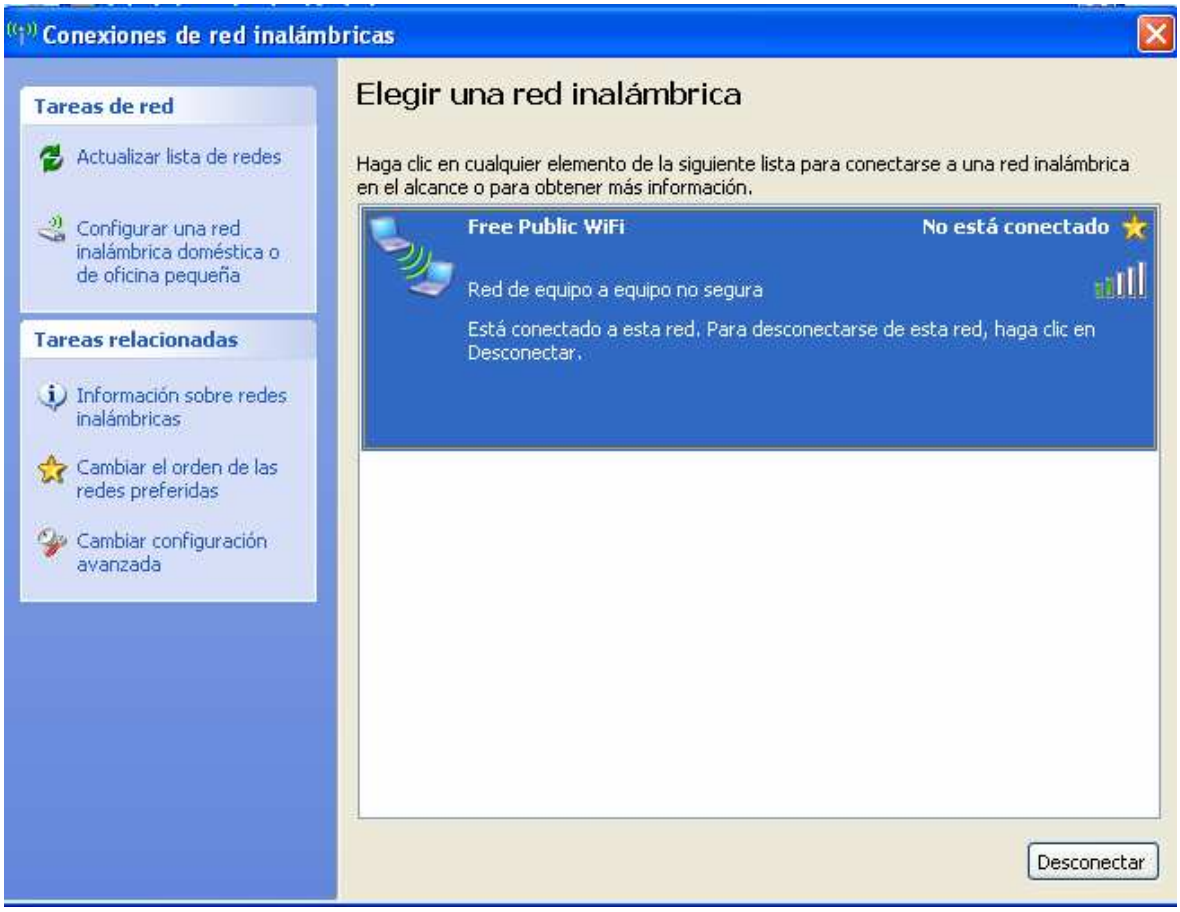
De allí en adelante seguir los procedimientos que indica el fabricante de la tarjeta de red inalámbrica por lo general este tipo de tarjetas externas no son detectadas de forma automática por el sistema operativo por lo que es necesario insertar el CD adjunto para instalar dicha tarjeta.

Cabe mencionar que los pasos anteriormente descritos son para la instalación de una tarjeta de red inalámbrica externa, la mayoría de computadores portátiles tienen ya incorporado dicha tarjeta, a continuación se procederá a describir como configurar la conexión a la red tanto de forma manual (IP fija) como de forma automática (DHCP).

3.5.1 Pasos para la configuración de una tarjeta de red inalámbrica con IP automática (DHCP).

Una vez que a sido conectada la tarjeta de red inalámbrica esta detectará las redes a las cuales puede conectarse y están a su alcance.

Figura 3.4. Ventana para elegir una red inalámbrica



Autor: Gabriel Sebastián Proaño B

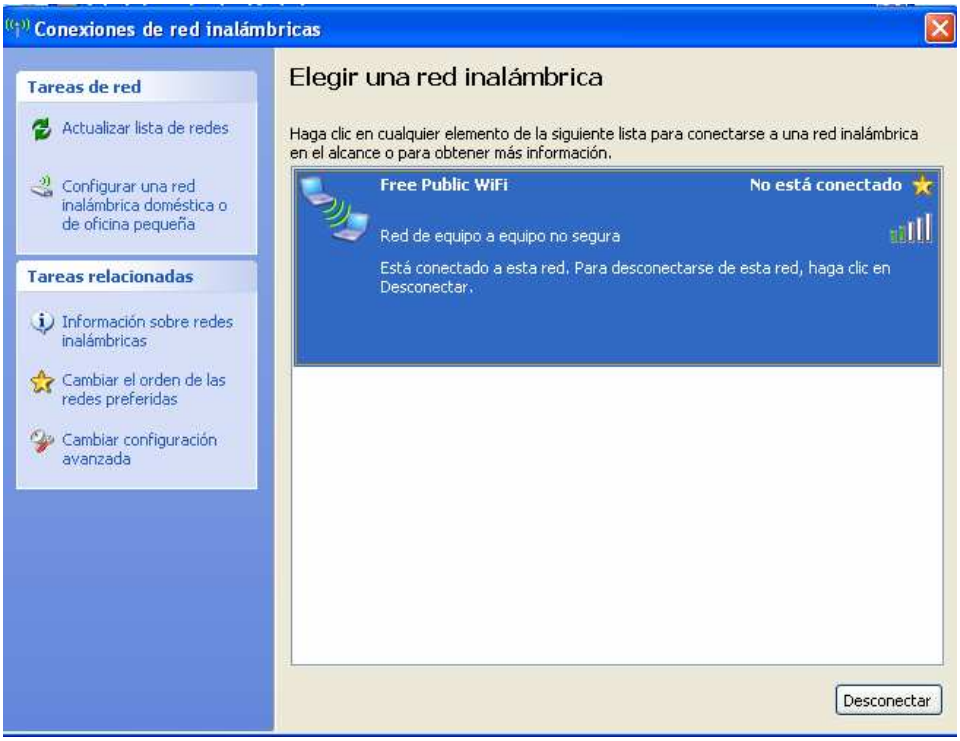
Dar doble click sobre la red a la cual deseamos conectarnos y la tarjeta tendrá acceso a dicha red, hay veces que la red posee clave para el acceso a la misma en este caso se tiene que ingresar la respectiva clave para poder ingresar.

3.5.2 Pasos para la configuración de una tarjeta de red inalámbrica con IP estática.

En ocasiones las redes inalámbricas necesitan a mas de la clave para su acceso una dirección IP fija para poder acceder a la red en este caso se deberán de seguir los siguientes pasos:

Una vez conectada la tarjeta de red inalámbrica esta detectará las redes a las cuales puede acceder y conectarse.

Figura 3.4. Ventana para elegir una red inalámbrica



Autor: Gabriel Sebastián Proaño B

Dar doble click sobre la red a la cual se desea acceder, de ser necesario introducir la clave de acceso a la misa.

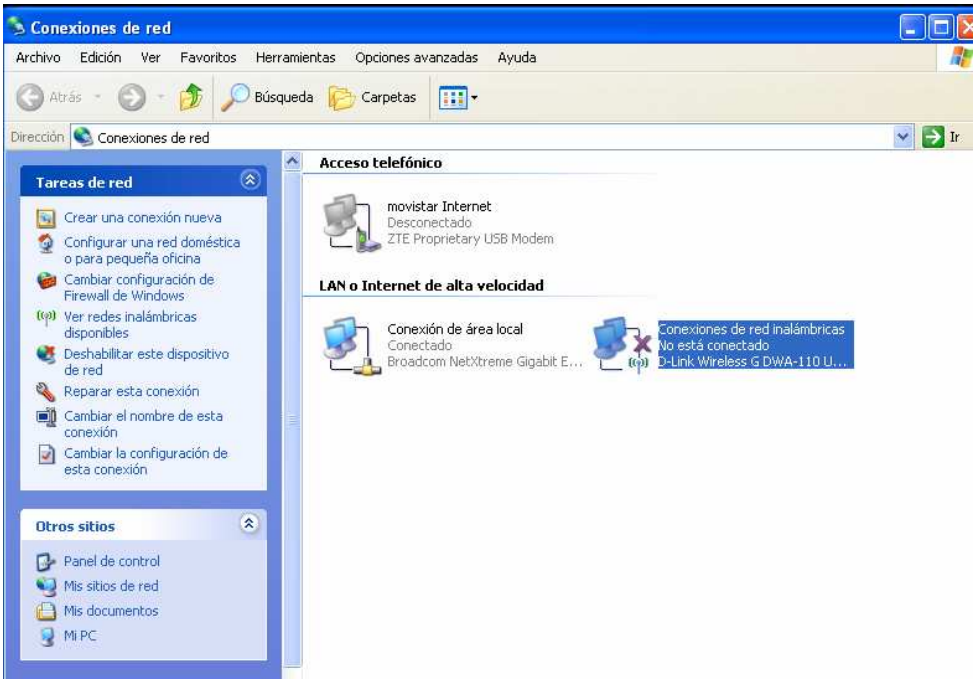
Una vez conectados a la red ir al escritorio y dar click derecho sobre mis sitios de red ahí nos desplegara un menú

Figura 3.5. Menú secundario de Mis sitios de red

Autor: Gabriel Sebastián Proaño B

Dar click sobre “Propiedades” y se desplegará la siguiente pantalla:

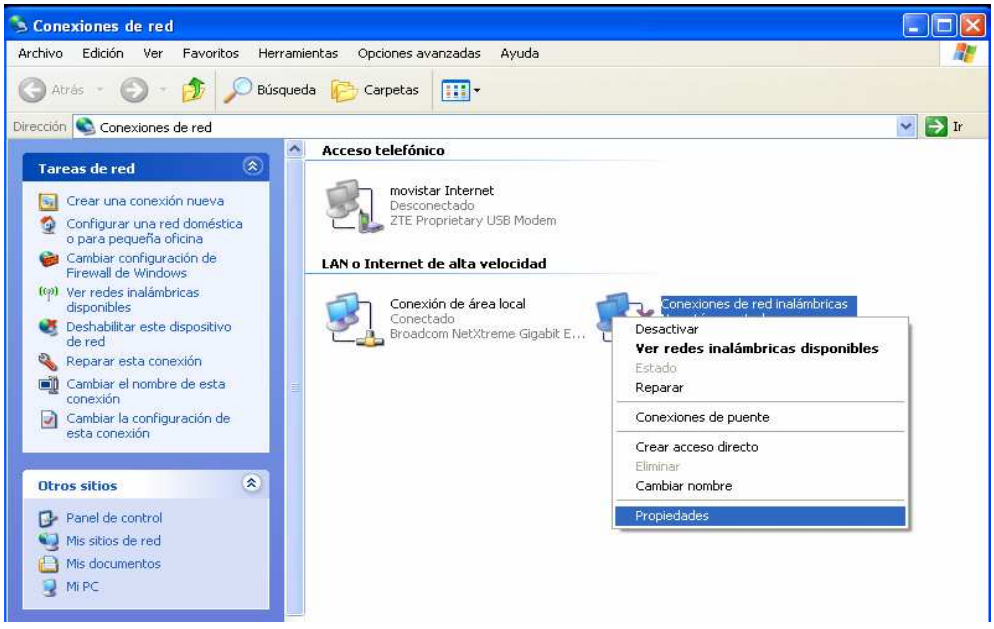
Figura 3.6. Ventana Conexiones de red



Autor: Gabriel Sebastián Proaño B

Dar click derecho sobre “Conexiones de red Inalámbricas” y se desplegará un menú allí escoger propiedades.

Figura 3.7. Menú secundario Conexiones de red inalámbricas



Autor: Gabriel Sebastián Proaño B.

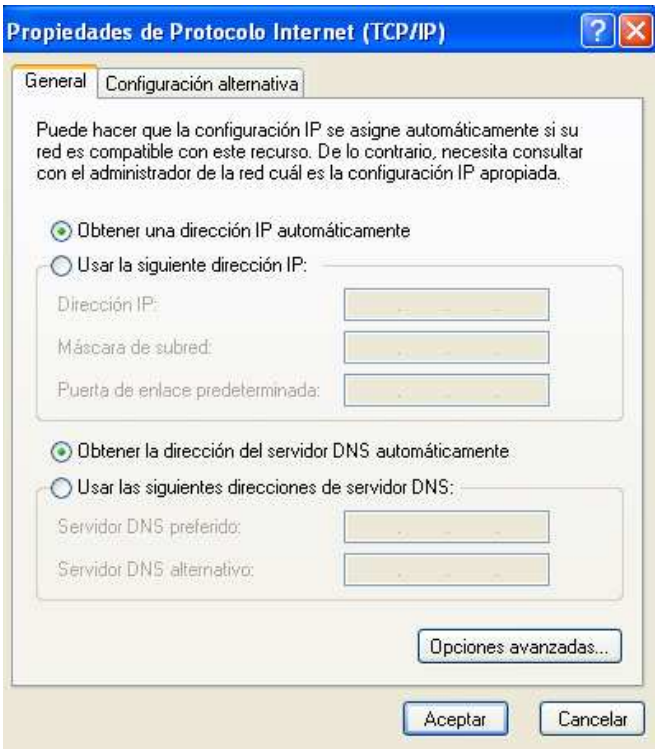
Dentro de la venta “Propiedades de Conexiones de red Inalámbricas” escoger la opción “Protocolos Internet (TCP/IP)”

Figura 3.8 Propiedades de Conexiones de red inalámbricas

Autor: Gabriel Sebastián Proaño B

Dar doble click sobre “Protocolo Internet (TCP/IP) y se desplegara la siguiente pantalla:

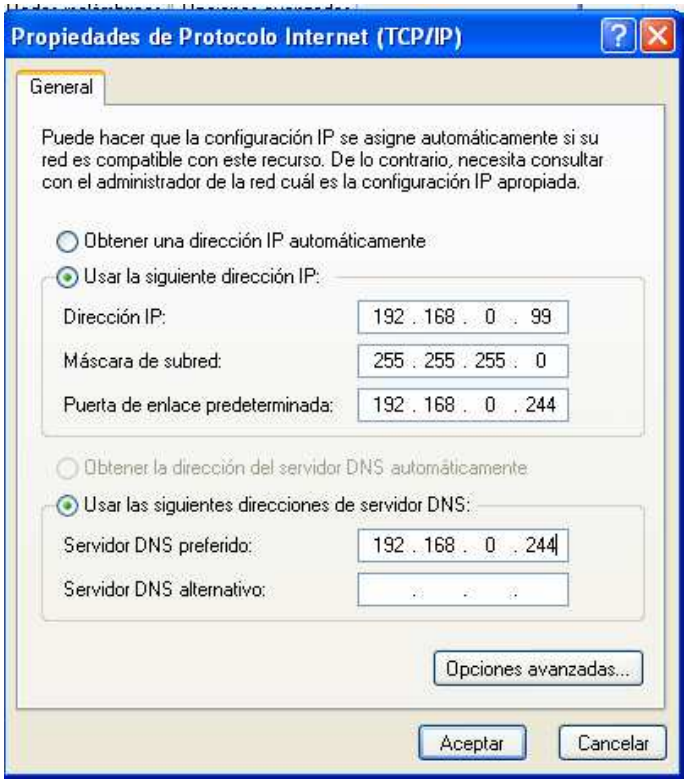
Figura 3.9 Propiedades de Protocolo Internet (TCP/IP) – IP automática



Autor: Gabriel Sebastián Proaño B

Escoger la opción “Usar la siguiente dirección IP” y allí escribimos la información sobre la Dirección IP, Mascara de subred que por lo general es 255.255.255.0 (a menos que hayan subredes), puerta de enlace y en el caso de necesitar conectarnos a Internet tendremos que introducir también el Servidor DNS preferido, quedara de la siguiente manera:

Figura 3.10. Propiedades de Protocolo Internet (TCP/IP) – IP fija



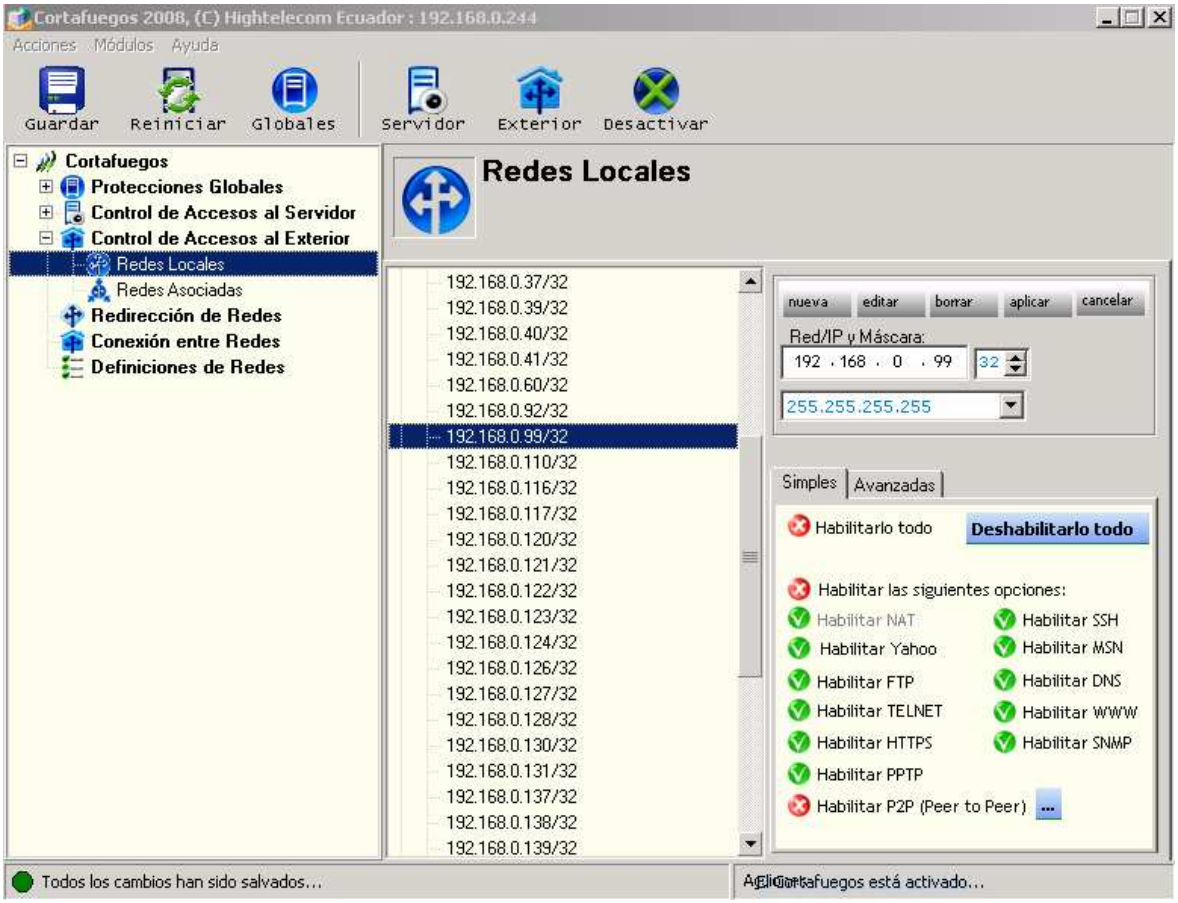
Autor: Gabriel Sebastián Proaño B

INFORMACIÓN: La dirección IP cambiará en el último digito para cada estación siendo este secuencial al igual que en la configuración para redes LAN.

La dirección IP fija que se asigna para una conexión inalámbrica necesariamente tendrá que estar administrada por un firewall para una adecuada protección allí se le podrá dar diferentes permisos para que dicha IP tenga autorizaciones específicas para la navegación en Internet.

En el siguiente gráfico se tiene el ejemplo de un servidor firewall el cual administra permisos a los usuarios que navegan por Internet.

Figura 3.11 Consola de administración de Cortafuegos



Autor: Gabriel Sebastián Proaño B

Se puede observar como a la IP que acabamos de asignar a la tarjeta inalámbrica (192.168.0.99) tiene los permisos abiertos para navegar sin restricción es decir no se necesita configurar ningún servidor Proxy, pero esta dirección IP no tiene los privilegios para conectarse a aplicativos punto a punto (peer to peer) como ares, emule, etc., los cuales consumen un alto ancho de banda ya que están diseñados para bajar música, videos entre otros.

CAPITULO IV

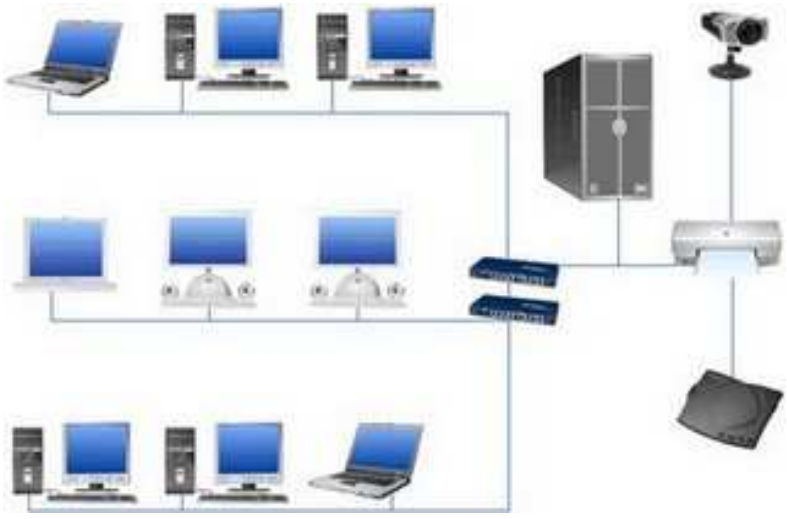
ESTUDIO COMPARATIVO

4.1 Estudio comparativo de diseño entre redes Lan y Wlan.

En este punto del análisis técnico comparativo que se ha venido realizando y una vez analizado de manera concisa y clara las principales características de cada una de las 2 redes comparadas nos es posible darnos cuenta que el diseño de redes Lan y Wlan difieren mucho en su diseño mientras las Lan utilizan cables para comunicarse las Wlan utilizan el aire para poder transmitir los datos.

Las redes Lan se comunican a través de cables de datos, generalmente basada en Ethernet, los cables de datos, conocidos como cables de red de Ethernet o cables con hilos conductores (CAT5), conectan computadoras y otros dispositivos que forman las redes.
Las redes alámbricas son mejores cuando se necesita mover grandes cantidades de datos a altas velocidades, como medios multimedia de calidad profesional.
En la figura 4.1 Se presenta un diagrama característico de cómo esta diseñada una red Lan:

Figura 4.1 Diseño red Lan



Fuente: http://es.wikipedia.org

Esto para las redes Lan, para las redes Wlan el diseño varia, las redes inalámbricas como ya se vio con mayor profundidad no es más que un conjunto de computadoras, o de cualquier dispositivo informático comunicados entre sí mediante soluciones que no requieran el uso de cables de interconexión.

En el caso de las redes locales inalámbricas, el sistema que se está imponiendo es el normalizado por IEEE con el nombre 802.11b. A esta norma se la conoce más habitualmente como WI-FI (Wiriless Fidelity).

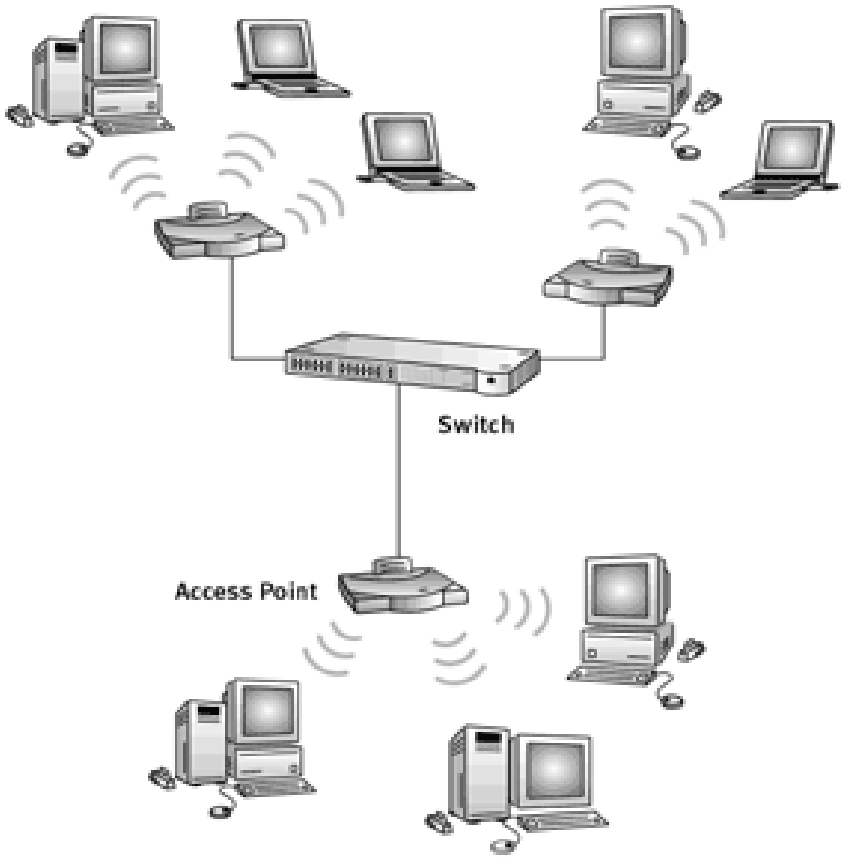
Con el sistema WI-FI se pueden establecer comunicaciones a una velocidad máxima de 11 Mbps, alcanzándose distancia de hasta 150 metros esto en condiciones ideales. No obstante, versiones más recientes de esta tecnología permiten alcanzar los 22, 54 y hasta los 100 Mbps cabe mencionar que esta tecnología se encuentra en desarrollo y por ahora su costo es muy elevado.

Los receptores de una red Wlan son bastante pequeños y pueden integrarse dentro de un dispositivo e incluso llevarlo en un bolsillo.

Una de las principales ventajas del diseño de las redes Wlan es que ante eventos inesperados los cuales podrían ir desde un usuario que se tropieza con un cable o lo desenchufa, hasta un pequeño terremoto o algo similar, responden de manera mucho mas satisfactoria que las redes Lan gracias a su diseño en estos casos una red cableada podría llegar a quedar completamente inutilizada, mientras que una red inalámbrica puede seguir operativa.

A continuación se muestra un diseño característico de una red Wlan como se puede observar en el grafico (figura 4.2) 3 access point están conectados a un switch o enrutador los cuales emiten señales para la comunicación de las diferentes estaciones de trabajo y/o periféricos.

Figura 4.2 Diseño característico de una red Wlan



Fuente: http://es.wikipedia.org

4.2 Estudio comparativo de velocidad entre redes Lan y Wlan.

Aunque se podría pensar que las velocidades de transmisión entre las redes Lan y Wlan podrían ser equivalentes la realidad es otra, en las redes Wlan existen diferentes estándares los mas comunes son 802.11b y 802.11g, los cuales tienen la mayoría de los equipos (generalmente laptops) y que transmite a una frecuencia de 2.4 GHz (la cual como se explico anteriormente es la óptima ,ver figura 3.1.), está disponible casi universalmente con una velocidad de hasta 11 Mbps y 54 Mbps, respectivamente es decir de un 20% a un 50% de la velocidad de las redes cableadas, la cual esta comprendida entre 1 Mbps y 1 Gbps de velocidad al trasmitir.

Cabe mencionar que todavía está en prueba el estándar 802.11n que trabaja a una velocidad de 108 Mbps es como imaginarse la misma velocidad de una red cableada, pero de forma inalámbrica.

Con estas premisas es fácil deducir que las redes inalámbricas ofrecen una velocidad inferior de transmisión de datos que las redes cableadas. Para hablar de forma concisa estamos diciendo que las velocidades no superan habitualmente los 10 Mbps, frente a los 100 que puede alcanzar una red Lan.

4.3 Estudio comparativo de seguridad entre redes Lan y Wlan.

La seguridad de los datos en una empresa hoy en día es un punto primordial el saber blindar la información que se transmite es fundamental para que esta no sea alterada borrada o que tengan acceso a la misma personas no deseadas.

La falta de medidas de seguridad en las redes es un inconveniente que está en aumento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van logrando día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben minimizarse las fallas de seguridad provenientes del interior mismo de la organización.

Con estas deducciones se puede decir que las redes tienen un rol fundamental en la seguridad de la información de una empresa, las redes Lan por ejemplo poseen mayor seguridad puesto que no están expuestas a que cualquier persona ingresen a ellas, es decir, para ello necesitan en primer lugar están dentro de la empresa, después poder conectarse a la red mediante un cable y por ultimo poseer una dirección IP, mientras que en las redes Wlan no se necesita estar dentro de la empresa puesto que se puede acceder a la red estando fuera de ella sin necesidad de cable, y la mayoría de veces una red Wi-fi esta diseñada de tal manera que las direcciones IP se asignan de manera aleatoria ya sea por un mal diseño de la misma o por comodidad del administrador de la misma.

Las redes Lan nos brindan seguridad para acceder a servicios de información internos (Intranet) y externos (Internet) a si como seguridad para el intercambio de archivos se podría decir que las redes Lan son seguras tanto a nivel de datos como a nivel de seguridad personal (numero de tarjetas de crédito por ejemplo).

Como se dijo anteriormente las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Esto fundamentalmente es una ventaja, pero se convierte en una desventaja cuando se piensa que cualquier persona con una computadora portátil solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura no esta definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan las redes Wi-Fi no es de lo más fiables. A pesar de esto también es cierto que ofrece una seguridad valida para la inmensa mayoría de las aplicaciones y que ya hay disponible un nuevo sistema de seguridad (WPA) que hace a Wi-Fi mucho más confiable.

En una Wlan cualquier persona con una terminal inalámbrica podría comunicarse con un punto de acceso privado si no se disponen de las medidas de seguridad adecuadas. Dichas medidas van encaminadas en dos sentidos: por una parte está el cifrado de los datos que se transmiten y en otro plano, pero igualmente importante, se considera la autenticación entre los diversos usuarios de la red. En el caso del cifrado se están realizando diversas investigaciones ya que los sistemas considerados inicialmente se han conseguido descifrar. Para la autenticación se ha tomado como base el protocolo de verificación EAP (Extesible Authentication Protocol), que es bastante flexible y permite el uso de diferentes algoritmos.

4.4 Estudio comparativo de ventajas entre redes Lan y Wlan.

LAN	WLAN
• Costos relativamente bajos • Ofrece el máximo rendimiento posible • Seguridad para Acceder a servicios de información internos (Intranet) y externos (Internet). • Seguridad para el intercambio de archivos. • El sistema de cableado estructurado permite que muchos servicios estén presentes en la red (voz, datos, vídeo, etc.) con la misma instalación, independientemente de los equipos y productos que se utilicen • Se facilita y agiliza mucho las labores de mantenimiento. • Es fácilmente ampliable • El sistema es seguro tanto a nivel de datos como a nivel de seguridad personal. • Una de las ventajas básicas de estos sistemas es que se encuentran regulados mediante estándares, lo que garantiza a los usuarios su disposición para las aplicaciones existentes, independientemente del fabricante de las mismas, siendo soluciones abiertas, fiables y muy seguras.	• 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 alámbrica. • Simplicidad y rapidez en la instalación: La instalación de una red inalámbrica puede ser tan rápida y fácil y además que puede eliminar la posibilidad de lanzar cable a través de paredes y techos. • Flexibilidad en la instalación, la tecnología inalámbrica permite a la red ir donde la alámbrica no puede ir. • 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. • Los sistemas de WLANs pueden ser configurados en una variedad

Fundamentalmente la norma TIA/EIA-568A define entre otras cosas las normas de diseño de los sistemas de cableado, su topología, las distancias, tipo de cables, los conectores, etc. • Al tratarse de un mismo tipo de cable, se instala todo sobre el mismo trazado • El tipo de cable usado es de tal calidad que permite la transmisión de altas velocidades para redes. • Tecnología broadcast (difusión) con el medio de transmisión compartido. • Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps • No hace falta una nueva instalación para efectuar un traslado de equipo • La simplicidad del medio de transmisión que utiliza (cable coaxial, cables telefónicos y fibra óptica) • La facilidad con que se pueden efectuar cambios en el hardware y el software • Gran variedad y número de dispositivos conectados • Posibilidad de conexión con otras redes	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. • Al no usar cables, se evitan obras para lanzar cable por muros y techos, mejorando así el aspecto y la habitabilidad de los locales, y reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios temporales de la red.

4.5 Estudio comparativo de desventajas entre redes Lan y Wlan.

DESVENTAJAS REDES LAN:

- El costo de instalación siempre ha sido un problema muy común en este tipo de tecnología, ya que el estudio de instalación, las canaletas, conectores, cables y otros no mencionados suman costos elevados en algunas ocasiones.

- El acceso físico tiene ciertos inconvenientes en las redes alámbricas. Ya que para llegar a ciertos lugares dentro de la empresa, es muy complicado el paso de los cables a través de las paredes de concreto u otros obstáculos.

- Dificultad y expectativas de expansión es otro de los inconvenientes ya que cuando pensamos tener un numero definidos nodos en una oficina, la mayoría del tiempo hay necesidades de construir uno nuevo y ya no tenemos espacio en los switches instalados.

- Extensión máxima no superior a 3 Km.

DESVENTAJAS REDES WLAN:

- Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas Wi-Fi lo hacen a 11 Mbps. Es cierto que existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tiene un precio superior al de los actuales equipos Wi-Fi.

  Aunque el 802.11n aun no ha sido aprobado oficialmente, actualmente se trabaja en distintos estándares como en el 802.11r que mejora el movimiento entre distintos puntos de acceso o el 802.11 VHT que pretende mejorar la velocidad del Wi-fi hasta en 1Gbit por segundo , pero estos son solo prototipos que en la actualidad no están disponibles.

- Para la mayoría de las configuraciones de la red local, el coste de los equipos de red inalámbricos es superior al de los equipos de red cableada.

- Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda de 2,4 Ghz. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes Wi-Fi funcionan en la misma banda de frecuencias incluida la de los vecinos. Este hecho hace que no se tenga la garantía de nuestro entorno radio electrónico este completamente limpio para que nuestra red inalámbrica funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

- La tecnología que actualmente se esta instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi (IEEE 802.11B). Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad, es posible que, cuando se popularice esta nueva tecnología, se deje de comenzar la actual o, simplemente se deje de prestar tanto apoyo a la actual.

  Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades del cliente y, aunque existe una incógnita, los fabricantes no desearían perder el tirón que ha supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales. La historia nos ha dado muchos ejemplos similares.

- Otro de los problemas que presenta este tipo de redes es que actualmente (a nivel de red local) no alcanzan la velocidad que obtienen las redes de datos cableadas. Además, en relación con el apartado de seguridad, el tener que cifrar toda la

información, supone que gran parte de la información que se transmite, sea de control y no de información útil para los usuarios, por lo que incluso se reduce la velocidad de transmisión de datos útiles.

- Dadas las interferencias existentes al tratar de implementar redes Wlan se puede llegar a decir que podría ser imposible el implantar en algunos entornos industriales las redes Wlan dados los fuertes campos electromagnéticos y cumplir así ciertos requisitos de calidad propios de las empresas.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones estudio comparativo de diseño entre redes Lan y Wlan.

En la fase final del estudio técnico comparativo se va a proceder a dar ciertas conclusiones que a su vez podrían ser tomadas como recomendaciones para el aprovechamiento al máximo tanto de redes Lan como Wlan:

El avance vertiginoso de los sistemas de computación, su fácil manejo e innumerables funcionalidades que ofrece, ha permitido el incremento del número de usuarios que trabajan con computadoras, dando como resultado el crecimiento del Internet; una vía de comunicación efectiva y eficaz, la cual une al mundo se han desarrollado aplicaciones que hace no mas de 2 décadas estaban destinadas solo para guiones de películas de ciencia ficción.

Las redes LAN permiten a los usuarios trabajar de una forma sencilla y efectiva, al mismo tiempo brinda seguridad en cuanto a la información ya que esta protegida por firewall[13].
Por otra parte el Intranet nos permite trabajar entre varias personas de una organización en proyectos, compartir información, llevar a cabo conferencias visuales y establecer procedimientos seguros para el trabajo de producción.

El desarrollo de las redes Wlan representa el siguiente escalón en la tecnología de redes, ya que permitirá dotar a las redes convencionales de nuevas posibilidades. Dentro de este marco se elaborarán arquitecturas para clientes, servidores, proxies, etc., que darán como resultado un mejor aprovechamiento de esta tecnología y por ende una solución a los inconvenientes que por ahora presenta.

13.- Combinaciones de hardware y software que solo permite a ciertas personas acceder a ella para propósitos específicos.

Las principales capacidades de las tecnologías inalámbricas pasan por el aumento de la movilidad y la flexibilidad en las redes. Para el correcto desarrollo de estas características es necesario que existan los terminales móviles (portátiles, PDAs), que deben ser los principales beneficiarios de estas tecnologías. De modo que el desarrollo de las WLAN irá ligado al del mercado de dichas terminales.

5.2 Conclusiones estudio comparativo de velocidad y rendimiento entre redes Lan y Wlan.

Las velocidades entre redes Lan y Wlan difieren mucho y se podría decir que las redes Wlan no tienen una velocidad satisfactoria para el envió y recepción en aplicativos complejos como multimedia actualmente no alcanzan la velocidad que obtienen las redes de datos cableadas.

La velocidad máxima de transmisión inalámbrica de la tecnología 802.11b es de 11 Mbps. Pero la velocidad típica es solo la mitad: entre 1,5 y 5 Mbps dependiendo de si se transmiten muchos archivos pequeños o unos pocos archivos grandes. La velocidad máxima de la tecnología 802.11g es de 54 Mbps. Pero la velocidad típica de esta última tecnología es solo unas 3 veces más rápida que la de 802.11b: entre 5 y 15 Mbps.

Hay que tener en cuenta también la tasa de error debida a las interferencias habituales en las redes Wlan. Estas pueden oscilar alrededor de 10-4 frente a las 10-10 de las redes cableadas. Esto representa 6 órdenes de magnitud de diferencia y esto es significativo en transmisión de información, estamos hablando de 1 bit erróneo cada 10.000 bits o lo que es lo mismo, aproximadamente de cada Megabit transmitido, 1 Kbit será erróneo.

5.3 Conclusiones estudio comparativo de seguridad entre redes Lan y Wlan.

La seguridad hoy en día es un punto que no hay que pasar por alto. Muchas de las organizaciones que instalan WLANs no contemplan la seguridad como una de sus prioridades. Es importante en cualquier organización la implantación de políticas de uso y seguridad. De esta manera todos los que pertenecen a la organización, se hacen responsables y concientes del uso y de la seguridad de la red y no se deja esa labor a una sola persona, como seria el caso del administrador de la red.

En lo que respecta a los dispositivos WLAN, se debe tomar en cuenta que las especificaciones definidas por los estándares son probadas en condiciones ideales, por lo tanto, son sólo teóricas . En la práctica, estos parámetros pueden variar dependiendo de donde y cómo sean instalados y configurados tales equipos.

La planeación y el diseño en una red, por más pequeña que sea, nos permitirá sacarle el máximo provecho, logrando un mejor desempeño en términos de velocidad de transmisión al correr nuestras aplicaciones y una mayor seguridad de nuestra información. Es importante planear y diseñar, antes de comprar, instalar y configurar cualquier red.

5.4 Conclusiones y recomendaciones finales sobre el estudio técnico comparativo

El progresivo abaratamiento de los ordenadores, incluidos los portátiles, facilitan la expansión de las redes domésticas e inalámbricas, y estas en un futuro se convertirán en algo normal en las casas debido a la facilidad de instalación y a la capacidad de interconexión con otros dispositivos pertenecientes al campo de la vida cotidiana.

De todo lo visto cabe destacar que las redes inalámbricas son algo real y que ya se ha conseguido implementar con éxito en diversos sectores. Además proporcionan ciertas características como la movilidad y la flexibilidad que con las redes cableadas son complicadas de obtener se convierten en imprescindibles para entornos cambiantes o que requieran gran capacidad de adaptación.

En cuanto a la tecnología a emplear parece estar bastante desarrollada, por lo que esto no es un problema en el desarrollo de este tipo de redes.

El auge que actualmente vive esta tecnología se debe fundamentalmente a que es capaz de ofrecer la movilidad de la que se carece el equipamiento tradicional (redes Lan), manteniendo unas prestaciones, coste y complejidad de conexión razonables; así, a efectos prácticos de aplicación, se puede considerar que una tasa de transferencia teórica que parte de los 11 Mbps permite toda una serie de aplicaciones de los entornos de trabajo más habituales, que no son grandes consumidoras de ancho de banda, tales como por ejemplo:

- Acceso a la información y la navegación web
- Consulta de correo electrónico
- Acceso a herramientas de trabajo colaborativo, entre otras.

El aporte de la movilidad significa un beneficio para los usuarios que, dependiendo del perfil de cada uno de ellos, podrán ganar en eficiencia, productividad o, simplemente en la oportunidad de realizar una consulta dada en un momento dado.

Para un óptimo funcionamiento de una red ya sea alámbrica o inalámbricas es fundamental desde mi experiencia en el manejo de este tipo de redes el designar a un responsable técnico del sistema que sea quien planifique y mantenga operativa la red local.
El administrador de la red local es una figura clave en el éxito de su funcionamiento, es quien mantiene los archivos y recursos, así como previene consecuencias nefastas siguiendo los procedimientos de seguridad (antivirus, copias de seguridad, etc.).
También decide los privilegios de cada uno de los usuarios o grupos de usuarios de la LAN restringiendo convenientemente el uso de sistemas vitales sólo al personal adecuado.

Algunas de las funciones de mantenimiento del administrador de la LAN deberían ser:

- Mantener operativa la red local.
- Decidir e implementar la política de seguridad en la red.
- Privilegios de los usuarios.
- Antivirus.
- Copias de seguridad.
- Búsqueda de mayores capacidades.
- Investigar nuevas soluciones o sistemas.
- Instalación de nuevos dispositivos y nuevos software

Cada día se facilita más el trabajo del administrador con la aparición de nuevas utilidades y herramientas de automatización de las tareas más habituales. Muchas de estas tareas pueden ser programadas para que se ejecuten de forma automática. Es el caso de las copias de seguridad o de la distribución de un antivirus por los distintos equipos de la red.

De todo lo mencionado anteriormente se podría tener como gran conclusión que las 2 tecnologías tienen sus fortalezas y debilidades y cada una de ellas tiene mayor aplicación en ciertos ámbitos, es decir, no se puede pretender configurar una red cableada en un centro comercial, centro de convenciones, parques o sitios públicos en donde acceder al Internet cada vez es mas frecuente, en estos casos sería optimo el uso de redes Wlan aunque se deberían de reforzar las medidas de seguridad de acceso a la llamada red de redes, mediante el asignamiento de direcciones IP de forma manual y no aleatoria (DHCP) esto claro implicaría que una persona, administrador de red, este constantemente fijando dichas direcciones, lo que podría ser muy tedioso para los usuarios de un centro comercial.

Por otro lado las redes Lan son mucho mas confiables en el aspecto de seguridad, velocidad, rendimiento y hasta diseño dada una buena planificación de la misma con cableado estructurado por ejemplo y equipo de comunicaciones (enrutadores o Switchs) de una calidad razonable, dado esto las redes Lan serian una decisión acertada para puntos estratégicos de una empresa en donde también se podrían dar combinaciones de los 2 tipos de red, es decir, red cableada para la organización y sus colaboradores y una red inalámbrica para los clientes en la sala de espera, eso si con restricciones de acceso o tan solo limitarlos para el uso de Internet y denegar el acceso de los mismos a los archivos o

estaciones de trabajo de la empresa, esto se puede conseguir fácilmente mediante un corta fuegos (firewall) en donde se asignan direcciones ip estáticas, esto a parte de seguridad nos permitiría resguardar el uso de nuestro ancho de banda, poniendo restricciones para aplicaciones punto a punto (peer to peer) .

Hoy en día dadas tantas aplicaciones informáticas su uso es cada vez mas común, frecuente y necesario en las actividades diarias, el dar una recomendación de cual seria la red optima para el envió y recepción de información seria infructuoso y el motivo de el presente estudio no fue ese, sino mas bien el conocer determinar y plasmar en donde las redes Lan y Wlan presentan puntos robustos y donde flaquean al momento de ser instaladas.

ANEXO A

GLOSARIO DE TÉRMINOS	
Software	Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora
Hardware	Conjunto de los componentes que integran la parte material de una computadora.
Hipertexto	Texto que contiene elementos a partir de los cuales se puede acceder a otra información
.com	Se utiliza para designar los nombres de dominio propios de entidades comerciales o empresariales
OSI	Organización Internacional de Normalización/Interconexión de Sistemas Abiertos.
HTTP	Acrónimo de HyperText Transfer Protocol, protocolo de transferencia de hipertexto. Se utiliza en las transferencias de información de páginas en Internet, de tal forma que puedan ser visualizadas en un navegador o explorador
FTP[7]	Acrónimo de File Transfer Protocol, protocolo de transferencia de archivos que se utiliza en Internet y otras redes para transmitir archivos entre servidores o entre un usuario y un servidor
Ethernet	Especificación de red de área local (LAN) desarrollada en 1976 por Xerox, en cooperación con DEC e Intel, originalmente para conectar los mini ordenadores del Palo Alto Research Center (EEUU).
IEEE	Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos
HyperLAN	HiperLAN (HIgh Performance Radio LAN) es un estándar de redes inalámbricas
ETSI	Escuela Técnica Superior de Ingenieros European Telecommunications Standards Institute
HomeRF	Estándar que pretendía diseñar un aparato central en cada casa que conectara los teléfonos y además proporcionar un ancho de banda de datos entre las computadoras.
802.11	Estándar ratificado por la IEEE en 1997, trabaja en la banda de frecuencia de 2.4GHz con velocidades hasta de 2Mbps.
802.11b	Estándar ratificado por la IEEE en 1999, trabaja en la banda de

	frecuencia de 2.4GHz con velocidades hasta de 11Mbps, conocido como Wi-Fi.
802.11a	Estándar ratificado por la IEEE en 1999, trabaja en la banda de frecuencia de 5GHz con velocidades hasta de 54Mbps, conocido como Wi-Fi5.
AP	Access Point, punto de acceso inalámbrico.
DSSS	Direct Sequence Spread Spectrum, espectro disperso de secuencia directa
DHCP	Dinamic Host Control Protocol, protocolo de asignación dinámica de direcciones IP
FHSS	Frequency Hopping Spread Spectrum, Espectro disperso con salto en frecuencia
GHz	Abreviación de GigaHertz. Un GHz representa un mil millones de ciclos por segundo.
IP	Internet Protocol, protocolo de Internet
LAN	Local área Network, red de área local.
LDAP	Lightweight Directory Access Protocol, sistema para autenticar usuarios para conectarlos a la red o con un ISP.
MAC	Media Access Control, control de acceso al medio.
Mbps	Abreviación de Megabits por segundo. Mbps es una medida utilizada para la transferencia de datos.
MHz	Abreviación de MegaHertz. Un MHz representa un millón de ciclos por segundo.
NIC	Network Interface Card, se refiere a interfase de red de computadora.
OFDM	Orthogonal Frequency Division Multiplexing, tipo de modulación para comunicaciones digitales inalámbricas.
RADIUS	Remote Authentication Dial-In User Service, sistema para autenticar remotamente usuarios.
RF	Radio Frecuencia.
SSID	Service Set Identifier, identificador del Conjunto de Servicios de

	una WLAN.
SSL	Secure Sockets Layer, protocolo de encriptación seguro a nivel de sockets
TLS	Transport Layer Security, protocolo de encriptación seguro en la capa de transporte
VPN	Virtual Private Network, redes privadas virtuales
WEP	Wired Equivalent Privacy, técnica de seguridad implementada en redes inalámbricas.
Wi-Fi	Wireless Fidelity, nombre con el que se le conoce al estándar 802.11b.
WLAN	Wireless Local área Network, red de área local inalámbrica.
Browser	Es un programa de software que es instalado en la computadora para permitir la navegación en la red.
Filtros:	Reglas que se establecen para evitar que determinados e-mail lleguen, pueden ser borrados automáticamente. Si provienen de determinada fuente o contiene un asunto especifico.
Firewall:	Un dispositivo de seguridad que previene de usuarios que usuarios no autorizados puedan entrar a redes privadas, como una red corporativa.
Cliente-servidor	Describe la relación entre dos computadoras diferentes.
Protocolos	Son las reglas que controlan la forma en que se transfieren paquetes de información de una estación de trabajo a otra.
Señal Análoga	Una señal continua, como la que se envía por teléfono.
Señal Digital	Una señal de encendido y apagado, el 0 y el 1 de la información de una computadora.
Router	Una computadora que redirige información

REFERENCIAS BIBLIOGRAFICAS:

- Redes Lan & Wan / FRANK DERFLER
- Instalación Y Mantenimiento de Servicios de Redes de Área Local./ MARTIN ROMERO, ARTURO.
- http://www.monografias.com/trabajos14/wi-fi/wi-fi.shtml
- http://es.wikipedia.org/wiki/WLAN
- http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/tiposde.htm
- http://www.abcdatos.com/tutoriales/tutorial/z1544.html
- http://www.psicofxp.com/forums/redes-informaticas.113
- http://redesinaalam.blogspot.com/
- http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica
- http://es.wikipedia.org/wiki/Red_de_computadoras#Clasificaci.C3.B3n_de_redes
- http://es.wikipedia.org/wiki/LAN
- http://www.redaragon.com/informatica/wireless/redwireless.asp
- http://andrade.espacioblog.com/post/2008/05/23/clasificacion-las-redes
- http://www.eveliux.com/mx/el-abc-de-las-redes-inalambricas-wlans.php
- http://www.poynting.co.za
- http://www.proxim.com
- http://www.uah.es (Universidad de Alcalá de Henares)
- http://www.multipoint.com.ar
- http://www.zonabluetooth.com
- http://www.ericsson.com
- http://www.okeda.com.ar