UNIVERSIDAD LASALLISTA BENAVENTE

ESCUELA DE INGENIERÍA EN COMPUTACIÓN

Con estudios incorporados a la

Universidad Nacional Autónoma de México

CLAVE: 8793-16

"PROYECCIÓN DE REDES A FUTURO: REDES INALÁMBRICAS"

TESIS

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

ULISES RANGEL CANCHOLA

Asesor: ING. CLAUDIA PATRICIA ROJANO HERNÁNDEZ

Celaya, Gto. **Junio de 2003**

AGRADECIMIENTOS

DIOS

Quiero agradecerte por acompañarme en este camino y por no dejarme solo cuando te necesite y por tenerme paciencia, que aunque muchas veces no te di la mano para agradecerte, en este momento lo hago y te doy gracias por todo lo que me has dado y espero que me sigas iluminando en este camino porque es difícil y necesitaré de tu ayuda siempre. Gracias señor!!!

A MIS PADRES

Les doy las más infinitas gracias de todo corazón por estar conmigo en las buenas y en las malas, por no dudar de mí en ningún momento, pero sobre todo por todo el amor y comprensión que me han dado a lo largo de todo este tiempo. Gracias por enseñarme lo que vale la vida, por enseñarme a apreciar cada momento de mi vida, por dedicarme su tiempo y darme todo sin esperar nada a cambio.

Me siento el hombre más afortunado del mundo por tenerlos a ustedes como mis padres, los amo.

MUCHAS GRACIAS.

A MI HERMANO

Gracias por el apoyo que me has dado, por estar ahí siempre y por los sabios consejos que me diste. Te estoy eternamente agradecido, eres un ejemplo, gracias.

A MI ABUELITA

Se que me estás viendo desde allá arriba, gracias por cuidarme, por consolarme cuando lloraba y por dedicarme tanto tiempo de tu vida, Dios te bendiga.

A MI ESPOSA

Te agradezco por todo lo que has hecho por mí, por escucharme, por ser mi amiga, por no dejarme caer y regañarme las veces que lo necesité. Te admiro por lo que eres y por lo que has logrado, la forma en la que luchas cada día por ser mejor persona, madre y esposa.

TE AMO.

A MIS HIJOS

Esto es por ustedes, son el mejor regalo que he recibido por parte de Dios, son mi luz y mi motivación para seguir adelante y con la frente en alto.

LOS AMO.

Por último quiero agradecerle a todos los que nunca creyeron en mí, porque gracias a su mala voluntad me esforcé más e hice que mi sueño de ser alguien en la vida se cumpliera.

INDICE

CAPITULO III

DISPOSITIVOS UTILIZADOS EN LAS REDES INALÁMBRICAS, WIRELESS LAN Y ESTÁNDAR IEEE 802.11

CAPITULO IV

LAN HÍBRIDA COAXIAL/INFRARROJOS, SEGURIDAD Y VPN'S

CAPITULO V

REDES INALÁMBRICAS CON LINUX

INTRODUCCIÓN

El objetivo de esta tesis es el conocer las ventajas y desventajas de las redes inalámbricas, su funcionamiento y describir las nuevas tecnologías para el mejoramiento del uso de éste tipo de redes, describir el funcionamiento de redes híbridas, es decir, conectando redes inalámbricas y redes tradicionales de cableado estructurado para mejor desempeño.

Las redes han sido la clave en la recolección, procesamiento y distribución de información, ya que de estas dependen muchísimas empresas para su buen funcionamiento y mantener un nivel competitivo; se dice que la empresa que posea más información es la que va a sobrevivir más tiempo.

A medida que crece nuestra habilidad para producir, recolectar y procesar información, crece la demanda para sistemas de información más sofisticados y poderosos; dicha demanda se incrementa con el paso del tiempo y se requieren de sistemas cada vez más rápidos para satisfacer las demandas de los usuarios.

La industria de las computadoras ha tenido un desarrollo impresionante en muy corto tiempo, reemplazando esquemas de trabajo viejos que antes se basaban en una sola computadora que hacía el proceso de la información. Ahora se interconectan varias computadoras o terminales entre sí para lograr una mayor rapidez y eficacia en cuanto al ordenamiento y procesamiento de la información vital para la empresa.

Estos sistemas de computadoras conectados entre sí, es lo que conocemos como ***"Redes de computadoras".*** Estas nos dan a entender un grupo de computadoras autónomas interconectadas. Al indicar que las computadoras son autónomas, se excluyen los sistemas en los que una computadora pueda forzosamente arrancar, parar o controlar a otra, éstos no se consideran autónomos.

Se dice que una computadora esta en ***RED***, si es capaz de intercambiar información con varias computadoras. Se pueden interconectar entre ellas con el ya conocido *"cable UTP"*, *"fibra óptica"* o bien *"cable coaxial"*, pero sin duda una de las tecnologías más discutidas de estos tiempos, es la de poder interconectar a las computadoras con una tecnología ***"INALÁMBRICA".***

La conexión de computadoras mediante luz infrarroja, esta siendo ampliamente investigada, las redes inalámbricas facilitan la operación en lugares en donde las computadoras no pueden permanecer mucho tiempo en un solo lugar o cuando se tienen computadoras en varios pisos o en edificios diferentes.

Pero en realidad tenemos que enfrentar un problema, esta tecnología apenas esta empezando a ser aceptada, y todavía no se sabe a ciencia cierta si las redes de tecnología inalámbrica puedan llegar a sustituir a las redes de cableado estructurado. El primer problema al que nos enfrentamos es que las redes de cableado estructurado alcanzan velocidades de transmisión muy altas y hasta ahora la velocidad mayor lograda en la tecnología inalámbrica es de 10Mbps, aunque hay dispositivos inalámbricos que alcanzan velocidades de 100Mbps, pero las redes de cableado estructurado alcanzan velocidades de 10Mbps y 1000Mbps, pensando a futuro, se espera que las redes inalámbricas alcancen velocidades de 1000Mbps, como el Gigabit Ethernet.

CAPITULO I

CARACTERÍSTICAS DE LAS REDES

1.1 ¿QUÉ ES UNA RED?

Una red es la manera de conectar varias computadoras entre sí, ya sea por medio de cable UTP (Unshield Twisted Pair), fibra óptica, cable coaxial o bien vía inalámbrica, estas comparten recursos e información para agilizar el trabajo en las oficinas y el intercambio de información, con la finalidad de hacer más eficiente el ordenamiento de los datos en lapsos más cortos de tiempo y con ello contar con estos de manera oportuna.

Cuando las computadoras empezaron a entrar en el área de los negocios, el conectar dos o tres computadoras nos traía ventajas pero esto se mejoro cuando aparecieron los sistemas *multiusuarios*. Un sistema *multiusuario* es el que cumple simultáneamente con las necesidades de dos o más usuarios que comparten los mismos recursos, es decir, si un usuario requiere de imprimir algún documento en especial, se manda la petición y el sistema *multiusuario* (Windows, Linux etc.) procesa la petición, recorre la red hasta localizar a la computadora que tiene instalada la impresora y prosigue a imprimir el documento, siempre y cuando dicha impresora este *"compartida"*.

En un principio se manejaba lo que eran terminales *"tontas"*, es decir no tenían procesador ni disco duro y estas terminales *"tontas"* las manejaba una computadora central o servidor, este almacenaba la información capturada de las terminales.

1.2 CARACTERÍSTICAS Y OBJETIVOS DE LAS REDES

Las redes en general "comparten recursos", estos recursos pueden ser utilizados por los usuarios, uno de los objetivos de las redes es que estos recursos y la información este disponible para el usuario que lo solicite. Es decir, si un usuario esta a 30 o 1000Km de la información, esta debe de estar disponible como si fuera de origen local.

También es importante destacar que las redes tienen la ventaja de acortar la distancia en el intercambio de datos, en otras palabras, los usuarios pueden recibir información de una persona que esté en otro país en cuestión de segundos o minutos, dependiendo del tamaño de esta y la velocidad de transmisión. Un ejemplo muy claro es el ***"Internet"***, es una ***RED*** mundial.

Para llegar a comprender lo que son las redes, debemos familiarizarnos con algunos conceptos básicos:

- ✓ Protocolo: Permite que los equipos se comuniquen a través de una red.
- ✓ Paquete: Es un conjunto de datos que se transmite en una red, es de longitud variable según el protocolo que se utilice.
- ✓ TCP: Proporciona un servicio de comunicación que parece un circuito, es decir, el flujo de información entre el origen y el destino parece que sea continuo.
- ✓ Puerto: Es un número que identifica a una aplicación que interviene o va a intervenir en una comunicación bajo TCP.
- ✓ Socket: Es la combinación del IP de la máquina y el número de puerto utilizado por el TCP
- ✓ IP: El protocolo IP proporciona un sistema de distribución que es poco fiable incluso en una base sólida. El protocolo IP especifica que la unidad básica de transferencia de datos en el TCP/IP es el datagrama.
- ✓ Datagrama: Es un conjunto de datos o información enviados en el Internet.
- ✓ TCP/IP: Protocolo de control de transmisión / protocolo de Internet. Es un protocolo de red para controlar el flujo de datos en las redes de área local (LAN) y las redes de área extensa (WAN).
- ✓ Microsoft Network (NetBEUI): Es un protocolo utilizado en las redes basadas en el Microsoft LAN Manager. Es muy rápido en pequeñas redes de 12 computadoras y equipos que no muevan ficheros de gran tamaño, se recomienda utilizar alguna opción mejor.

- ✓ ARP (Address Resolution Protocol): El protocolo ARP se encarga de convertir las direcciones IP en direcciones de red física.
- ✓ RARP (Reverse Address Resolution Protocol): Es el encargado de asignar una dirección IP a una dirección física.
- ✓ Mascaras: Se utiliza para dividir o subdividir lógicamente a una red.
- ✓ Gateway: Ordenador o dispositivo que conecta redes de diferente protocolo.
- ✓ Router (Ruteador): Es un elemento de Hardware que trabaja a nivel red, tiene como propósito conectar una LAN a una WAN. Tiene la capacidad de asignar el encabezado del paquete a una ubicación de una LAN y elige la mejor ruta de acceso para el paquete, con lo que optimiza el rendimiento de la red.
- ✓ Mascara de subred: Es un parámetro de configuración de TCP/IP que extrae la configuración de red y de host a partir de una dirección IP. Este valor de 32 bits permite que el destinatario de los paquetes IP distinga, en la dirección IP, la parte de ID de red (nombre del dominio) y el ID de host (nombre del host).

Ya familiarizados con los conceptos anteriores, nuestro entendimiento de lo que son las redes y cómo funcionan será más amplio ya que estos términos son frecuentemente utilizados en el estudio de las redes.

1.3 FORMAS DE TRANSMISIÓN DE DATOS EN LAS REDES

Existen dos medios para la transmisión de datos en las redes:

- ✓ Terrestre: Transmiten la señal por conducto físico.
- ✓ Aéreo: Transmiten y reciben por microondas, ondas electromagnéticas, infrarrojo o rayo láser.

Terrestre:

- ✓ Cable UTP o par trenzado: Es el que comúnmente utilizamos para interconectar las computadoras. Consiste de dos filamentos de cobre, cada uno forrado por un plástico aislante, entrelazados entre sí. Este entrelazado básicamente es para evitar la diafonía y atenuación que pueda existir. Hay dos tipos de cable trenzado, el comúnmente utilizado en las líneas telefónicas, no protege casi nada de interferencias.
- ✓ Cable Coaxial: Es muy utilizado en las redes debido a su buen funcionamiento y su amplio ancho de banda. Esta bien cerrado y la transmisión de datos es muy buena bajo una pantalla sólida y un exterior muy resistente.
- ✓ Fibra Óptica: Actualmente se está sustituyendo a los cables coaxiales y al par trenzado por fibra óptica, todo esto debido a su gran desempeño para transmitir miles de millones de bits, además los impulsos luminosos no son dañados por la radiación del ambiente.

1.4 Componentes de una RED

La forma básica de cómo se compone una red es la siguiente:

- ✓ Servidor (Server): El servidor es la máquina principal de una *red*, es la que se encarga de administrar los recursos y el flujo de la información. Muchos de los servidores son *"dedicados"*, es decir, que tiene tareas específicas. Por ejemplo un *servidor* para comunicaciones, sólo para controlar el flujo de los datos, un *servidor* de impresiones, sólo para imprimir...etc. Un servidor debe de tener ciertas características, como una amplia memoria para correr los distintos programas, una gran capacidad de disco duro para poder almacenar todo la información y que sea de alto rendimiento en cuanto a velocidad y procesamiento.
- ✓ Sistema operativo de RED: Es el sistema que se encarga de administrar la *red* de manera general y para esto debe de ser un sistema multiusuario. Existen diversos tipo de sistemas para administrar las redes, como por ejemplo Unix, Windows NT, Netware de Novell, Linux...etc.
- ✓ Estación de trabajo (Workstation): Es una computadora que se encuentra físicamente conectada al servidor por medio de algún tipo de cable, ya sea el cable UTP, cable coaxial o fibra óptica. Esta computadora cuenta con sistema operativo propio y solo se necesita agregarla al grupo de trabajo para que se conecte a la *RED* y así poder trabajar en ella.
- ✓ Recursos para compartir: Al hablar de recursos a compartir nos referimos a todos aquellos dispositivos que por su alto costo no se puede tener uno para cada computadora, como lo son las impresoras láser, escáner, plotters etc. También se pueden compartir los archivos o programas de alguna máquina en específico y poder hacer uso de ellos, esto a través de los permisos concedidos por el administrador de la *red.*

- ✓ Hardware de RED: Básicamente el hardware de *red* es el dispositivo por el cual conectamos la maquina en red, estos componentes son las tarjetas de red, el cable por el cual se conecta la tarjeta y las estaciones de trabajo en si.
- ✓ Dispositivos de conectividad: Proporcionan la facilidad de conectar varias LAN de diferentes tipos y así tener una especie de *red* homogénea; estos dispositivos son los ruteadores, bridges, switch, hub etc.

Básicamente estos son los componentes de mayor relevancia en la arquitectura de las redes, estos pueden cambiar dependiendo las necesidades que se tengan en alguna empresa o escuela.

1.5 TIPOS DE REDES

Según el lugar y el espacio que ocupen, las redes se pueden clasificar de la siguiente manera:

1. Redes **LAN** (Local Area Network) o Redes de área local: Éste tipo de redes son las que se expanden dentro de un área relativamente pequeña, es decir, están dentro de edificios. Así mismo una LAN puede estar conectada con otras LAN's por medio de cable de línea telefónica o microondas. Las LAN's pueden transmitir a velocidades muy altas, algunas inclusive más rápido que por línea telefónica pero las distancias son limitadas.

A su nivel más elemental una LAN no es más que un medio compartido (en ella se comparten impresoras, escáner y otro tipo de periféricos y cuenta con una serie de restricciones para los usuarios).

2. Redes **WAN** (Wide Area Network) o Redes de área amplia: Este tipo de red es la que esta compuesta por varias redes LAN, estas redes LAN interconectadas entre si es lo que conocemos como una red **WAN.**

Cubren un área extensa y se interconectan por medio de cable telefónico, coaxial, fibra óptica o por medio de enlaces aéreos o satélites. Entre las WAN's más grandes de el mundo se encuentra la **ARPANET**, que fue creada por la Secretaría de la Defensa de Estados Unidos y se convirtió en lo que ahora se conoce como ***"INTERNET"*** y a la cual a su vez se le conectan pequeñas redes de escuelas, dependencias gubernamentales etc.

3. Redes **INFRARROJAS**: Estas redes están limitadas por el espacio ya que no tienen longitudes de emisión muy amplios. Generalmente se encuentran en un solo cuarto o piso. Algunas compañías que tienen sus oficinas en varios edificios utilizan las ventanas como medio de emisor/receptor, es decir, se ponen en las ventanas un puerto infrarrojo que recibe y envía la señal. Un ejemplo muy vago es cuando al momento de encender nuestra televisión el control remoto emite una señal infrarroja y ésta es recibida por el modulo receptor, así es como funciona el intercambio de datos en las redes infrarrojas. Pero estas redes tienen un problema, no se sabe a ciencia cierta qué estándar se va a utilizar en cuanto al tipo de frecuencia que se requiera para la transmisión de la información, esto con la finalidad de no interferir con otras frecuencias utilizadas; por ejemplo las usadas por radiodifusoras, celulares etc. Los países se están poniendo de acuerdo para ver que banda van a implementar para la transmisión y el tipo de frecuencia que deben utilizar.

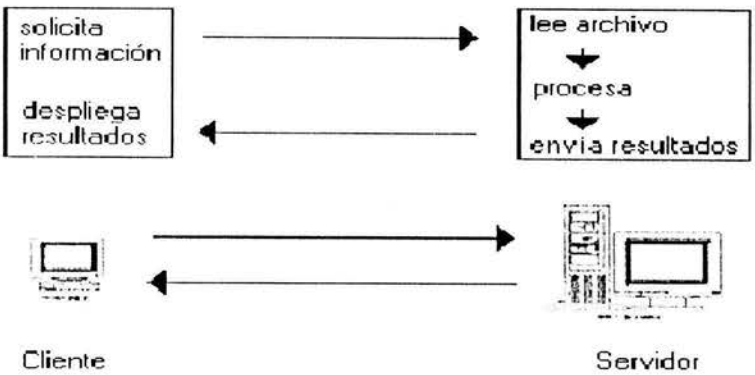
4. Redes de **RADIOFRECUENCIA**: Por otro lado las *redes de radiofrecuencia,* básicamente la idea es tomar una señal de banda convencional y distribuir su energía en un dominio más amplio de frecuencia. *"Así, la densidad promedio de energía es menor en el espectro equivalente de la señal original. En aplicaciones militares el objetivo es reducir la densidad de energía abajo del nivel de ruido ambiental de tal manera que la señal no sea detectable. La idea en las redes de*

Falta página

N° 8

No tiene que atender al usuario de manera directa si no que tiene la funcionalidad de atender a varios clientes al mismo tiempo. Algunos de los sistemas operativos que manejan redes "*cliente servidor*" son: Windows NT, NetWare de Novell, VINES de Banyan y LAN Server de IBM entre otros. Todos estos sistemas operativos de red, pueden realizar procesos solicitados por los clientes de manera simultánea ya que son sistemas "*multitarea*" (Fig. 1)[2].

Fig. 1 Red Cliente/Servidor



1.7 MÉTODOS DE ACCESO AL MEDIO

1.7.1 TOKEN RING

También conocido como IEEE 802.5, fue creada por IBM y algunos otros fabricantes. Opera con velocidades que van desde los 6 Mbps ó 16 Mbps, Token Ring emplea una topología de estrella. Cada computadora se conecta a un cable que a su vez, se enchufa a un Hub que se le llama Unidad de Acceso a Multiestaciones (MAU).

Se pueden conectar las MAU de diferentes anillos de tal forma que los anillos que están separados aparezcan como una sola red.

Token Ring se basa en el paso de una señal o también conocido como Token Passing, es decir, que pasa un Token (señal) a las computadoras que integran la red. Se podría describir a un Token como una forma de obtener acceso a la red. De esta manera la computadora que está en posesión de un Token tiene permiso para transmitir su señal a otra computadora, si la otra computadora necesita enviar

[2] Ver en manual de Diplomado en Redes de Computadoras 2001, CRODE Celaya.

la información, acepta el Token y envía, en caso contrario el Token pasa a otra computadora y el proceso sigue.

El MAU realiza el proceso de saltar un nodo de la red que se encuentre apagado, pero dado que cada nodo que no esté funcionando bien puede hacer que deje de funcionar toda la red, Token Ring no es tan eficiente como CSMA/CD de Ethernet en redes que su actividad es muy poca, pues requiere de una sobrecarga adicional, pero conforme va aumentando la actividad en la red Token Ring puede llegar a ser más eficiente que CSMA/CD, ya que Token Ring evita las colisiones comunes del CSMA/CD y que por lo regular dan como resultado tener que volver a enviar la información (Fig. 2)[3].

Fig. 2 IBM High Speed 100/16/4 Token Ring PCI

1.7.2 ¿QUE ES ETHERNET?

Ethernet es una topología de red que basa su operación en el protocolo MAC CSMA/CD[4]. En la implementación de *"Ethernet CSMA/CD"*, una computadora con un paquete listo para enviar, retrasa la transmisión hasta que ésta verifique que el medio por el que se va a transmitir este libre y después de empezar a transmitir existe un tiempo muy pequeño en el cual puede ocurrir una colisión, es decir, en una colisión las computadoras dejan de transmitir la información y esperan un tiempo, vuelven a verificar el medio de transmisión para determinar si se encuentra desocupado.

---

[3] Para más información ver:
http://www.techdepot.com/product.asp?/productid=107934&affid=673

[4] CSMA/CD: Censor de Medio de Acceso Múltiple/con Detección de Colisión (Carrier Sense Multiple Access/Colision Detect).

1.8 PROTOCOLOS PARA LA COMUNICACIÓN

1.8.1 NetBEUI, IPX/SPX

El NetBEUI, tiene como función enlazar el software y hardware de la red en las computadoras.

El significado de NetBEUI es NetBIOS Extended User Interfase o Interfaz de Usuario Extendido para NetBIOS. Esta es la versión de Microsoft del NetBIOS (Network Basic input/output System, Sistema Básico de entrada/salida de red). Este protocolo es básico en la red de Windows para trabajo en grupo.

IPX/SPX

Es el conjunto de protocolos de bajo nivel, lo utiliza el sistema operativo de red Netware de NOVELL y el SPX se encarga de actuar sobre IPX para tener la seguridad de la entrega de los datos.

1.9 PROTOCOLO TCP/IP

1.9.1 ARQUITECTURA DEL PROTOCOLO

Oficialmente no existe un modelo del TCP/IP, sin embargo, es de gran utilidad caracterizar el conjunto de capas como si poseyera cinco, las capas son las siguientes:

- Capa de aplicación: Comunica a los procesos o aplicaciones entre computadoras distintas.
- Capa de transporte: Da un servicio para la transferencia de datos extremo a extremo. Esta capa puede incluir algunos aspectos de seguridad.
- Capa Internet: Esta capa esta relacionada con el encaminamiento de los datos de la computadora de origen a la destino a través de una o más redes conectadas a través de dispositivos que encaminen los datos.
- Capa física: Estipula las características del medio de transmisión, el sistema para la codificación de las señales y la tasa de señalización.

CAPITULO II

REDES INALÁMBRICAS

2.1 Definición de Red inalámbrica

2.2 Elementos utilizados en la transmisión

2.3 Métodos en la transmisión vía infrarroja

2.4 Datos y señales digitales

2.5 Codificación de señales Digitales y Analógicas

2.6 Generalidades de Redes de área local Ethernet Híbridas

2.7 Configuración básica de red inalámbrica (WLAN)

2.7.1 Punto a Punto (Peer to Peer)

2.8 Puntos de Acceso (Access Point)

2.9 Funcionamiento de los Puntos de Extensión

2.10 Categorías de las redes inalámbricas

2.10.1 Distancia de cobertura y desempeño

2.1 DEFINICIÓN DE RED INALÁMBRICA

Una WLAN o Wireless LAN, funciona con ondas electromagnéticas, radio e infrarrojo para hacer un enlace por medio de un adaptador a equipos conectados a la red en lugar de los cables coaxiales, UTP o fibra óptica que son implementados en las LAN convencionales con cableado. Las redes inalámbricas más que una sustitución de las redes convencionales, son una extensión de ellas porque permiten un intercambio de datos de forma limpia y transparente entre los usuarios; a fin de cuentas esa es la finalidad de las redes.

En las redes inalámbricas se utilizan medios no guiados, principalmente el aire (al decir medios no guiados, nos referimos a que no se utilizan cables como en las redes de cableado estructurado) se irradia energía que es transmitida por una antena transmisora y esta energía, a su vez, es recibida por otra antena. Se utilizan dos configuraciones para la emisión y recepción de esta energía, los cuales son: *direccional y omnidireccional.*

Direccional: Toda la energía se concentra en un haz, que es emitida en una dirección, por lo tanto el emisor y el receptor deben de estar alineados para recibir la energía de tal manera que no debe de haber pérdidas de energía, pero esta pérdida en ocasiones es inevitable cuando el clima no es de todo adecuado, las lluvias provocan perdidas de energía.

Omnidireccional: La transmisión es dispersada en varias direcciones, por lo tanto varias antenas pueden recibirla. En este método existe más perdida de energía por lo mismo de que no es canalizada a cierta dirección establecida. Cuanto mayor es la frecuencia de la señal a transmitir más factible es la transmisión *direccional.*

Por lo tanto, para los enlaces que son de punto a punto (peer to peer) se suele utilizar la transmisión por microondas (altas frecuencias). Para enlaces con varios receptores se utilizan las ondas de radio (bajas frecuencias).

Los infrarrojos se utilizan para transmisiones a muy corta distancia, como por ejemplo en una misma habitación (en alguna oficina).

2.2 ELEMENTOS UTILIZADOS EN LA TRANSMISIÓN

Suelen utilizarse diferentes métodos para la transmisión, uno de ellos es el transmitir por medio de ***microondas***. Básicamente se utilizan antenas parabólicas para conexiones a larga distancia de punto a punto. Se utilizan en sustitución del cable coaxial, cable UTP ó la fibra óptica, esto es porque se implementan menos repetidores y amplificadores aunque se necesitan antenas que estén alineadas, se utilizan en las transmisiones de televisión y voz.

La principal pérdida de la señal es la atenuación, esta atenuación aumenta cuando la distancia a la que debe de llegar la señal es muy larga y como se mencionó antes, la atenuación aumenta con los cambios climatológicos.

La interferencia es otro inconveniente de la transmisión por microondas ya que hay demasiados dispositivos que funcionan vía inalámbrica y puede haber un solapamiento de de señales, es decir, que se interrumpa la señal y se reciba la señal distorsionada. Un claro ejemplo, lo tenemos al sintonizar una estación de radio, hay veces que la señal de alguna estación se cruza con la otra y ni se recibe bien la señal de una ni de otra.

Otro método utilizado en la transmisión es por medio de ***microondas manejadas por satélite***. El satélite tiene la función de amplificar o retransmitir las diferentes señales que le llegan en una dirección adecuada, el satélite a su vez debe de mantener una alineación con los receptores y emisores que lo utilizan, es decir, el satélite debe de ser *geoestacionario*.

La palabra *geoestacionario* se refiere a que el satélite debe de acoplarse a los movimientos que hace la Tierra (rotación, traslación) así como a los diferentes

climas que se tienen en diversas partes del mundo para enviar las señales al lugar específico.

"El rango de frecuencias para la recepción del satélite debe ser diferente del rango al que este emite, para que no haya interferencias entre las señales que ascienden y las que descienden. Debido a que la señal tarda un pequeño intervalo de tiempo desde que sale del emisor en la Tierra hasta que es devuelta al receptor o receptores, ha de tenerse cuidado con el control de errores y de flujo de la señal".[5]

Por lo antes mencionado, el satélite transmite y recibe en rangos distintos, esto por obvias razones de seguridad en la información y evitar interferencias que hacen que la transmisión sea muy mala o casi nula.

Las diferencias entre las ondas de radio y las microondas son las siguientes:

Las microondas son unidireccionales y las ondas de radio omnidireccionales.

Las microondas son más sensibles a la atenuación producida por la lluvia.

En las ondas de radio, al poder reflejarse estas ondas en el mar u otros objetos, pueden aparecer múltiples señales "hermanas".

Transmisión por ***infrarrojos***. En este tipo de transmisión, los emisores y la parte receptora deben de estar alineados por la posible reflexión del rayo en superficies distintas como las paredes, el techo. En este método de transmisión no hay problemas de seguridad ni de posibles interferencias porque estos rayos no pueden atravesar paredes ni los objetos que se interpongan en el camino del rayo y tampoco se necesita de un permiso en especial para poder transmitir como es en el caso de la transmisión de ondas de radio y microondas, en estos métodos de transmisión si es necesario un permiso para asignar una frecuencia de uso.

[5] Ver http://www.geocities.com/elplanetamx/masderedes.htm

2.3 MÉTODOS EN LA TRANSMISIÓN VIA INFRARROJA

Los infrarrojos a su vez se pueden utilizar de diferentes maneras, como lo es la transmisión de *PUNTO A PUNTO*. En este modo, tanto el emisor como el receptor deben de estar los más cerca posible para tener una alineación correcta, es decir, requiere una línea de vista entre las estaciones para tener un buen enlace entre estos dos puntos (Fig. 3).

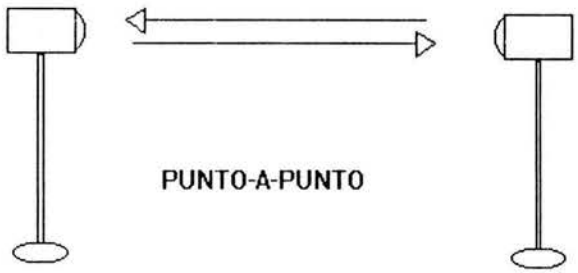


Fig. 3

Modelo *CUASI-DIFUSO*. Este modelo básicamente es de emisión radial, es decir que cuando una estación emite una señal óptica, esta señal puede ser captada por las demás estaciones al mismo tiempo. En este modelo no es necesario que las estaciones estén alineadas como en el modelo punto-a-punto, pero si deben de estarlo con la superficie de reflexión, esto para una mejor recepción en la señal emitida (Fig. 4).

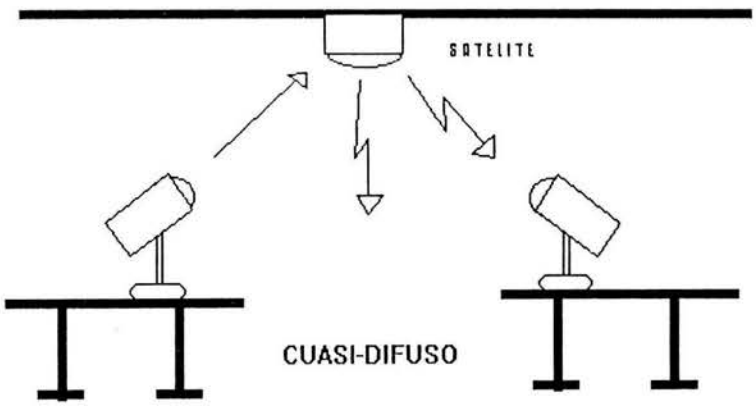
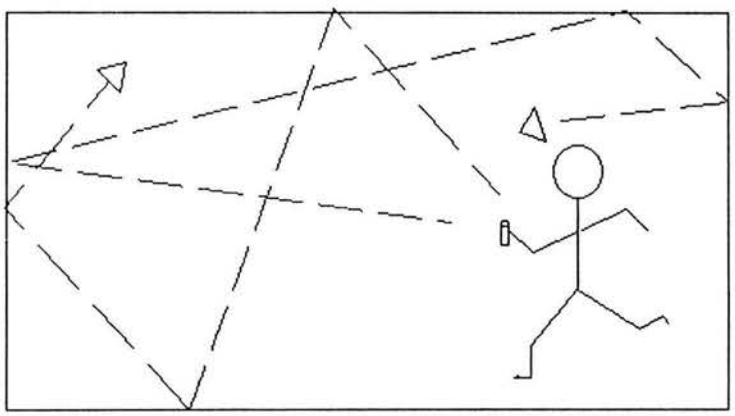


Fig. 4

Modelo *DIFUSO*. En este modelo la línea de vista no es necesaria, ya que la radiación del rayo utiliza diversos objetos que se encuentra en su camino como medio de reflexión. El poder de salida de la señal óptica debe de ser suficiente como para llenar el cuarto y así la estación puede estar orientada hacia cualquier lado.

El modelo **difuso** a comparación de los anteriores es más flexible debido al rango de alcance que este tiene y es mucho más sencillo de implementar como se ve en la figura, sin embargo esta flexibilidad esta a costa de excesiva emisión óptica (Fig. 5).



DIFUSO

Fig. 5

Como podemos ver en el esquema, el método difuso tiene una ventaja sobre los otros dos métodos anteriormente mencionados, la cual es que aprovecha mucho mejor la reflexión porque la señal rebota en los objetos que se encuentran en el cuarto, aparte de que no necesitan estar alineadas las estaciones de trabajo, es decir el ángulo receptor es mucho más amplio y capta con mayor facilidad la señal.

En cuanto a los métodos de *punto-a-punto* y *cuasi-difuso* cabe mencionar que la reflexión no es bien aprovechada o no se aprovecha porque las estaciones deben de estar alineadas con el emisor.

2.4 DATOS Y SEÑALES DIGITALES

Una señal digital es una serie de pulsos; para datos digitales lo único que se tiene que hacer es convertir cada pulso en bit de datos. En una señal *unipolar* se tiene que codificar un 0 como una tensión baja y un 1 como una tensión alta o al revés.

En una señal *bipolar* ya sea positiva o negativa, se codifica a un 1 como una tensión positiva y a un 0 como una tensión negativa o al revés.

La razón de datos en una señal es la velocidad de transmisión expresada en bits por segundo, a la que se transmiten los datos y la razón de modulación es la velocidad con la que cambia el nivel de la señal y depende del esquema de codificación elegido.

"Factores a tener en cuenta para utilizar un buen sistema de codificación:

1. Espectro de la señal: La ausencia de componentes de altas frecuencias disminuye el ancho de banda. La presencia de componente continua en la señal obliga a mantener una conexión física directa (propensa a algunas interferencias). Se debe concentrar la energía de la señal en el centro de la banda para que las interferencias sean las menores posibles.
2. Sincronización: para separar un bit de otro, se puede utilizar una señal separada de reloj (lo cuál es muy costoso y lento) o bien que la propia señal porte la sincronización, lo cuál implica un sistema de codificación adecuado.
3. Detección de errores: es necesaria la detección de errores ya en la capa física.
4. Inmunidad al ruido e interferencias: hay códigos más robustos al ruido que otros.
5. Coste y complejidad: el coste aumenta con el aumento de la razón de elementos de señal." [6]

---

[6] Ver http://www.geocities.com/elplanetamx/masderedes.htm

Por lo antes mencionado se concluye que en las señales digitales se debe de concentrar la señal en el centro de la banda, sincronizarse, detectar errores en lo que se refiere a instalación de emisores y receptores de señales digitales (capa 7 del modelo OSI)[7] y tener cierta inmunidad en cuanto a interferencias, todo esto para un mejor provecho y calidad de la señal.

2.5 CODIFICACIÓN DE SEÑALES DIGITALES Y ANALÓGICAS

En la codificación de datos digitales mediante señales analógicas es necesario convertir estos datos a formato analógico, para hacer esto existen varios métodos, los cuales se mencionan a continuación:

1. Desplazamiento de amplitud (ASK): Los valores binarios son representados por dos valores de amplitud de la señal portadora. Para ejemplificar lo mencionado lo representaremos con lo siguiente: s(t)=A * cos (2 * pi * f * t), la cual simboliza

   el 1 y s(t)=0, simboliza el 0 en este caso[8]. Este método es muy susceptible a cambios repentinos de la ganancia y es sumamente utilizado en la fibra óptica; el 1 significa la presencia de luz y el 0 representa la ausencia de luz.
2. Desplazamiento de frecuencia (FSK): En este método los dos valores binarios se representan por dos frecuencias próximas a la señal portadora. FSK es menos sensible a los errores que es método ASK. Se utiliza para transmisiones telefónicas a altas frecuencias y también se utiliza para LAN's con cable coaxial.
3. Desplazamiento de fase (PSK): La fase de la portadora se desplaza. En este caso un 0 se representa como una señal con la misma fase que la señal anterior y un 1 se representa como la señal con fase opuesta a la anterior enviada. Si se utilizan varios ángulos de fase, es decir, uno para cada señal, es posible codificar más bits.

---

[7] OSI: Interconexión de Sistemas Abiertos. Modelo de referencias de Interconexión de Sistemas Abiertos propuesto por la ISO, divide las tareas de la red en 7 capas.
[8] Ver ejemplo en http://www.geocities.com/elplanetamx/masderedes.htm

2.6 GENERALIDADES DE REDES DE ÁREA LOCAL ETHERNET HÍBRIDAS

2.6.1 LAN HÍBRIDA

Una *"LAN Híbrida"*, es la combinación de una LAN convencional con una WLAN o red inalámbrica, es decir, una LAN Híbrida contiene nodos conectados con cable UTP, fibra óptica o cable coaxial y a su vez cuenta con una extensión de computadoras que se conectan vía inalámbrica para formar una sola red. Esta topología nació con la finalidad de poder extender aún más los alcances de las redes convencionales cableadas y darles más funcionalidad.

Existen ciertas ventajas de las Redes de Área Local Inalámbricas o LAN's sobre las de cableado estructurado, las cuales son, la flexibilidad en el localizado de la estación, su instalación no requiere de mucho tiempo y la configuración no es muy compleja.

Las tecnologías utilizadas para las LAN's inalámbricas son dos; *Radio Frecuencia e Infrarrojas.* Estas dos tecnologías ya fueron explicadas en los capítulos anteriores pero se hará un análisis un poco más profundo para el entendimiento de lo que es en sí una *Red de Área Local Híbrida.*

2.7 CONFIGURACIÓN DE REDES INALÁMBRICAS (WLAN)

2.7.1 PUNTO A PUNTO (PEER TO PEER)

Por motivos de extensión se ha preferido describir y analizar el funcionamiento de una red inalámbrica (WLAN) bajo los estándares más usuales de funcionamiento.

Las redes inalámbricas y su especial fisonomía se pueden configurar de diferentes formas, buscando que cubran las necesidades básicas de los usuarios. La forma más básica de configuración se presenta al conectar dos computadoras que vienen equipadas con tarjetas o adaptadores (PC Cards) para redes inalámbricas (WLAN) y así de este modo tener una pequeña red inalámbrica, siempre teniendo en cuenta que estén dentro del rango que cubren.

Esta pequeña red se le conoce como "punto-a-punto" (peer to peer), mencionada anteriormente. La siguiente figura nos muestra esta simple configuración (Fig. 6)[9]:

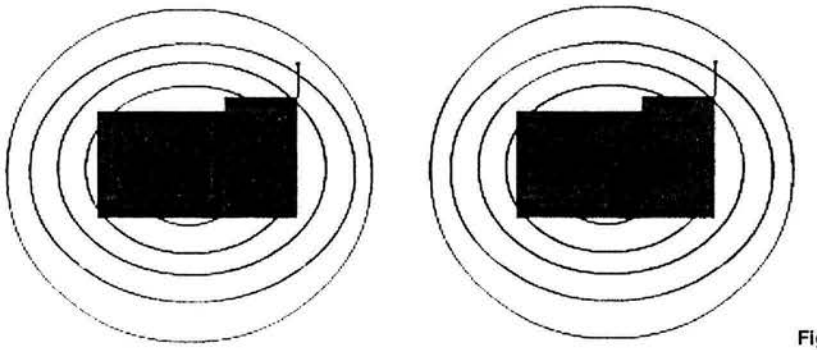


Fig. 6 Punto a Punto

En esta configuración, cada maquina tiene acceso a los recursos de la otra, pero no cuentan con un servidor central, es decir, todo el soporte recae en los usuarios ya que no requiere de una administración como en las redes en las que están involucradas mucho más número de maquinas que, a diferencia de la red punto-a-punto estas si requieren de una administración y un soporte riguroso del que se encarga el administrador de la red.

[9] Esquema hecho por el autor.

2.8 PUNTO DE ACCESO (ACCESS POINT)

En si lo que hace un *Punto de Acceso* es: Guardar y Repetir, es decir, valida y retransmite los mensajes que recibe. El *Punto de Acceso ó Access Point*, permite alcanzar un rango más grande en el cual los dispositivos pueden lograr una comunicación, ya que el *punto de acceso* (AP) tiene como función actuar como un "*repetidor*" y a través de este *punto de acceso* se puede colgar a la red cableada; así, la configuración punto-a-punto se puede mejorar. Cada AP sirve para varios clientes según el número de transmisiones que éste pueda generar (Fig. 7).[10]

Fig. 7 Intel PRO/Wireless 5000 LAN Access Point

El AP se debe colocar en la parte alta para garantizar una cobertura de radio amplia y así poder garantizar la conexión. El rango de los Puntos de Acceso (AP) es finito, va desde los 150 metros en lugares cerrados y llega hasta los 300 metros en lugares abiertos, como escuelas o industrias en donde es más factible que se lleguen a implementar varios AP con la finalidad de cubrir por completo la zona deseada y de este modo los usuarios puedan mover sus maquinas sin perder la conexión. A este peculiar modo de funcionamiento se le llama "*ROAMING*".

[10] Ver: http://www.intel.com/network/connectivity/products/5000_lan_access_point.htm

2.9 FUNCIONAMIENTO DE LOS PUNTOS DE EXTENSIÓN (EP)

Los puntos de extensión se pueden utilizar para aumentar el número de AP's (Puntos de Acceso). Esto es para incrementar el área a cubrir y resolver ciertos problemas en cuanto al alcance de transmisión, pero esto a su vez implica un costo más elevado.

Básicamente lo que hace un Punto de Extensión es expandir el alcance de la red mediante la retransmisión de las señales de una maquina a un Punto de Acceso, en otras palabras, otro tipo de repetidor. Otra forma de implementar los Puntos de Extensión (EP), es encadenándolos para que pasen mensajes entre los AP's y las maquinas que estén a una distancia lejana con la finalidad de hacer un tipo *puente* entre ellos. En teoría así funcionan, pero ya en la práctica es muy diferente porque el AP tiene la tarea de realizar un doble radio o cobertura doble. En el mercado no existe tal punto de acceso con estas características, aunque no tardara en salir con los avances logrados en este tipo de investigaciones. Otro de los componentes que se deben de tomar en cuenta y considerar su uso es el de "*Antenas*", ya que son de gran utilidad para enlazar lo que son edificios separados por una distancia de unos 1000 metros. Se puede instalar una antena en cada edificio haciendo que se vean mutuamente para lograr la conexión. Las antenas están conectadas a las redes cableadas mediante un AP que permite que exista la conexión sin necesidad del cable, la figura que se muestra a continuación muestra las antenas direccionales y como se deben de implementar (Fig. 8).[11]

[11] Esquema hecho por el autor.

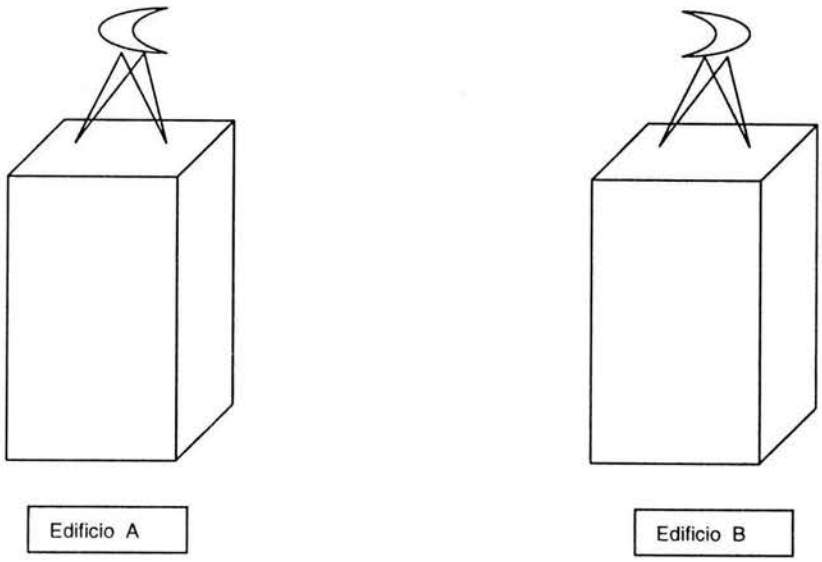


Fig. 8 Antenas direccionales

2.10 CATEGORÍAS DE REDES INALÁMBRICAS

Existen dos amplias categorías de redes inalámbricas (WLAN), las cuales son:

a) De larga distancia

b) De corta distancia

Las redes llamadas de *larga distancia*, se implementan para transmitir la información en espacios que pueden variar desde una ciudad o hasta varios países, mejor conocido como redes MAN, Metropolitan Area Network. Las velocidades a las que transmiten son relativamente bajas, oscilan desde los 4.8 Kbps hasta 19.2 Kbps.

Esto es una desventaja en cuanto a las transmisión de voz y video o para transmitir paquetes muy grandes ya que se tardaría demasiado tiempo en enviar y en recibir.

Las redes de *corta distancia*, se utilizan principalmente en redes corporativas en las cuales sus oficinas están ubicadas en uno o varios edificios que no están muy retirados entre sí, con velocidades de transmisión de 280 Kbps hasta 2 Mbps.

Dentro de las redes de larga distancia se derivan otros dos tipos, las cuales son:

a) Redes de Conmutación de Paquetes Públicas y Privadas
b) Redes Telefónicas Celulares

Estas últimas son un medio para transmitir información a un alto costo, debido a que los modems celulares son mas caros y delicados que los convencionales, ya que requieren de circuiteria especial. Estos circuitos especiales permiten mantener la pérdida de señal cuando el circuito se alterna entre una célula y otra, esta pérdida de señal no afecta en nada a la comunicación de voz porque, el retraso en la comunicación dura unos cuantos cientos de milisegundos, lo cual no se percibe. A diferencia de la comunicación de voz, en la transmisión de datos puede hacer estragos la pérdida de señal.

Este tipo de transmisión tiene sus desventajas, las transmisiones son muy lentas, la transmisión celular se intercepta fácilmente; factor que se debe de tomar en cuenta para la seguridad de la información.

Todas estas desventajas hacen que la comunicación celular se utilice poco, o solo para los archivos que son muy pequeños, como las cartas, planos, mensajes etc.

La otra opción existente en las redes de larga distancia, es la denominada *"Red Pública de Conmutación de Paquetes por Radio"*. Este tipo de red no tiene problemas de pérdida de señal, ya que están diseñadas para soportar paquetes de datos en lugar de comunicaciones de voz.

2.10.1 DISTANCIA DE COBERTURA Y DESEMPEÑO

La distancia que pueden cubrir tanto en las ondas de radiofrecuencia como infrarrojos, depende del diseño y el camino que siga la propagación, en especial en los lugares que están cerrados, porque cuando la señal se cruza con objetos como escritorios, paredes ó incluso las personas, esta es bloqueada; de manera que se debe de tener en mente este tipo de obstáculos en la transmisión.

En su mayoría los sistemas de redes inalámbricas se tiende a utilizar la radiofrecuencia, esto es porque tiene mayor grado de penetración y puede librar a la mayoría de los obstáculos que se encuentran en los lugares cerrados.

Como se menciono anteriormente, el rango de cobertura de una red inalámbrica (WLAN), va desde los 30 a los 250 metros, aunque la distancia de cobertura puede ser más amplia implementando los Puntos de Acceso (AP), permitiendo que los usuarios se desplacen de un lugar a otro sin perder la conexión. Esta funcionalidad ofrece una gran ventaja a los usuarios que poseen computadores portátiles o notebooks, para que se puedan mover libremente con su equipo evitando el cable que, muchas veces, suele ser muy estorboso. Ahora bien, en cuanto al desempeño se puede decir que depende de los productos implementados, así como el número de usuarios que soporta, de la propagación, y la estructuración del sistema inalámbrico utilizado.

Por otro lado, cuando se implementan *"Redes Híbridas"*, ocurre el problema de los llamados y bien conocidos *"Cuellos de botella"*. Este problema se da frecuentemente en la parte cableada de la red porque muchas veces el cable esta dañado o simplemente porque los equipos limitan el ancho de banda, es decir, algunos son muy viejos y no soportan altas velocidades; entonces esto genera los retrasos en la transmisión, pero gracias a las velocidades de transmisión alcanzadas por las nuevas tecnologías implementadas en los dispositivos para redes WLAN, los usuarios en Token Ring o Ethernet, generalmente, no experimentan ninguna diferencia en el desempeño respecto a otros usuarios enlazados a través de cable.

De esta manera podemos decir que, los problemas de *cuellos de botella*, puede solucionarse un poco con la tecnología inalámbrica.

Para tener un buen desempeño en la transmisión y recepción en las redes WLAN, se debe realizar un estudio previo del área en donde se van a colocar los AP's para ver si se tiene una buena propagación de señal, esto con el objetivo de *"llenar el área de cobertura con celdas que se traslapen (overlapping) de manera que los clientes puedan tener movilidad a lo largo del área."*[12]

Overlapping funciona de manera similar que el Roaming, es decir, que a medida que se desplace el cliente, su conexión es transferida a otro AP.

[12] Ver: http://www.proxim.com

En este capítulo se hablará específicamente de los diferentes dispositivos utilizados en las redes inalámbricas así como el estándar IEEE 802.11.

Se escogió hablar de la tecnología que nos maneja ORiNOCO porque presenta soluciones rentables para las diferentes arquitecturas de redes de tecnología inalámbrica que se puede emplear en las empresas, escuelas, en el hogar y oficinas pequeñas.

CAPITULO III

DISPOSITIVOS UTILIZADOS EN LAS REDES INALÁMBRICAS, WIRELESS LAN Y ESTANDAR IEEE 802.11

3.1 ESTÁNDAR IEEE 802.11

En concreto, el estándar IEEE 802.11, se encarga de estudiar la arquitectura e infraestructura de las WLAN o redes inalámbricas. La conclusión de este estándar fue en junio de 1997.

En este estándar se encuentran las especificaciones físicas y de nivel MAC (Control de Acceso al Medio, Medium Access Control) que se deben de tomar en cuenta en la implementación de una red de área local inalámbrica (WLAN).

La norma 802.11 ha tenido diferentes modificaciones con el fin de corregir y tener extensiones a manera de mejorar, así mismo se implementaron las siguientes especificaciones:

- 802.11 especificación para 1-2 Mbps en la banda de los 2.4 Ghz, usando salto de frecuencias (FHSS)[13] o secuencia directa (DSSS).[14]
- 802.11b, esta es una extensión de 802.11 para proporcionar 11 Mbps cuando se utiliza DSSS.
- Wi-Fi (Wireless Fidelity) estándar publicado por la WECA para certificar productos 802.11b capaces de interoperar con los productos hechos por distintos fabricantes.
- 802.11a es una extensión de 802.11 para proporcionar 54 Mbps usando OFDM.
- 802.11g extensión de 802.11 para proporcionar 20-54 Mbps usando DSSS y OFDM. Tiene compatibilidad con 802.11b y tiene mayor alcance y menor consumo de potencia que 802.11a.

[13] FHSS: Espectro Ensanchado por Salto de Frecuencia
[14] DSSS: Espectro Ensanchado por Secuencia Directa

Estas extensiones fueron publicadas con a finalidad de hacer que la tecnología inalámbrica sea más eficiente y hacer más entendible a los usuarios la finalidad de las WLAN.

3.1.2 ESTÁNDAR IEEE 802.11b

El estándar denominado IEEE 802.11b y la empresa de fabricación Wireless Ethernet Compatibility Alliance (WECA), han diseñado nuevos productos que rompen con el tope de velocidad, garantizan la compatibilidad con los fabricantes y sus precios son mas bajos. El hacer compatible los productos tradicionales de cableado con la tecnología inalámbrica, es una forma práctica de extender las redes cableadas.

Sin embargo las redes inalámbricas deben superar un pequeño problema técnico, el estándar 802.11b utiliza la banda de radio, la cual corresponde a los 2.4 Ghz., esta frecuencia es utilizada por millones de teléfonos celulares (inalámbricos), hornos de microondas y el apagado y encendido del alumbrado público.

3.1.3 ESPECTRO ENSANCHADO POR SALTO DE FRECUENCIA (FHSS)

La tecnología FHSS consiste en transmitir una parte de la información en una frecuencia determinada en un intervalo de tiempo a la cual se le llama *"dwell time"* y es inferior a los 400 ms. Cuando pasa este tiempo hay un cambio de frecuencia de emisión y sigue transmitiendo a otra frecuencia. Así, cada tramo de información es transmitido en frecuencias distintas con intervalos de tiempo que son muy cortos.

Cada transmisión utilizando una frecuencia concreta, se hace implementando una señal portadora de banda estrecha que cambia (salto) con el tiempo. Este procedimiento es el equivalente a realizar una partición de la información en el dominio del tiempo. El ordenamiento de los saltos de frecuencia que el emisor debe realizar, esta determinado por una secuencia pseudo aleatoria que esta definida en tablas, que deben de conocer el emisor y el receptor.

3.1.4 ESPECTRO ENSANCHADO POR SECUENCIA DIRECTA (DSSS)

Consiste en generar un patrón de bits, al cual se le llama *"señal de chip"*, para cada bit que compone la estructura de la señal de información, y la posterior modulación de la señal resultante por medio de una señal portadora de RF. Cuando se recibe, es necesario hacer lo inverso para obtener la señal original.

3.2 PUNTO DE ACCESO ORiNOCO BG-2000 BROADBAND GATEWAY

El ORiNOCO BG-2000, es un punto de acceso que proporciona conectividad inalámbrica a una LAN. Actuando como puente, el BG-2000 Access Point, cuenta con dos puertos Ethernet 10/100 Base-T y un radio Wi-Fi, en forma simultanea soporta estaciones alambricas e inalámbricas. Esto lo hace una buena opción en redes para hogares y oficinas pequeñas.

El BG-2000 Access Point es completamente compatible con las soluciones certificadas Wi-Fi, también debido a su sensibilidad superior del receptor y su resistencia a las interferencias ocasionadas por microondas, el BG-2000 de ORiNOCO ha demostrado buen desempeño en la industria basándose en el estándar IEEE 802.11b, ya que proporciona un funcionamiento inigualable y un amplio funcionamiento en cuanto a procesamiento se refiere.

ACCESO A INTERNET CON SEGURIDAD

El BG-2000 puede compartir una conexión de banda amplia de Internet (xDSL, cable o ISDN) con múltiples estaciones usando la conversión de dirección de red (NAT), el protocolo dinámico de la configuración del anfitrión (DHCP), el protocolo Ethernet punto-a-punto (PPPoE) y una red privada virtual. Adicionalmente cuenta con un *firewall* para control de acceso, encriptación WEP, que permite un acceso seguro en hogares. El *firewall* protege la entrada de los hackers a la red local. Los oficinistas pueden accesar a su red corporativa a través de VPN.

El BG-2000 es configurable con el estándar del navegador Web. Los administradores de la red pueden centralmente manejar el BG-2000 vía Telnet, basado en una línea de interfaz de comando. El BG-2000 es de fácil instalación, provee de un acceso seguro a Internet y las velocidades de transmisión son aceptables.

En la siguiente figura se muestra la forma de implementar el BG-2000, es una configuración sencilla y de fácil instalación (Fig. 9)[15] y también se muestra una imagen de este mismo (Fig. 10).[16]

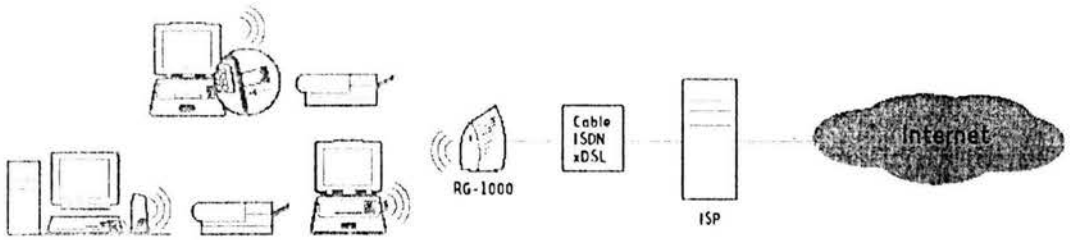


Fig. 9 Implementación del ORiNOCO BG-2000

Fig. 10 ORiNOCO BG-2000 Access Point

[15] Ver: http://www.orinocowireless.com
[16] Ver: http://www.orinocowireless.com

3.2.1 ESPECIFICACIONES DEL ACCESS POINT ORiNOCO BG-2000

A continuación se muestran las especificaciones del BG-2000 y el rendimiento que éste tiene:

- Alto rendimiento en transmisiones de 11 Mbps
- Radio de acción de ancho de cobertura de hasta 1750 y 550 m
- Herramientas de fácil entendimiento y resolución de problemas
- Certificado IEEE 802.11b (Wi-Fi)
- Seguridad de alto nivel con una clave de 128 bits RC4 encriptada y control de acceso
- Traducción del puerto de la dirección de red (NAPT)
- DHCP Cliente/Servidor (RFC2131, RFC2132)
- Opción externa de reajuste
- Estadística del funcionamiento: Ethernet
- Autoprueba del sistema y registro del acontecimiento
- Manejo de la seguridad: contraseña administrativa, contraseña del usuario, comunidad configurable SNMP, fijación del paquete IP
- Configuración del Internet Explorer (HTTP)
- Firewall (IP y filtrado de paquetes, filtrado de puerto estático)
- VPN
- TFTP

Como se puede observar, el Punto de Acceso BG-2000 de ORiNOCO es de fácil manejo e instalación, ofrece grandes ventajas sobre otras marcas y cuenta con una certificación que lo respalda y es considerado como uno de los mejores en el mercado.

3.3 ORiNOCO WORLD PC CARD

Este tipo de tarjeta (Fig. 11)[17] está diseñada para conectarse en cualquier red inalámbrica Ethernet y es compatible con cualquier equipo certificado Wi-Fi. Esta tarjeta trabaja en redes inalámbricas con altas velocidades que van desde los 11 Mbps, funcionando con 2.4 Ghz.

La tarjeta se implementa en laptos y dispositivos portátiles de computadoras. La tarjeta ORiNOCO ha demostrado ser la mejor por su alto desempeño y su fácil instalación, cuenta con la certificación IEEE 802.11b, es altamente resistente a las interferencias para proteger los datos y no consume mucha energía.

Especificaciones

- Sistemas operativos con los cuales es compatible: Novell Client 3.X y 4.X, Windows 95/98/2000/Me/XP y Windows NT; Apple Macintosh, Windows CE y LINUX.
- El voltaje que consume: 5VDC (+/- 0.2v)
- Rendimiento en condiciones normales de trabajo: 150.000 horas basadas en carga de trabajo de 2040 horas/año (operación continua).
- Garantizada por 3 años.
- Rango de temperatura que soporta: 0-55 °c y 95% de humedad.
- Guía de instalación en CD-ROM.

Fig. 11 ORINOCO WORLD PC CARD

[17] Ver: http://www.orinocowireless.com

3.4 ACCESS POINT ORiNOCO RG-1100

El RG-1100 actúa como un punto de acceso para proveer de una conexión vía inalámbrica y un acceso a Internet vía DSL, cable o IDSL. Diseñado para uno a diez usuarios, el RG-1100 es la solución ideal para las redes en hogares y oficinas que no necesitan de una red local muy grande. Al igual que el RB-2000, su resistencia a interferencias por microondas es muy alta y permite una multiconexión, es decir, varios usuarios pueden estar conectados al mismo tiempo gozando del mismo ancho de banda. Su configuración no requiere de mucho tiempo y es de fácil manejo, soporta velocidades de 11 Mbps y cuenta con los estándares especificados por la norma IEEE 802.11b.

ESPECIFICACIONES

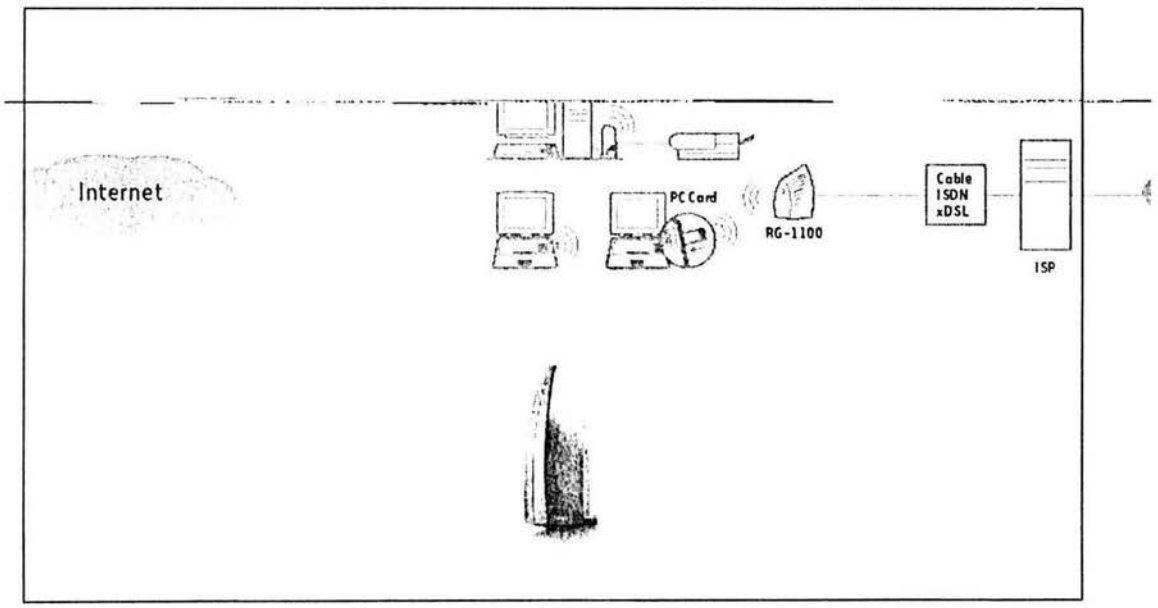
Las especificaciones del ORiNOCO RG-1100 son las siguientes:

- Tarifa de alto rendimiento 11 Mbps
- Certificación IEEE 802.11b (Wi-Fi)
- Radio de cobertura de 533.4/167.64 metros
- Seguridad de alto nivel usando un código encriptado de 128 bits
- Manejo con control remoto usando SNMP
- Ethernet 10 Base-T
- Socket RJ-45
- Canales de frecuencia de 2400 – 2483.5 Mhz.
- Compatibilidad con Windows 95/98/2000/Me y NT

Como se puede observar el RG-1100 no tiene requerimientos muy altos debido a que fue diseñado para redes caseras y oficinas muy pequeñas, pero tiene un alto rendimiento en condiciones de operación normales, además permite el libre desplazamiento de los usuarios cuando tienen que cambiar su computadora de lugar y con ello se evitan las pérdidas de tiempo, ya que en las redes

convencionales cableadas se tenía que desconectar el cable, desplazarse al lugar deseado, conectar el cable y esperar a que la computadora sea detectada por la red para lograr la conexión. De manera que con el RG-1100 se evitan todos estos problemas de tener que conectar y desconectar el cable y se goza de una mayor comodidad para los usuarios de la red.

En el siguiente cuadro se muestra la forma de cómo se puede implementar un RG-1100 en el hogar (Cuadro 1)[18] o en alguna oficina pequeña; asimismo se muestra la imagen de cómo es el ORiNOCO RG-1100 físicamente:



Cuadro 1: Instalación del ORiNOCO RG-1100

[18] Ver: http://www.proxim.com

3.5 TARJETA SKYLINE CARDBUS CARD 802.11a

Una tarjeta de *CardBus* , es una tarjeta de PC que utiliza una interfaz de 32 bits, esto significa que una tarjeta de *CardBus* puede transferir la información mucho más rápido que las tarjetas convencionales de 16 bits. La instalación de una *CardBus*, es sumamente sencilla, solo se tiene que introducir la tarjeta en una de las ranuras de la computadora e instalar el software. Se dice que las nuevas computadoras portátiles son compatibles con tarjetas *CardBus.*

Este tipo de tarjetas también esta diseñada para laptops, recibe y manda archivos grandes desde cualquier punto de la WLAN, las conexiones telefónicas no interfieren con la conexión ni los hornos de microondas, el video y audio es de alta calidad ya que la velocidad manejada es de 108 Mbps, una muy buena velocidad, pero una vez más nos enfrentamos al problema de que las altas velocidades son limitadas por los propios equipos, de manera que se tiene que implementar dispositivos de alta capacidad para poder exprimirlos al máximo y con ello gozar de los beneficios que ésta tecnología nos aporta.

Conectando este tipo de tarjeta a cada computadora móvil y varios Puntos de Acceso, se logra una pequeña red corporativa sin necesidad de estar conectada a través de un cable. Esta es una gran ventaja en cuanto a la velocidad lograda, porque muchos de los usuarios se quejaban por las bajas velocidades de transmisión de sus equipos, aunque con cable se logran velocidades de hasta 350 Mbps, 108 Mbps es una velocidad aceptable y a esto aunarle dispositivos de transmisiones altas, se puede lograr una red inalámbrica casi tan veloz como una red con cableado estructurado.

ESPECIFICACIONES

Requerimientos:

- Windows 98 (segunda edición), Windows Me/2000/XP
- Slot para tarjeta CardBus de 32 bits
- 64 MB de memoria RAM o más
- Procesador de 300 Mhz. o más

En la siguiente figura (Fig. 12)[19] se muestra una pequeña red inalámbrica que utiliza un punto de acceso y una tarjeta CardBus:

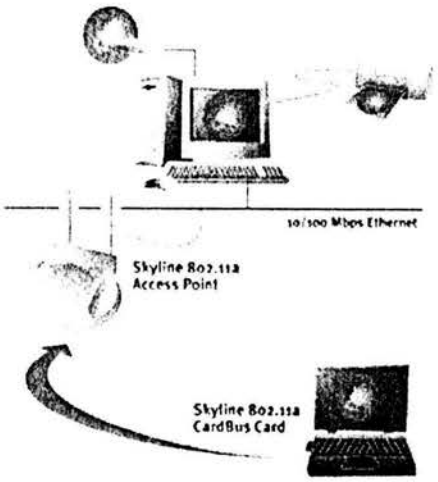


Fig. 12 Red Inalámbrica

3.6 RUTEADORES ORiNOCO OR-1100 y OR-1000

Este tipo de ruteador contiene un slot doble que sirve como punto de salida para las redes inalámbricas. El OR-1100, sirve como una base para la comunicación con varias salidas para ruteadores. La arquitectura del slot doble del OR-1100, permite que este opere como una salida central soportando la conexión satelital. El segundo slot, también puede ser utilizado como un punto de acceso local.

El ORiNOCO OR-1100 (Ruteador Central Externo) y el OR-1000 (Ruteador Remoto Externo), son radio inalámbricos que operan en la frecuencia de 2.4 GHz. El OR que esta situado centralmente se conecta a múltiples OR's en localidades remotas. Otra particularidad de este tipo de ruteadores es que además de funcionar como ruteadores, también pueden ser configurados como puentes para LAN's, hasta tres canales de radio pueden ser colocados en la base. Cada uno de estos OR's pueden soportar 48 OR's localizados remotamente. Estos son ideales para las empresas con conectividad LAN. El OR-1100 y OR-1000, son la solución

[19] Ver: http://www.proxim.com

para los ISP's, quienes quieran crear un sistema inalámbrico de Internet donde los ruteadores son los preferidos.

Estas unidades, ofrecen ruteo estándar IP, obteniendo la habilidad de conectar múltiples LAN con diferente IP. Un OR para conexión externa o Ruteador Cliente Externo (RCE) para conexión a un solo cliente, controles de ancho de banda que mantienen las velocidades para descargar archivos de Internet a una velocidad de 1 Mbps y para subir archivos al Internet con velocidad de 600 Kbps, que a su vez previene que un usuario use todo el ancho de banda sobre el espectro.

A continuación se muestran las especificaciones del OR-1100 y 1000:

- Soporta dos WLAN PC Cards
- Transmisión de datos de 11Mbps y 5.5Mbps
- El mecanismo sofisticado dinámico previene la colisión de datos
- 10/100 Base-T Ethernet Interfase, permite integración en esquemas de 10 y 100 Mbps Ethernet
- Alta seguridad usando encriptado de 64 y 128 bits
- Extiende la conexión hasta 3 millas utilizando un amplificador Incontinenti

ORiNOCO OR-1100 (Fig. 13):[20]

Fig. 13 OR-1100

[20] Ver: http://www.orinocowireless.com

3.7 KIT ORiNOCO PARA CONEXIÓN PUNTO A PUNTO

3.7.1 CONEXIÓN EDIFICIO A EDIFICIO

La conexión inalámbrica edificio a edificio (punto a punto), es un sistema pre-configurado que habilita a los usuarios para una fácil, rápida y económica instalación de un puente inalámbrico LAN, entre dos localidades, ya sea siendo un puente, un trailer o incluso en un bote. Esta tecnología avanzada ofrece todos los beneficios del estándar IEEE 802.11b con si inigualable desempeño. El kit para conexión de ORiNOCO incluye todo lo que se necesita para establecer la conexión punto a punto, ruteadores, cables, antenas, software y toda la documentación de los diferentes dispositivos que se implementan.

Una de las ventajas que ofrece esta tecnología, es la funcionalidad del protocolo maestro/esclavo (master/slave), ya que provee de una mas confiable conexión inalámbrica de edificio a edificio que otras tecnologías.

3.7.2 FUNCIONAMIENTO

A continuación se muestra el diagrama (Fig. 14)[21] de cómo es la conexión edificio a edificio:

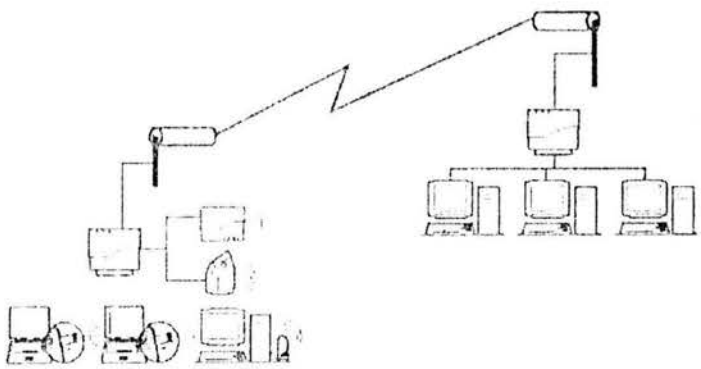


Fig. 14 Instalación de conexión edificio a edificio

[21] Ver: http://www.orinocowireless.com

En la figura anterior, el funcionamiento de la conexión edificio a edificio consta de la instalación (en este caso) de dos antenas direccionales, las cuales están conectadas mediante un AP (Punto de Acceso) para lograr la conexión inalámbrica, de ahí el AP distribuye la señal a las computadoras conectadas en red. Se puede observar que en la figura, el edifico de el lado derecho tiene una red cableada y la de el lado izquierdo es una red inalámbrica.

Para el caso de el edifico de la izquierda, la conexión llega vía inalámbrica desde el punto de acceso a las computadoras en donde se implementa el kit de ORiNOCO ya antes mencionado, cada una de las computadoras o nodos cuentan con la tarjeta para conexión inalámbrica y con ello poder recibir la señal. Esta señal llega a la antena direccional y baja hasta el ruteador, del ruteador la señal pasa por el AP y de ahí es transmitida a cada computadora. En el edifico de la derecha, la señal llega a la antena direccional y baja hacia lo que es el ruteador y a las computadoras de la red cableada. En este caso no se implementa un AP.

Este tipo de red *"Red Híbrida"* se puede implementar en empresas en donde los usuarios necesitan desplazarse de un lugar a otro dentro de un edificio, y requieran de una conexión continua (Fig. 15).[22]

Fig. 15 Kit ORiNOCO punto a punto o edificio a edificio

[22] Ver: http://www.orinocowireless.com

CAPITULO IV

LAN HÍBRIDA COAXIAL/INFRARROJOS, SEGURIDAD Y VPN'S

4.8.1 Compatibilidad de los diferentes dispositivos inalámbricos de la red

4.8.2 Factibilidad del uso de las WLAN

4.1 COMPONENTES QUE INTEGRAN UNA LAN HÍBRIDA COAXIAL/INFRARROJOS

La arquitectura de una LAN Híbrida puede variar dependiendo del lugar en donde se valla a implementar, es decir, se deben de checar los espacios físicos para ver si es factible la instalación de este tipo de red o no. La máxima compatibilidad que tienen las redes Ethernet con las redes inalámbricas es la llamada ***"segmentación"***. La segmentación consiste en dividir la red en *"células"*. Una célula es un grupo de computadoras que a su vez están interconectadas entre sí, dichas células conforman toda una red. Estas células están distribuidas ya sea dentro de un edificio o en varios edificios, podríamos decir que cada LAN existente en una ciudad se puede considerar como una célula. Cada célula representa una parte de la red, éstas células están unidas por cable o por un pequeño satélite (por así decirlo), el cual se encarga de distribuir la señal entre los nodos. Además, las células inalámbricas requieren de cables para interconectarse entre sí, ya que la radiación infrarroja no puede penetrar obstáculos opacados. De esta manera, la interconectividad entre nodos inalámbricos y cableados en un mismo segmento es posible y las células inalámbricas ubicadas en diferentes partes pueden comunicarse a través de un repetidor. En la siguiente figura se representa una LAN híbrida formada por células inalámbricas y cableadas:

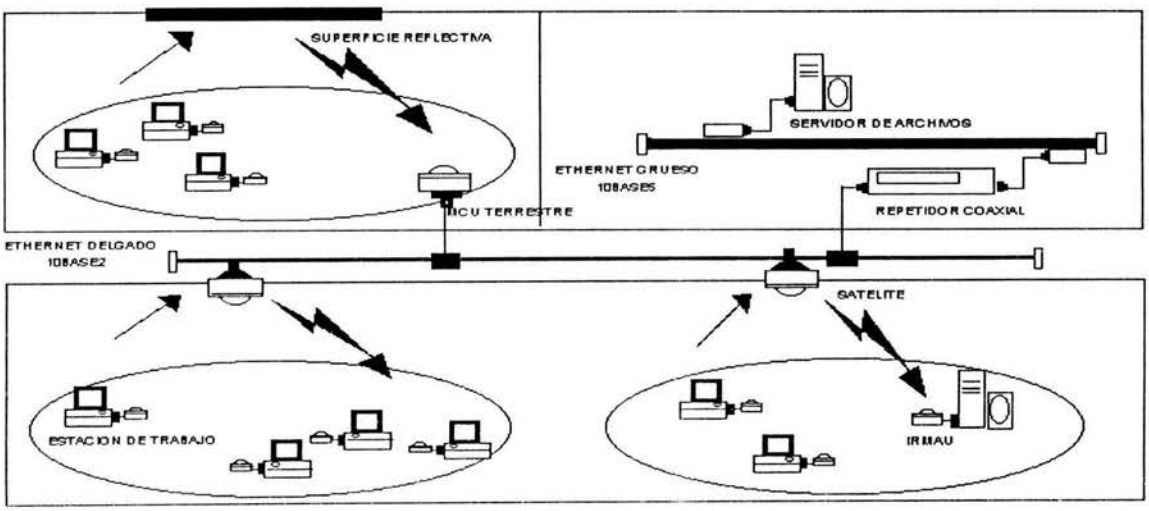


Fig. 16 LAN Híbrida

Como se puede observar en la figura anterior (Fig. 16),[23] la red está dividida en varias células interconectadas con un segmento de cable, el servidor se conecta a un repetidor y este mismo se encarga de distribuir la señal a través del cable que, al mismo tiempo se conecta con los repetidores. De esta manera tenemos una ***LAN Híbrida Ethernet***.

A diferencia de los componentes de una red Ethernet cableada, dos componentes son requeridos para soportar una LAN híbrida, los cuales son: un componente para adaptar la estación al medio óptico, la Unidad Adaptadora al Medio Infrarrojo (IRMAU), y otro componente para el puente de nivel físico, del coaxial al óptico, la Unidad Convertidora al Medio (MCU), que viene siendo un descendiente del repetidor Ethernet.

4.1.2 FORMA DE OPERACIÓN Y CARACTERÍSTICAS DEL IRMAU

La forma de operación del IRMAU es muy similar a la del MAU coaxial. El IRMAU debe de tener las siguientes características:

- Recepción de convertidor óptico a eléctrico
- Transmisión de convertidor eléctrico a óptico
- Detención y resolución de colisiones

"El IRMAU es compatible con las estaciones Ethernet en la Unidad de Acoplamiento de la Interfase (AUI). Esto permite utilizar tarjetas Ethernet ya existentes. Para las estaciones inalámbricas no es necesario permitir una longitud de cable de 50 metros, como en Ethernet, la longitud máxima del cable transreceptor debe de estar a pocos metros (3 como máximo), esto será suficiente para soportar las separaciones físicas entre estaciones e IRMAU, con la ventaja de reducir considerablemente los niveles de distorsión y propagación que son generados por el cable transreceptor.

[23] Ver: http://www.geocities.com/elplanetamx/masderedes.htm

Los IRMAU's basados en células de satélite ó reflexión pasiva difieren en el nivel de poder óptico de emisión y en la implementación del método de detección de colisiones.'[24]

4.1.3 UNIDAD CONVERTIDORA AL MEDIO (MCU)

La función de la MCU es similar al repetidor coaxial, sigue realizando las funciones de detección de colisión, regeneración, regulación y reformateo, pero con la variante de que algunos procesos han sido rediseñados.

La forma en que operan las células que están basadas en *reflexión activa* o de satélite surge cuando es recibido un paquete en la interfase coaxial, el satélite lo repite en la interfase óptica únicamente. De manera otra manera, cuando un paquete es recibido por la interfase óptica, el satélite lo repite en ambas interfases.

La *reflexión activa* utiliza un dispositivo de salida reflexivo (conocido como satélite), es decir, dicho satélite se encarga de amplificar la señal óptica para un mejor aprovechamiento de esta. De manera que cuando la interfase óptica está recibiendo un paquete y se detecta una colisión en cualquiera de las dos interfases, el satélite se encarga de reemplazar la señal que debería de transmitir por un patrón llamado CP (Colisión Presente). El satélite continúa enviando el CP hasta que no detecte actividad en la fase óptica. Por lo tanto, la interfase coaxial no realiza ninguna actividad, y sigue enviando la señal colisionada a la interfaz óptica. El satélite no realiza ninguna actividad cuando se detecta la colisión en la interfase coaxial mientras la célula no esté transmitiendo a los nodos. El satélite no bloquea la interfase coaxial, que a diferencia del repetidor éste sí la bloquea, la colisión puede ser detectada por los diferentes satélites que se encuentran colgados de un mismo segmento coaxial, de manera que una señal excesiva estará circulando por todo el cable.

[24] Ver: http://www.monografias.com

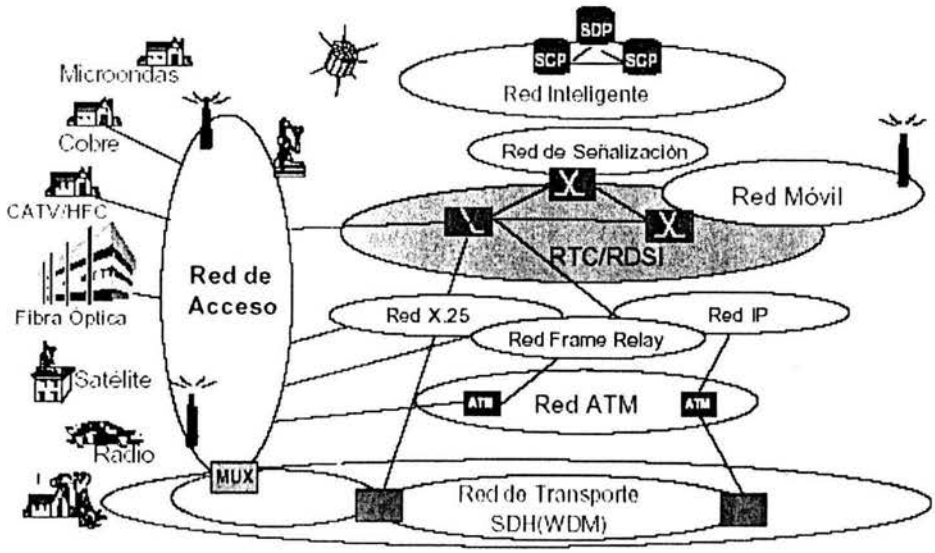


Fig. 17 Red completa de telecomunicaciones

En la figura se muestra la configuración de una ***"Red Híbrida"***; en este caso es una red de telecomunicaciones en la cual están enlazadas varias LAN, microondas, coaxial, fibra óptica, satelital, radiofrecuencia, móvil. El objetivo de este tipo de redes es ampliar un poco más una LAN pero implementando otros métodos y buscando cada vez más mayores velocidades de transmisión y recepción de datos.

4.2 CONFIGURACIÓN DE UNA RED HÍBRIDA COAXIAL/INFRARROJOS

Los componentes que están saliendo al mercado imponen mayores restricciones, sobretodo en la parte física de la red. Como se mencionó anteriormente, se tiene que fabricar componentes que no limiten al ancho de banda, ya que en muchas de las ocasiones podemos tener un ancho de banda muy grande; pero si el equipo no esta preparado para aprovecharlo al máximo, no sirve de nada, el propio equipo lo reducirá y se seguirá trabajando con lentitud.

La Ethernet híbrida debe de respetar que solamente se puede tener un máximo de cinco segmentos (tres coaxiales) y cuatro repetidores entre dos estaciones de trabajo. Ahora bien, el MCU tendrá la función de un repetidor coaxial al momento de definir la red, con funciones muy parecidas. La transformación de un paquete entre dos estaciones inalámbricas de diferentes células, es llevada a través de dos MCU.

La máxima extensión de una LAN híbrida es obtenida cuando uno de sus segmentos es totalmente híbrido.

En la siguiente figura (Fig. 18)[25] se muestra un segmento híbrido con dos enlaces punto a punto, un segmento no híbrido que a su vez están conectados por repetidores coaxiales:

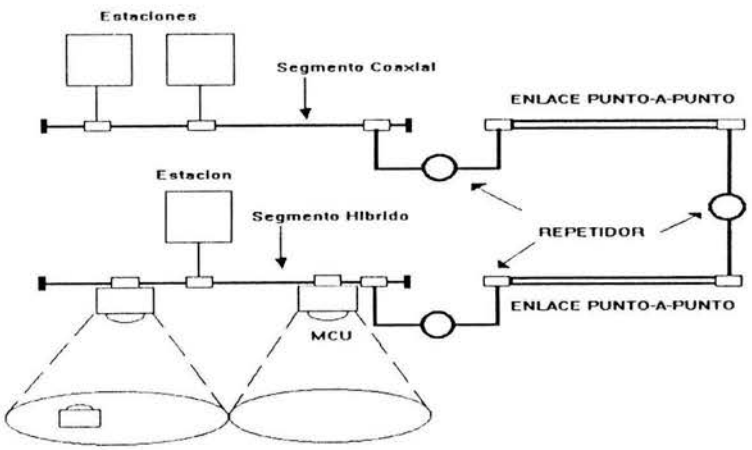


Fig. 18 LAN Ethernet Híbrida

[25] Ver: http://www.atenea.udistrital.edu.co/cursos/teleprocesos/redes/html/cap3/htm

Como se puede observar en la figura anterior, tenemos los segmentos coaxiales de los cuales están colgadas dos estaciones de trabajo; la señal pasa por el segmento coaxial y ésta a su vez llega a los repetidores que se encargan de distribuir la señal entre las estaciones de trabajo. En el segmento híbrido el MCU funciona como los repetidores coaxiales, recibe la señal, amplifica y retransmite la misma.

Esta es una configuración sencilla y de fácil entendimiento de lo que es una LAN Híbrida pero como ya hemos visto se pueden tener redes híbridas muy grandes como la mostrada anteriormente (Fig. 17).

4.3 RUTEO DE COMPUTADORAS INALÁMBRICAS BASADO EN TCP/IP

El protocolo TCP/IP es uno de los más mencionados en el estudio de las redes, es el protocolo manejado en Internet y, como ya se ha mencionado, es el encargado de la conexión entre redes y de que los datos sean confiables. Existen más protocolos utilizados en Internet como protocolos de transferencia de correo, protocolos de ruteo, protocolos encargados de la transferencia de archivos y muchos otros más, pero nos centraremos en el famoso protocolo TCP/IP y de cómo se rutean las computadoras móviles con dicho protocolo. En la siguiente figura se describe la estructura del protocolo de Internet, que a su vez estas capas son utilizadas por el protocolo Internet (Fig. 19).[26]

Fig.19 Capas del protocolo de Internet

[26] Ver: http://www.atenea.udistrital.edu.co/teleproceso/redes/html/cap3/htm

El protocolo IP, fue diseñado usando el modelo implícito de clientes de Internet o Internet Hosts, en el cual a cada computadora que integra la red se le asigna una dirección, de manera que anteriormente, no era permitido que computadoras inalámbricas o móviles se desplazaran entre redes IP diferentes sin que se perdiera la conexión, ahora cada computadora móvil se asigna a una nueva *red lógica*; la cual no esta relacionada con ninguna otra red existente. Este sistema opera con tres entidades diferentes las cuales son:

- Computadoras móviles o MC
- Ruteador móvil o MR (sirve como guía para red lógica)
- Estación base o BS

Básicamente, el funcionamiento de este modelo es, que las MC se conectarán a la Estación Base (BS) que está más cerca o la que le convenga, y la comunicación entre los sistemas existentes y computadoras inalámbricas sea hecha por un ruteador móvil (MR). En otras palabras, el MR y la BS controlan y a su vez mantienen la topología de la *red lógica*; de esta manera los clientes de otras redes existentes pueden comunicarse con la nueva red lógica de manera limpia, transparente y sin ningún problema. A continuación se muestra una figura en donde se muestran los componentes mencionados (Fig. 20).[27]

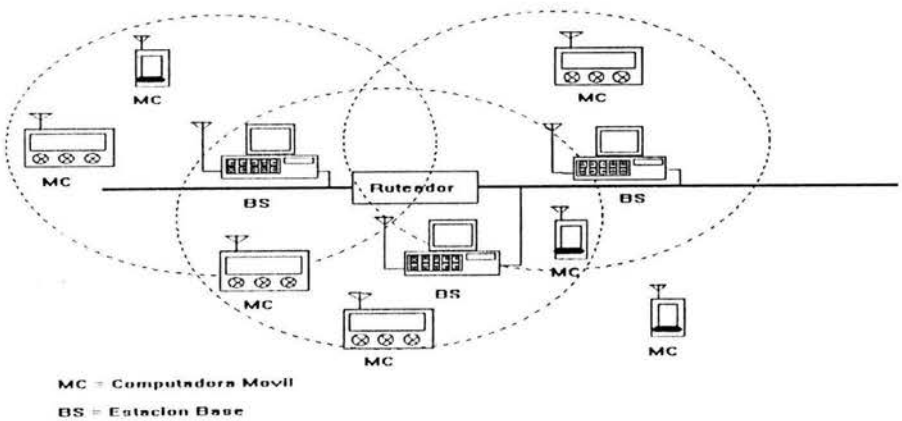


Fig. 20 Topología

[27] Ver: http://www.ataenea.udistrital.edu.co/cursos/teleproceso/redes/html/cap3.htm

Este método, permite a las Computadoras Móviles desplazarse en una red que es *lógicamente* distinta a otras.

Al decir *"lógicamente"* distintas, nos referimos a que una red está configurada de manera que las direcciones IP de una red cableada son diferentes respecto de las direcciones del grupo de las redes inalámbricas, de manera que cuando las Computadoras Móviles se desplazan por el grupo de la computadoras cableadas no pierden la conexión, ya que se les asigna direcciones IP diferentes y así son detectadas como una *"red lógicamente distinta"*.

4.4 ASPECTOS Y SERVICIOS DE SEGURIDAD EN LAS WLAN

El protocolo utilizado por el estándar wireless es el ***WEP*** (Wired Equivalent Privacy), como base de los diferentes mecanismos de seguridad implementados en las redes inalámbricas. ***WEP*** es el encargado de autenticar de las estaciones y también se encarga de el cifrado de las comunicaciones, utiliza para ello claves de seguridad de 40 bits convirtiéndolos en 64 bits al sumar un *vector de inicialización* de 24 bits.

Los mecanismos de seguridad ofrecidos por el estándar 802.11b se pueden clasificar de la siguiente manera:

- Autenticación
- Confidencialidad
- Control de acceso
- Integridad de los datos

Autenticación: La autenticación consiste en que, cuando se desea establecer la comunicación entre dispositivos, primero se debe de establecer una asociación entre ellos. Así, el cliente solicita la autenticación al AP, y este a su vez responde identificando el tipo de autentificación que está presente en la red, de manera que el cliente responde a la autenticación y si es satisfactoria, se procede a la asociación. El primer paso que se debe de seguir para la autenticación de un

cliente en una red inalámbrica es el conocimiento de SSID (Service Set Identifier), en otras palabras, se debe de conocer el SSID para poder accesar al sistema.

En el estándar 802.11b, se plantean dos posibles opciones para la autenticación de un cliente, las cuales son:

- Open system
- Shared key

Open system: Este es el mecanismo de autenticación por defecto, el cual permite que cualquier estación integre la red tras la negociación de los parámetros de red que se necesitan, de manera que se hace una autenticación *nula*, la cual permite que cualquier computadora o estación de trabajo, integre la red.

Shared key: Se realiza mediante un mecanismo denominado *desafió/respuesta* cifrado. Este mecanismo es necesario durante el proceso de que ambas estaciones posean una clave común ó autenticación simétrica. Una red 802.11b, puede utilizar este tipo de autenticación, solo si emplea el protocolo ***WEP***.

Confidencialidad: Para lograr una confidencialidad en una red inalámbrica, se debe de utilizar **WEP** como protocolo de cifrado.

Control de acceso: Si la autenticación *shared key* está activada, todos los paquetes existentes deben de estar perfectamente cifrados, en caso contrario se desechan, otra forma de control de acceso y autenticación, se logra apoyándose en lo que es el filtrado de trafico por las direcciones MAC controladas por el AP.

Integridad de los datos: El ***WEP*** utiliza un Código de Redundancia Cíclica muy simple (CRC32), para tener la seguridad e integridad de los datos, siendo insuficiente la utilidad y la eficiencia de este tipo de control, se deben de buscar nuevas opciones para mantener la integridad de los datos.

4.4.1 DESVENTAJAS DEL WEP

El protocolo WEP, no es lo mejor que se tiene para la seguridad de las WLAN, ya que contiene diversas vulnerabilidades desde el momento de su diseño, lo cual es una desventaja porque permite comprometer este tipo de redes y lo que se busca es una seguridad muy buena y que sea factible el implementar las redes inalámbricas.

El WEP cuenta con un algoritmo robusto y conocido (RC4), pero este a su vez cuenta con diversos defectos como la reutilización de claves que ya han sido usadas anteriormente. WEP no es la solución para la seguridad del cifrado de extremo a extremo, sino que sólo abarca el segmento inalámbrico de la red. WEP cuenta con una doble función, es decir, funciona como cifrador y autenticador que tampoco favorece porque al momento de una ruptura en alguna de sus dos funciones compromete tanto a uno como a la otra. La longitud de la clave que es de 64 bits, resulta ser muy corta, pero se tuvo que implementar de ese tamaño debido a las leyes de exportación de Estados Unidos en el momento de la creación del estándar, que fue en septiembre de 1999, de manera que ciertos fabricantes han tenido que ampliar la longitud de sus claves a 128 bits; en el estándar para las claves no se define ningún método para distribuir las claves, ni de autenticación para los puntos de acceso.

4.4.2 DESVENTAJAS DE LA IMPLEMENTACIÓN

A pesar de las desventajas propias al diseño del protocolo, muchas veces la puesta en práctica de los estándares nunca es ideal y siempre viene acompañada de defectos, incluso en los fabricantes con más prestigio. Hay muchas herramientas nuevas y de libre distribución que permiten sacar ventaja de las debilidades con mayor o menor éxito, y en caso de que no se hallan diseñado todavía, es muy factible que las desarrollemos nosotros mismos. Como el estándar no define ningún método para la distribución de claves para el proceso de autenticación, algún intento que se haga para el rotamiento de éstas lo hace un procedimiento que se convierte en tedioso, de tal manera que en la práctica las claves no son cambiadas con frecuencia, y debería de ser así.

La forma no controlada del cambio de las claves puede facilitar al intruso el acceso a la WLAN, porque sólo debe de conocer el SSID de la red, una dirección IP que sea válida, y en caso de que ésta esté habilitada la autenticación *shared key*, las claves de acceso WEP. Para conocerlas se deben de llevar a cabo acciones tan complejas como introducir el equipo en el radio que cubre un punto de acceso; para efectuar esto se puede apoyar en elementos de conectividad que son muy comunes como antenas direccionales que actúan extendiendo el alcance de la señal.

Una vez dentro de el radio de el punto de acceso, este retransmite el SSID varias veces por segundo por lo que es fácil su obtención. Algunos AP de determinados fabricantes deshabilitan esta función, pero existen otros métodos que son utilizados como la captura de la señal y posteriormente se analizan las tramas asociadas con la red. La obtención de una dirección IP es similar porque los AP están configurados para ofrecer el direccionamiento mediante lo que se le conoce como DHCP, y en los casos en que las direcciones IP de la red estén configuradas manualmente será valido introducir una dirección que sea admitida, siempre y cuando se capture un paquete proveniente de la red.

Los puntos de acceso siempre ofrecen una configuración de fábrica insegura en los que ya están predefinidos los parámetros SSID, canal, utilización del WEP. Existen

ciertos ataques a las WLAN, los cuales aprovechan las debilidades y son los siguientes:

- Ataque de escucha/monitorización pasiva (eavesdropping)
- Ataques de intercepción/inserción (man-in-the-middle)
- Ataques de denegación de servicio (jaming)

Ataques de escucha/monitorización pasiva: Las redes inalámbricas son vulnerables a lo que es la monitorización, lo único que se necesita es tener acceso al flujo de datos y estarlos monitoreando. Lo primero que se debe de hacer es tener asociación con el sistema que se quiere accesar; en redes basadas en *open system* este proceso es transparente, con ello se aumenta su complejidad en los sistemas que usan la autenticación *shared key*. Aquí la autenticación se logra tras capturar y crackear algunos paquetes, con herramientas que facilitan esta tarea; cuando se logra realizar todo esto se empieza a monitorear el tráfico presente en la red.

A la implementación de este tipo de ataque también se le conoce como *"wardriving"*, que evolucionó a *"drive-in-hacking"*, el cual consiste en localizar e identificar los diferentes puntos de acceso implementados, cualquier ubicación puede ser rastreada.

Ataques de intercepción/inserción (man- in- the- middle): Este tipo de ataque se basa en secuestrar la sesión mediante el uso de dos estaciones ajenas, ya que una estación que está transmitiendo no es capaz de detectar a otra computadora que tiene la misma dirección IP y es adyacente a esta misma.

El ataque inicia atacando a la estación que se encuentra conectada al AP mediante dos estaciones ajenas; la primer estación ajena adopta la misma dirección IP que la estación original; con ello, la segunda estación ajena empieza a mandar gran cantidad de datos que empiezan a saturar la conexión de la estación original, de manera que la primer estación ajena empieza a recibir los datos legítimos del AP que originalmente estaban siendo enviados a la estación original, y dado que la

estación ajena está recibiendo todos los datos provenientes del AP y la estación original está siendo saturada con tráfico en demasía, la primer estación ajena suplanta a la estación original.

"Algo más complicado son los ataques de suplantación de AP. Para ello y basándose en las diferencias de autenticación de AP del protocolo y de sus implementaciones, es posible colocar un AP más cercano al usuario con los mismos datos de configuración de red. En este caso los clientes se conectan al AP intruso permitiendo al elemento hostil la captura y redirección del tráfico de red de los usuarios legítimos, este ataque se le conoce como evil-twin, y aunque la incidencia es baja, actualmente se prevé su incremento en el futuro."[28]

Por lo antes mencionado se puede decir que la vulnerabilidad de las WLAN se ve reflejada en varios aspectos como protocolos, frecuencias de transmisión etc., pero principalmente en la configuración de los AP. Se debe de tener un tipo de encriptado en la información de mas de 128 bits para que puede ser mas difícil la codificación de estas señales y a su vez contar con un dispositivo de seguridad implantado en las computadoras que detecte cuando su IP o dirección MAC es duplicada, y al momento que la duplicación es detectada enviar una señal al AP y automáticamente deshabilitar esa dirección IP y desconectar la computadora original y la ajena o tal vez al detectar las conexiones intrusas en la red se les empiece a "bombardear", por así decirlo, con paquetes de información inservible hasta que se sature su conexión y con ello "botarlas" de la red con este tipo de saturación.

Ataques de denegación de servicio (jaming): Como ya se ha mencionado anteriormente, es fácil el ataque a dispositivos wireless, estos ataques pueden ir desde los mas sencillos utilizando dispositivos de radiofrecuencia (RF) de alta potencia con la finalidad de generar interferencias y hacer que el uso de la WLAN sea más difícil y a su vez prevenir al usuario para que no utilice el servicio durante las interferencias.

---

[28] Ver: http://www.sgi.es/prensa/articulos_interes/sic-52-art/javier_mejias.PDF

En la capa MAC 802.11b nos dice que no se transmitirá mientras se detecte otra actividad de radiofrecuencia.

4.5 ASPECTOS DE SEGURIDAD EN LA COMUNICACIÓN INALÁMBRICA

El estándar 802.11b establece diversas formas para tener entornos de redes inalámbricas más seguras; los mecanismos más utilizados son:

1. WEP (Wired Equivalent Protocol): Como ya hemos mencionado anteriormente, fue el primer mecanismo diseñado para la privacidad y para comprimir datos y que se envían a través de las ondas de radio.
2. WEP2: Esta es una modificación hecha para el WEP (2001); nació como consecuencia de una serie de vulnerabilidades encontradas, pero hoy en día no existe una buena implementación para el WEP2.
3. Open System Authentication: Definido por el estándar 802.11. Consiste en autenticar todas las peticiones que recibe. El principal problema que tiene es que no comprueba ni encripta.
4. ACL (Access Control List): Este es utilizado como un mecanismo de autenticación, la dirección IP o MAC de cada estación, siendo que si la dirección no está dentro de la lista de las permitidas, simplemente no se le da acceso.
5. Closed Network Access Control: El acceso a la red es permitido sólo a los que conozcan el nombre de la red o SSID, el cual viene a actuar como una contraseña válida para el acceso inmediato a la red.

4.5.1 SEGURIDAD INALÁMBRICA HARMONY

Hablando de seguridad la plataforma Harmony para WLAN, permite una administración centralizada para todos los parámetros de seguridad, incluyendo otras capacidades que se mencionarán a continuación:

- Distribución centralizada de claves WEP
- ACL's que soportan hasta 10,000 clientes
- Firewall con filtrado IP

La tecnología Harmony está configurada para permitirle al los encargados de administrar la red, desplegar redes 802.11b evitando la carga de tiempo utilizada por actualizaciones de seguridad de cada punto de acceso que integra la red.

Mediante la seguridad que ofrece Harmony los usuarios son limitados al acceso del servidor de archivos, de correo y para que puedan tener acceso al Internet; otros recursos que son más importantes y que sólo pueden ser accesados por el personal pertinente, no podrán ser accedidos por cualquier usuario (Fig.21).[29]

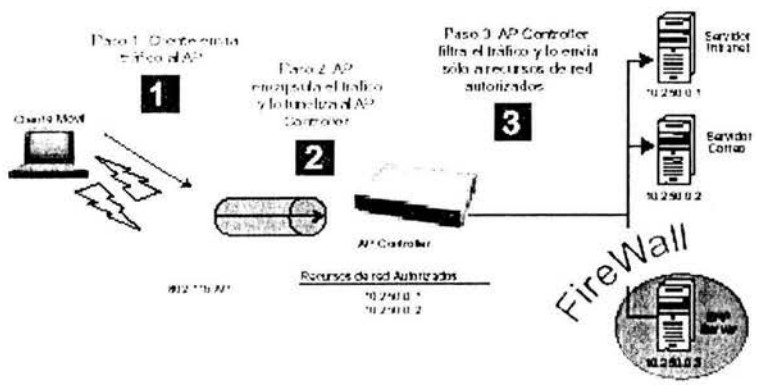


Fig. 21

[29] Ver: http://www.secont.com.ar

4.5.2 SEGURIDAD POR MEDIO DE TUNELIZACIÓN VPN HARMONY

Para las empresas que son muy grandes, lo que es la administración de las claves WEP y ACL's puede tornarse un tanto pesado para elaborarse, de manera que el uso de una Red Privada Virtual (VPN) para todo el tráfico wireless es una solución viable.

Básicamente, una VPN se implementa cuando la comunicación es insegura; las VPN's son implementadas en empresas que necesitan que sus oficinas remotas y sus agentes que se tienen que desplazar de un lugar a otro, se puedan conectar al Internet y a la red corporativa para que puedan accesar a cualquier servicio de la red. Una Red Privada Virtual tiene la capacidad de reforzar la seguridad mediante la autenticación de los clientes (mencionado anteriormente) que utilizan el sistema; con la autenticación de usuarios, lo que es el nombre del usuario y la contraseña son cifrados, la validez del lugar en el cual ingresaron y la dirección MAC son verificados. Donde se pueden utilizar métodos de cifrado más robustos como el RC5 y 3-DES se recomiendan para conservar la integridad de los datos.

"John Pescatore, un analista de Gartner Group, recomienda el uso de VPN's en un resumen, debido a los asuntos de seguridad del estándar actual IEEE 802.11b, uno de los beneficios de este método es que mantiene la interoperabilidad entre diferentes fabricantes de clientes inalámbricos 802.11b, gracias a que no se basa en implementaciones de seguridad propietarias. De hecho con el crecimiento de 802.11b en espacios públicos, una VPN permitirá a viajantes de negocios acceder a su e-mail o diferentes recursos de la red corporativa mientras viaja. Siguiendo esta sugerencia Harmony incorpora la habilidad de tunelizar todo el tráfico inalámbrico a un servidor VPN."[30]

[30] Ver: http://www.secont.com.ar

La tunelización permite utilizar una VPN es una red inalámbrica, de manera que, implementando la tunelización, se ahorra dinero y tiempo que con las soluciones con AP's ya conocidas. Así una red que basa su arquitectura en AP's tradicionales, implementará una VLAN ó tal vez funcionará en la misma subred para asegurar que todo el tráfico de las conexiones inalámbricas sea enviado al servidor VPN; con ello las grandes empresas que implementan este método se vuelve una carga, debido a que se utilizan sub-redes para la división de sus departamentos y como todo el tráfico es desviado al servidor VPN, éste se satura y se alenta la red.

Un grupo de científicos asociados con la universidad de California, descubrieron un error en el protocolo WEP 802.11b; el error consiste en que este protocolo habilita a las computadoras portátiles o notebooks, a que se puedan conectar a la red inalámbrica sin necesidad de que sean autentificadas. Este tipo de error permite que los hackers intercepten la transmisión para y desde una computadora portátil, de manera que pueden leer y modificar estos datos sin que sufran detección alguna. Gartner mencionó que las vulnerabilidades como el WEP se harían más frecuentes a medida que las compañías implementaran diferentes medidas para hacer la encriptación y la autenticación en los diferentes dispositivos inalámbricos que tienen un limitado procesador y compatibilidad de memoria.

Los complejos protocolos, el cifrado débil, las claves compartidas, la confusión del usuario, las restricciones del ancho de banda y los diferentes dispositivos, impulsan a los fabricantes a que tomen medidas más drásticas en cuanto a la arquitectura de los dispositivos móviles que van saliendo al mercado.

Pero como es bien sabido, las tecnologías que van emergiendo siempre son inseguras, hasta que las investigaciones hechas y los ataques de los hackers obligan a desarrollar tecnologías cada vez más seguras, ya que cualquier software contiene serios problemas de seguridad. Este tipo de situación no debe de espantar a la gente pero se deben de tomar serias precauciones.

Con la tecnología que nos maneja Harmony los AP's pueden ser instalados en cualquier parte del segmento Ethernet; así, todo el tráfico se tuneliza a lo que se le conoce como un *AP Controller* y de ahí al servidor VPN.

El *AP Controller* tuneliza todo el tráfico inalámbrico al servidor VPN, de manera que la configuración de una única sub-red para los AP's no es necesaria. Cuando se implementa este método los clientes comienzan a acceder a la WLAN dando su nombre al AP Controller de la siguiente manera (Fig. 22):[31]

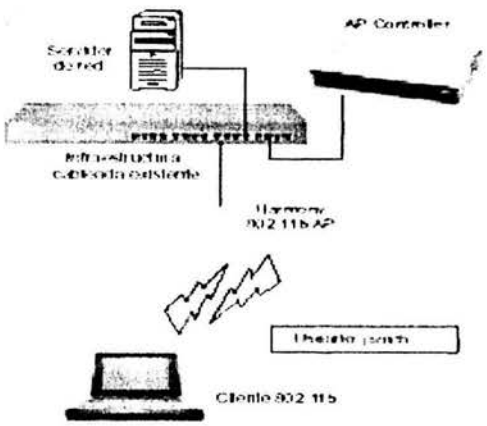


Fig. 22 AP Controller

En la figura anterior se muestra la manera en que el AP Controller recibe el nombre de usuario mostrado por el cliente que solicita el acceso a la red; dicho nombre de usuario es verificado en la base de datos de usuarios y contraseñas. Si el usuario está dado de alta en la base de datos se procede a realizar la conexión, de manera que si el usuario es autentificado el AP Controller genera una clave única de cifrado para ese usuario. Debido a que la contraseña del cliente es cifrada junto a la clave, no puede ser interceptada ni utilizada para que se utilice por cualquier otro usuario, por lo tanto, se protege de ataques de intercepción de claves.

[31] Ver: http://www.secont.com.ar

4.6 ¿POR QUÉ IMPLEMENTAR UNA VPN (RED PRIVADA VIRTUAL)?

Las Redes Privada Virtuales o VPN, surgieron de la necesidad de poder tener una privacidad en los diferentes departamentos de una empresa, de manera que se necesitaba un medio físico que pudiera lograr este tipo de comunicación PRIVADA. Hasta no hace mucho tiempo se implementaba el cable telefónico, de hecho, se sigue utilizando en algunos corporativos, pero la desventaja que se tenía era su alto costo, se tenía que pagar una tarifa por su uso y de esta manera su costo se incrementaba. La ventaja que este tiene es su disponibilidad y se garantiza la privacidad.

Además de la privacidad entre los diferentes departamentos de las empresas, surgió la necesidad de darle acceso a los usuarios móviles de la empresa, con ello la se vio en la necesidad de implementar un RAS (Remote Access Service), este tipo de usuario puede conectarse a la red de la empresa y usar los diferentes recursos de esta.

Una VPN es una herramienta para simular una red privada sobre una red de dominio público, como lo es el Internet.

"La idea es que la red pública sea Vista desde dentro de la red privada como un cable lógico que une las dos o mas redes que pertenecen a la red privada. Las Virtual Private Networks (VPN) son una alternativa a la conexión WAN mediante líneas telefónicas y al servicio RAS, bajando los costos de éstos y brindando los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones."[32]

[32] Ver: http://www.monografias.com/computacion/redes/

4.6.1 ESTRUCTURA VPN's

Básicamente las VPN's permiten el acceso a la red privada a los usuarios móviles; con ello pareciera como si los usuarios móviles estuvieran dentro de la red, que a su vez es conveniente para las personas que no tiene un lugar fijo de trabajo dentro de la empresa. Esto representa gran ventaja y comodidad para las personas que trabajan desde su casa o que tiene que salir por cuestiones de negocios (Fig. 23).[33]

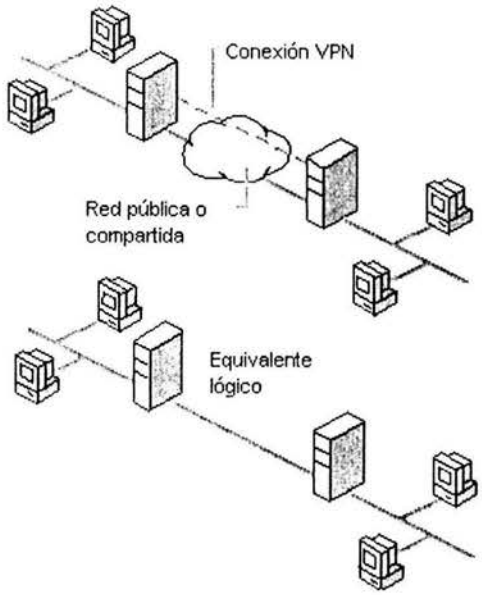


Fig. 23 VPN

Ahora bien, la forma en la cual se realiza la comunicación entre la red privada y la red pública, es estableciendo túneles de virtuales entre estos dos puntos para los cuales se manejan esquemas distintos para la transmisión de los datos usando la red de dominio público. Se utiliza diferente encriptación y a su vez la autenticación también es distinta para que se conserve la integridad de los datos enviados, ya que con el uso de la red pública (Internet) se debe de manejar un sistema de seguridad mucho más robusto por obvias razones de seguridad.

[33] Ver: http://www.monografias.com/computacion/redes/

Cuando se habla de *"tunelización"* se refiere al modo de transferir datos, en los cuales son encapsulados tipos de paquetes de datos dentro del paquete de datos de un protocolo cualquiera que no es necesariamente diferente al del paquete original. Cuando el paquete original llega a su destino, este es desempaquetado de manera que vuelva a su estado original, cuando los paquetes se envían por medio de Internet van encriptados.

Tanto la encriptación como la autenticación manejada en las VPN's es esencial, ya que se asegura a los diferentes usuarios que se encuentran intercambiando información. La autenticación dentro de las VPN's funciona de manera similar como cuando un usuario hace un Log-in en un sistema proporcionando su nombre de usuario y contraseña, pero la diferencia estriba en que las necesidades de aseguramiento son mayores. La mayoría de los sistemas que implementan VPN's utilizan sistemas de claves compartidas.

La manera en que es realizada la autenticación en las VPN's se lleva a cabo al inicio de sesión, y luego durante la misma para asegurar que no halla algún intruso. Todas las VPN, tienen un tipo de sistema de encriptación que básicamente empaqueta los datos formando un paquete netamente seguro, aunque algunas veces el tipo de encriptación es violado y visto el contenido de los paquetes por los famosos "hackers".

Hay dos tipos de encriptado que se usan en las VPN's, los cuales son:

- Encriptación de clave secreta
- Encriptación de clave pública

Encriptación de clave secreta: En este tipo de encriptación se implementa una clave "secreta" que conocen todos los usuarios que necesitan accesar a la información que esta encriptada, esta contraseña a su vez es utilizada para encriptar y desencriptar la información. Pero como toda clave que es conocida por varios usuarios tarde o temprano es distribuida a algunos otros usuarios, de manera que se debe de cambiar constantemente.

Encriptación de clave pública: Este tipo de encriptación se utilizan dos claves, la pública y la secreta, la clave pública es enviada a los usuarios; al momento que se desee encriptar datos se usa la clave secreta propia de cada usuario y también es utilizada la clave pública del otro usuario, así al recibir la información el otro usuario puede desencriptarla haciendo uso de su propia clave privada. Como cualquier buen método tiene sus desventajas, la desventaja de este tipo de encriptación es lo tardado que resulta hacerlo de esta manera.

4.6.2 PROTOCOLOS UTILIZADOS PARA LAS VPN's

Los protocolos utilizados son los siguientes:

PPTP (Point to Point Tuneling Protocol)

El funcionamiento de este protocolo provee a los usuarios de acceso remoto y a los servidores de red una Red Privada Virtual. A manera de protocolo de túnel, encapsula los datagramas de cualquier protocolo de red en protocolos IP, que son identificados como cualquier detagrama IP. Este encapsulamiento provee la ventaja de que cualquier protocolo puede ser ruteado a través de una red IP.

La estructura de PPTP permite a los usuarios conectarse a un servidor RAS (descrito anteriormente) desde cualquier punto de Internet y con ello pueden tener los mismos permisos de autenticación, encriptación y los accesos a la red.

IPSec

El surgimiento de IPSec fue para remediar algunas deficiencias de IP, como lo es la protección de los datos transferido y ofrece la garantía de que el que está enviando el paquete sea el que dice el paquete IP.

IPSec brinda confidencialidad, autenticidad y protección a repeticiones apoyándose en dos protocolos extras, Encapsulated Security Payload (ESP) y también Authentication Protocol (AH).

¿Pero qué es AH?; AH es un protocolo que provee de confidencialidad, autenticación, la diferencia más grande entre ESP y AH, es que AH se encarga de proteger las partes de encabezado IP así como las direcciones de origen y destino, es decir, el encabezado es como una etiqueta ó identificador que tiene cada paquete que es enviado, entonces AH protege ese identificador para que el paquete llegue a su destino, de manera que si ese "identificador" es corrompido o cambiado se perderá el paquete automáticamente, ya que necesita de ese identificador para que la máquina que lo solicitó lo identifique y lo jale, si no, estará viajando sin rumbo hasta desintegrarse, porque estos paquetes tienen tiempo de vida.

ESP también provee autenticación, integridad, confidencialidad y protección a repeticiones, protege el paquete entero que sigue al encabezado. El encabezado de ESP, permite que la carga sea rescrita en forma encriptada, como no considera el encabezado IP, éste no garantiza nada sobre el mismo, solamente lo que es la carga.

L2TP (Layer 2 Tuneling Protocol)

Protocolo que facilita los túneles de paquetes PPP a través de una red de tal manera que sea lo más transparente que se pueda para los usuarios de los dos extremos del túnel y para las diferentes aplicaciones que ejecuten.

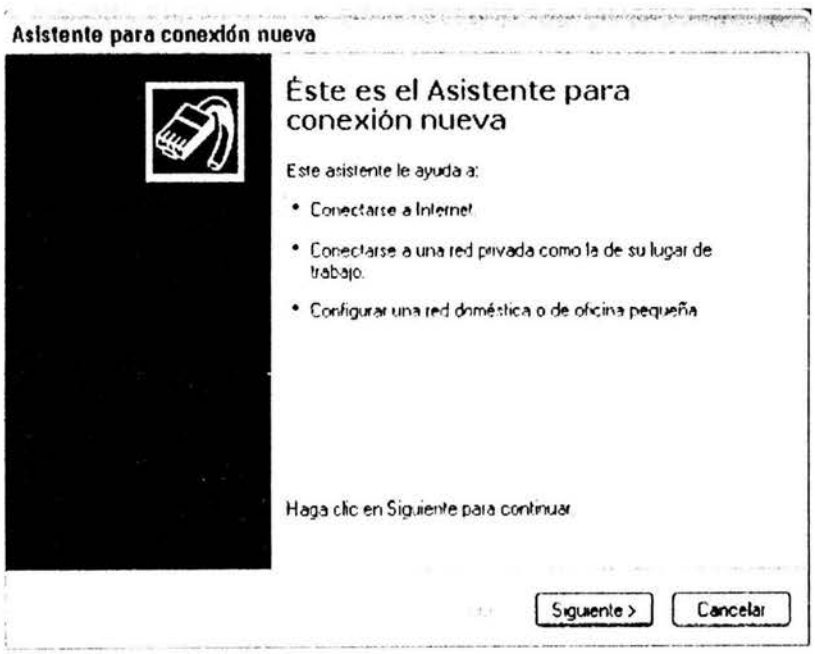
L2PT tiene la finalidad de crear túneles para marcos PPP entre el sistema remoto o cliente LAC y un LNS localizado en la red de área local. Un LAC (L2PT Access Concentrator) es una computadora o nodo que actúa como un extremo de un túnel L2TP y es par de un LNS. El LAC esta situado en medio de un LNS y un sistema remoto y este a su vez manda paquetes entre ambos. L2TP utiliza dos tipos de mensaje; el de control y el de datos. Los mensajes de control son utilizados para el mantenimiento, borrado de los túneles y llamadas; los mensajes de datos se encargan de encapsular los marcos PPP y a su vez son mandados a través del túnel.

4.7 CONFIGURACIÓN DE UNA VPN CON WINDOWS XP

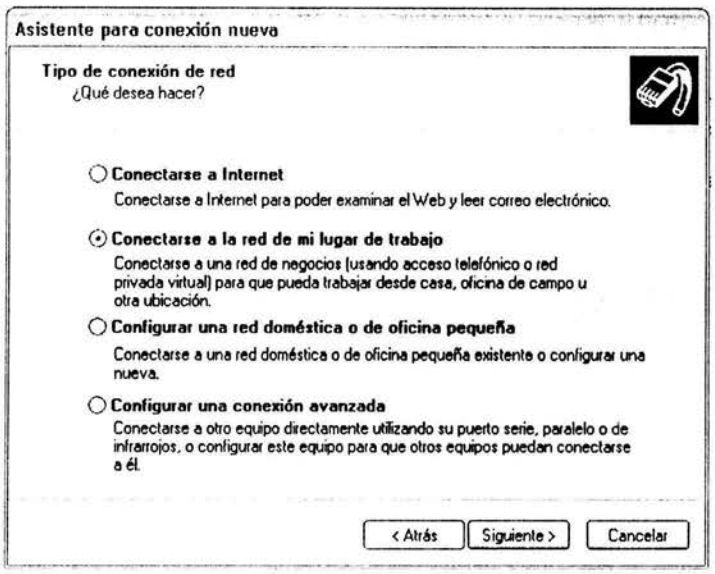
Para configurar una VPN bajo Windows XP se tienen que seguir los siguientes pasos:

Primero se debe de verificar que funcione perfectamente la conexión a Internet, después se podrá configurar la conexión de acceso remoto por VPN:

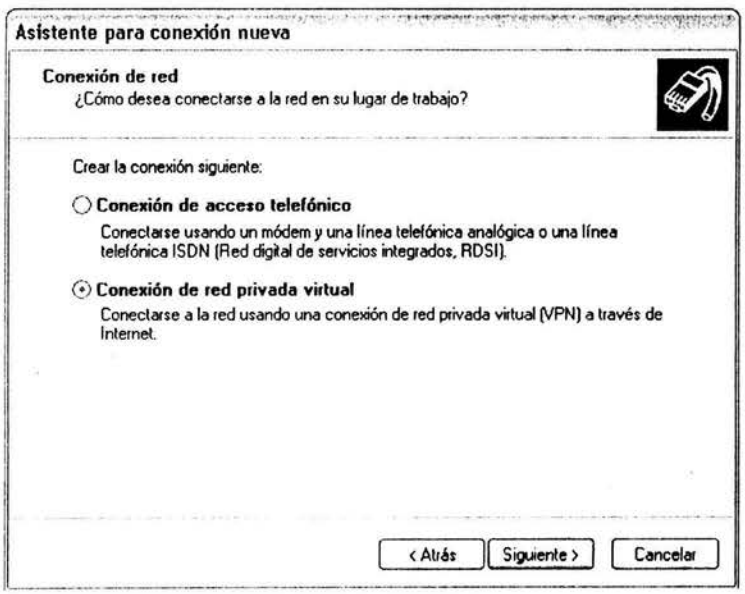
1) Para empezar se debe de accesar a Inicio → Programas → Accesorios → Comunicaciones → Asistente para conexión nueva → Siguiente



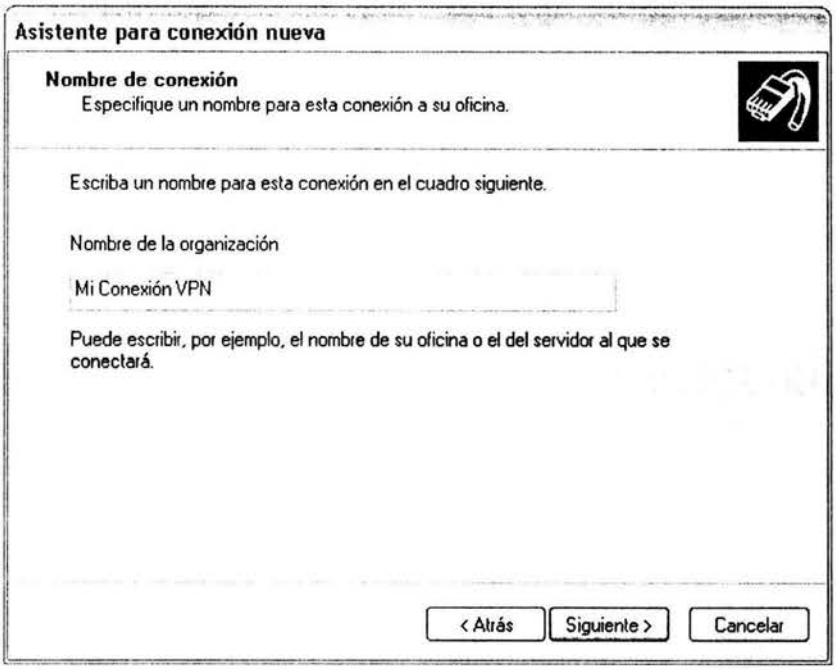
2) Se prosigue a seleccionar *"Conectarse a la red de mi lugar de trabajo"* → Siguiente



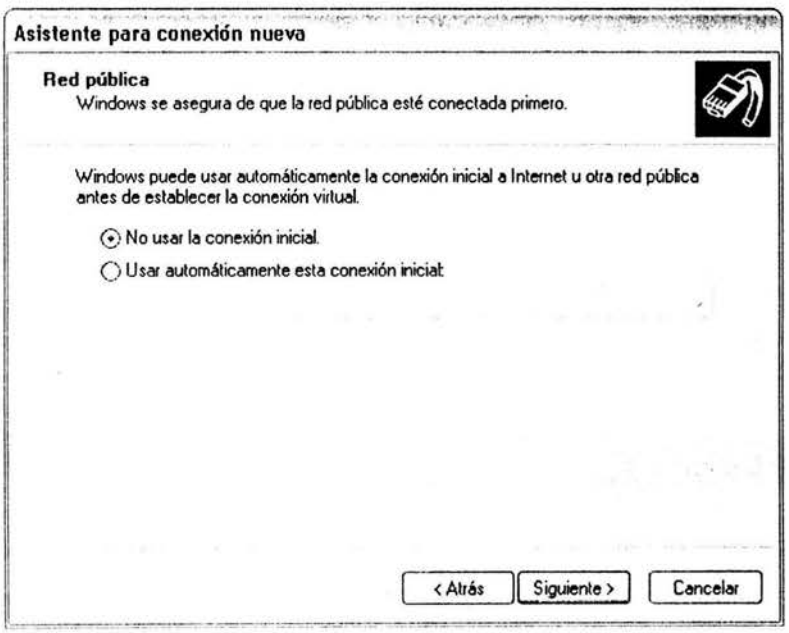
3) Se selecciona *"Conexión de Red Privada Virtual"* → Siguiente



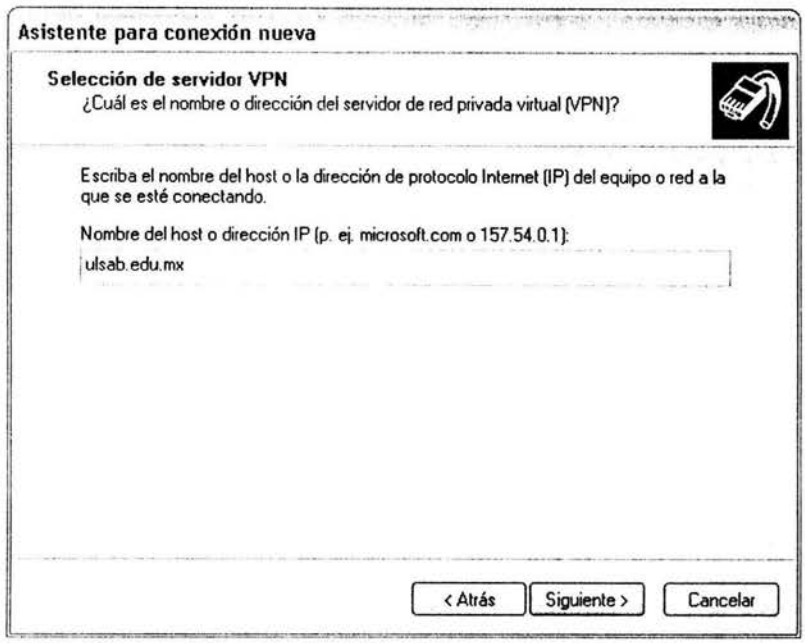
4) Escribir el nombre de la organización, por ejemplo Mi Conexión VPN → Siguiente



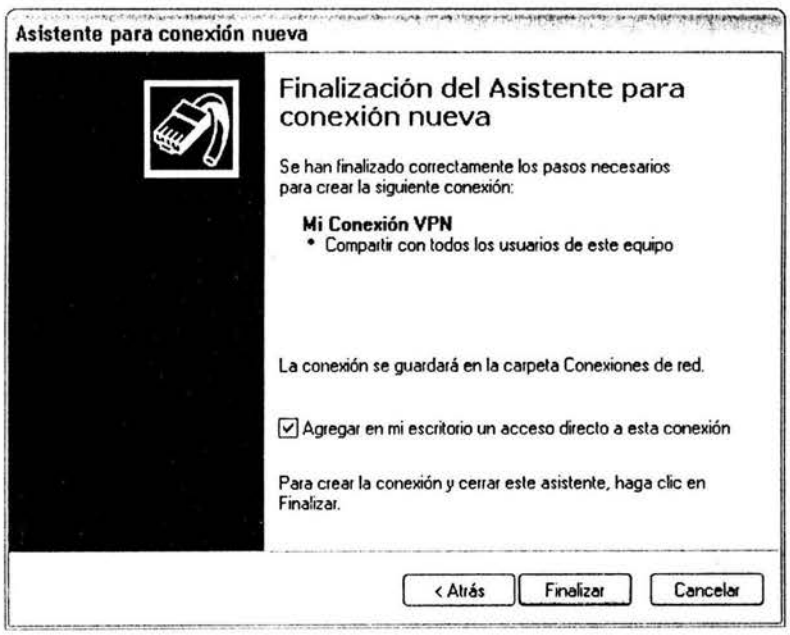
5) La opción de *"No usar conexión inicial"* debe de estar seleccionada → Siguiente



6) Nombre del host, por ejemplo ***ulsab.edu.mx*** → Siguiente

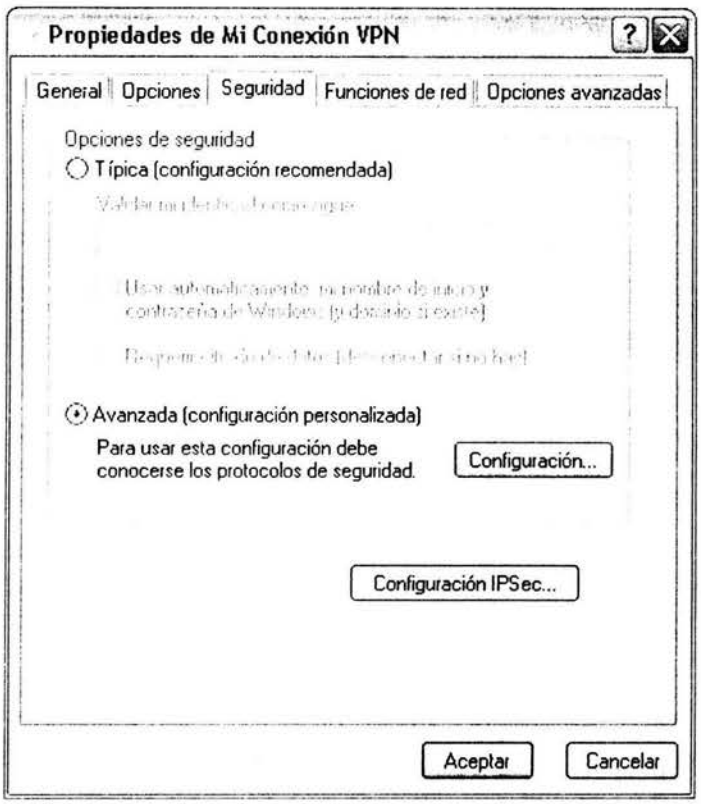


7) Clic en finalizar y si se quiere un acceso directo se selecciona la opción marcada

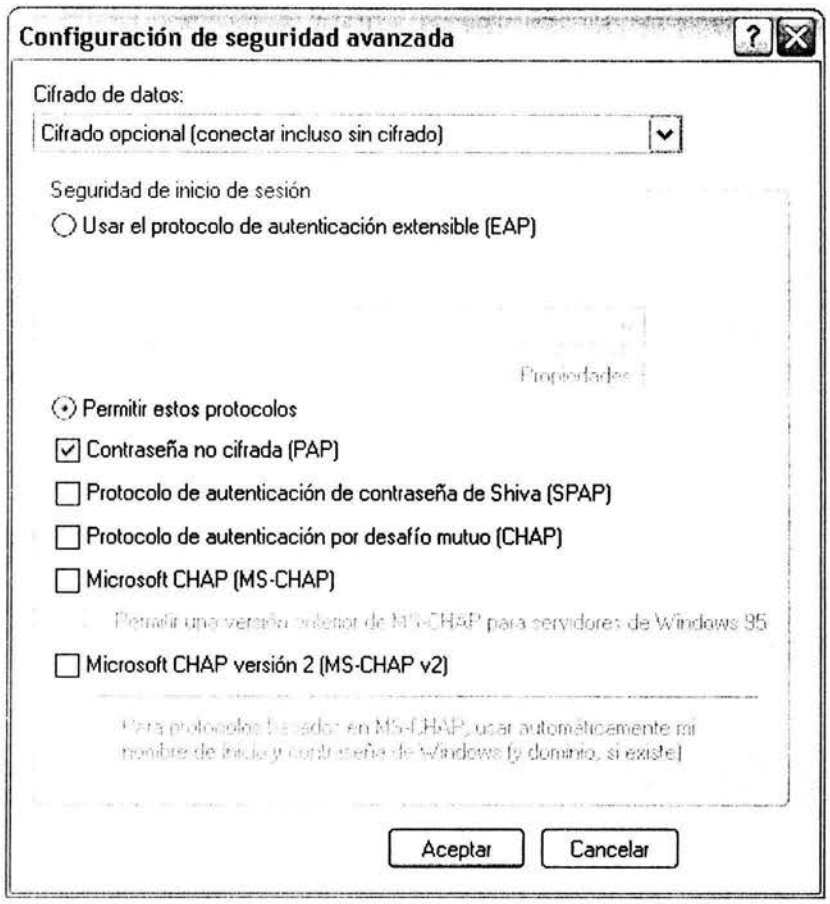


8) A continuación se procede a configurar nuestra VPN. Inicio → Programas → Accesorios → Comunicaciones → Conexiones de red, después clic con el botón derecho sobre el icono de Mi Conexión VPN → Propiedades y clic en la cejita de

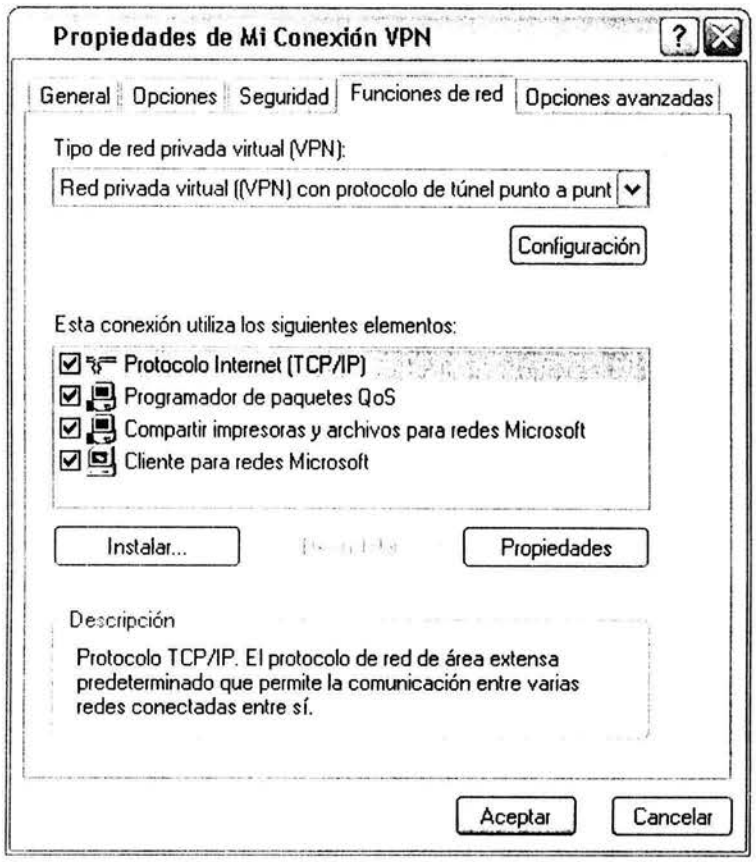
Seguridad, seleccionar *"Avanzada (configuración personalizada)"* y clic en **Configuración**



9) En cifrado de datos, seleccionar *"Cifrado opcional (conectar incluso sin cifrado)"*, después habilitar la opción *"Permitir estos protocolos"*, **OJO: QUE QUEDE SOLO SELECCIONADA "CONTRASEÑA NO CRIFRADA (PAP)", Y CONTESTAR "SI" A LA PREGUNTA QUE APARECE AL MOMENTO DE DAR CLIC EN "ACEPTAR"**



10) En la cejita *"Funciones de red"*, en tipo de de red privada virtual (VPN) seleccionar Red Privada Virtual (VPN) con protocolo de túnel punto a punto (PPTP) → Aceptar



Como podemos observar, la configuración de una VPN bajo Windows XP no es muy compleja como se pensaba, sólo se debe prestar atención en la configuración y los protocolos que se van a utilizar, sobre todo en la seguridad es en donde se debe prestar especial atención ya que al momento de compartir la información con los demás usuario de la VPN se corre el riesgo de que llegue a personas equivocadas, pero de ahí en fuera no tiene ningún problema mayor.

Se escogió hablar de la configuración de una VPN bajo Windows XP, porque es la versión nueva de Windows que viene en las computadoras que adquieren los usuarios; además se puede configurar bajo Windows 98, Windows ME Edition, Windows 2000 y Windows NT, de manera que se espera que esta información sirva a las personas que la lean.[34]

[34] Todas las imágenes de configuración VPN bajo Windows XP fueron hechas por el autor.

4.8 CONSIDERACIONES BÁSICAS EN EL DISEÑO DE WLAN

Antes de empezar a instalar la red, se deben de revisar algunos aspectos de diseño y medidas de seguridad para la protección de la red, ya que es importante para evitar posteriores ataques que puedan ocurrir.

En el diseño de las WLAN se pueden tomar en cuenta las siguientes medidas básicas para un mejor aprovechamiento de estas:

- Redes Privadas Virtuales (VPN) a nivel de firewall para el encriptado de los datos de la WLAN.
- Los puntos de acceso no deben de estar conectados directamente con la red, de manera que se debe de implementar un firewall entre la conexión y el punto de acceso así como un mecanismo de autenticación y un encriptado más estricto.
- No se deben de colocar los puntos de acceso atrás del firewall
- Los usuarios de la WLAN, deben de acceder a ella utilizando dispositivos de seguridad tales como Secure Shell (SSH), VPN, IPsec etc.

El diseño de las redes inalámbricas varía dependiendo las necesidades que se tengan, de manera que algunas medidas de seguridad pueden variar.

Las WLAN tienen dos componentes principales, los cuales son las estaciones de trabajo y los puntos de acceso, de manera que cuando se instala una red inalámbrica se debe de tomar en cuenta el área en la cual se va a instalar la red, se debe de revisar las frecuencias utilizadas para la transmisión para evitar posibles interferencias, así como revisar el lugar en donde se van a instalar las antenas direccionales.

Muchas veces los cambios climatológicos influyen mucho en las transmisiones, cuando se presentan lluvias muy fuertes o cuando el aire tiene mucha fuerza, se puede perder una parte de la información o tal vez se pierda completa, así como también se pueden llegar a dañar los componentes, entonces se deben de considerar ciertos puntos para evitar fallos en la red.

Cuando se van a adquirir los componentes para la instalación de una red inalámbrica se deben de tomar en cuenta varios aspectos técnicos como los siguientes:

- Cobertura
- Rendimiento
- Integridad y fiabilidad
- Compatibilidad

Cobertura: Las distancias que puedan cubrir las señales infrarrojas o de radiofrecuencia van en función del diseño del protocolo y de la ruta de propagación que debe de seguir la señal, especialmente para los lugares cerrados.

Como ya se había mencionado anteriormente, la propagación de la señal puede ser interrumpida por diferentes objetos que se encuentren a su paso, como paredes, escritorios, personas etc., entonces la cobertura disminuye con este tipo de percances que muchas veces por no tomar en cuenta este tipo de obstáculos se tienen muchos problemas a la larga. De manera que la mayor parte de los sistemas utiliza lo que es *radiofrecuencia* (RF) debido que pueden penetrar la mayor parte de obstáculos y es una buena opción para lugares cerrados. La cobertura de una WLAN oscila de los 30 a los 100 metros pero; como, ya es sabido, se puede extender con los puntos de acceso.

Rendimiento: El rendimiento en las redes inalámbricas va muy ligado a la colocación de los dispositivos, así como de l número de usuarios que se tengan, de los factores de propagación; a su vez también depende de los cuellos de botella que existan en la parte cableada de la red.

Integridad y fiabilidad: Las interferencias pueden llegar a degradar el funcionamiento de los dispositivos inalámbricos provocando graves fallos y la mala distribución de la información, pero los robustos diseños de las nuevas tecnologías de las WLAN y la distancia limitada que recorren las señales proporciona una integridad en la información aceptable, esta integridad es igual o mejor que en las redes cableadas.

Compatibilidad: La mayoría de las WLAN proporcionan un estándar de compatibilidad con redes cableadas Ethernet o Token ring. Las computadoras con conexión inalámbrica son soportadas por el sistema de la red de la misma forma que cualquier otra computadora de la red cableada, la única diferencia son los drivers, que una vez instalados la red cableada *"adopta"* a las computadoras inalámbricas como si fueran cualquier otro dispositivo de la red cableada.

4.8.1 COMPATIBILIDAD DE LOS DIFERENTES DISPOSITIVOS INALÁMBRICOS DE LA RED

Se debe de tener en mente que algunos dispositivos de ciertos fabricantes no son 100% compatibles con los dispositivos de otro fabricante; existen tres posibles razones para esta incompatibilidad:

- Diferentes tecnologías no son compatibles: Algunos sistemas se basan en la tecnología de Espectro Ensanchado por Salto de Frecuencia (FHSS), el cual no es compatible con la tecnología de Espectro Ensanchado por Secuencia Directa.

- Los sistemas que utilicen diferente distinta banda de frecuencias para la transmisión no podrán comunicarse, aunque éstos utilicen la misma tecnología para sus diferentes dispositivos.
- Aunque los vendedores lleguen a utilizar los mismos dispositivos para enviar y recibir así como la misma banda de frecuencia, no podrán ser compatibles debido a diferencias en la implementación de cada fabricante.

Aunque las diferencias que existan entre los dispositivos de varios fabricantes sean muy pequeñas, esas pequeñas diferencias marcan la pauta para que existan conflictos a la hora de implementarlos.

4.8.2 FACTIBILIDAD DE USO DE LAS WLAN

REQUERIMIENTOS DE CONOCIMIENTO

Los usuarios de las redes inalámbricas no necesitan de un conocimiento extra para utilizarlas, ya que las WLAN funcionan de la misma manera que las redes cableadas convencionales, los productos de una WLAN incorporan herramientas de diagnóstico para detectar posibles errores para corregir los problemas asociados con los dispositivos inalámbricos.

INSTALACIÓN

Estas herramientas fueron incorporadas con la finalidad de simplificar muchos de los problemas que se tenían en las redes cableadas en cuanto a instalación y configuración se refiere, además los puntos de acceso son los únicos dispositivos que necesitan cable. La falta de cable hace que el desplazamiento sea mas fácil, de manera que es muy sencillo llevar la red de un lugar sin necesidad de modificarla en su totalidad y sólo adecuándola al nuevo lugar en la que se va a implementar.

COSTO

Los costos que se generan, son de infraestructura para los puntos de acceso y las tarjetas para conexión inalámbrica de las computadoras. Estos costos dependen del número de puntos de acceso que se van a utilizar.

El costo de los puntos de acceso va desde los 1000 a los 2000 dólares, de manera que el número de puntos de acceso que se requieran depende de la distancia que se quiera cubrir y del número y tipo de usuarios que integraran la red inalámbrica. Las tarjetas inalámbricas tienen un precio que va desde los 300 hasta los 1000 dólares. En cuanto al costo de mantenimiento de una WLAN, es más bajo que la instalación y el mantenimiento de las redes cableadas; esto es, porque las redes WLAN eliminan todo lo que es el costo de instalación de los tendidos de cable asociado con la instalación y reparación cuando los segmentos se dañan por X cosa, a su vez, una WLAN simplifica los cambios, desplazamiento de la red y extensiones que se le hagan por lo que se reducen los costos.

ESCALABILIDAD

La arquitectura de una WLAN puede ser sencilla o bastante compleja ya que pueden soportar bastantes nodos o extensas áreas físicas instalando más puntos de acceso para amplificar la señal y cubrir más terreno.

Los dispositivos inalámbricos de los usuarios finales han sido diseñados para funcionar sin batería de alimentación proveniente de las computadoras portátiles o corriente alterna, puesto que no cuentan con conexión propia cableada de manera que los fabricantes buscan la manera de maximizar el uso de la energía de la computadora y ampliar mas el tiempo de vida de cada batería.

4.9 EL FUTURO DE LAS REDES INALÁMBRICAS

En muy poco tiempo se han logrado avances significativos en esta nueva tecnología, poco a poco IEEE tiene nuevas iniciativas sobre diferentes aspectos, algunos de los aspectos sobre los cuales se están trabajando son los siguientes:

- Mejoras de seguridad
- Operación de puentes (bridges)
- Interoperabilidad entre puntos de acceso
- Extensiones a mayores anchos de banda

También se está trabajando en el aspecto de la seguridad, que como es sabido no hay una seguridad muy buena. Uno de los puntos más esperados es el de la calidad de servicio QoS, el cual será 802.11e, que es esencial para aplicaciones multimedia, como lo es la videoconferencia.

Como se ha mencionado anteriormente, el estándar 802.11b es el más amplio que existe; pero hay otro problema aparte del de la seguridad que se debe de atender con prontitud: la banda de frecuencias por la cual se transmite ya se está saturando y su velocidad no es muy elevada, es lo equivalente a una red Ethernet que opera a 10 Mbps con un hub. Aunque de momento ya se opera en la frecuencia que utilizan los hornos de microondas y los teléfonos inalámbricos, pero con la desventaja de que estos aparatos pueden afectar el buen funcionamiento de una WLAN basada en el estándar 802.11b, y dentro de poco empezarán a pegar las WPAN (Wireless Personal Area Network) que son para comunicaciones a corta distancia que se van moviendo dentro de el mismo espectro; como el medio de transmisión en este tipo de redes es el aire, no existe algún dispositivo que regule el ancho de banda como lo hace un switch Ethernet, de manera que puede que las WLAN se mueran en el intento y queden completamente saturadas de manera que se presida de éstas en donde no quede otra opción.

Para dar solución a estos problemas se cuenta con el estándar 802.11a, el cual utiliza una banda que todavía no esta saturada y maneja velocidades más altas, pero esta banda no esta libre en todo el mundo y puede llegar a presentar problemas más adelante, por ejemplo en Japón cuenta con la mitad de ancho de banda y en lo que es Europa esta restringida y de hecho IEEE esta trabajando para poder adaptarla.

En la práctica lo que se esta implementado en estos días es 802.11b y es difícil que las empresas migren ya que tienen mucho dinero invertido y es poco factible que tiren su dinero por una tecnología nueva, con poco soporte y mucho más cara.

Lo que resulta evidente es que todas las miradas están puestas en esta tecnología y que las empresas que resultan ampliamente beneficiadas son las que mas muestran interés, si así sucede será necesario incluirlas dentro de los programas de formación tecnológica de redes.

CAPITULO V

REDES INALÁMBRICAS CON LINUX

Se escogió hablar de las redes bajo Linux ya que es una buena opción para implementarse en alguna empresa o campus universitario. Las empresas y escuelas de hoy en día están tratando de minimizar sus gastos en cuanto a las licencias que tienen que pagar por año, dependiendo del software que utilicen y cuantas copias requieran, las licencias van incrementando. Linux ofrece su tecnología libre de pago, aunque no es tan libre porque se paga una módica cantidad por los manuales, pero es por donde las empresas pueden ahorrarse miles de pesos, ahora bien el migrar de una plataforma a otra resulta un poco difícil ya que la mayoría de los usuarios están muy ligados a la tecnología que Microsoft maneja y cambiar a una tecnología que para muchos es completamente diferente resulta complicado por el cambio de esquemas y protocolos.

Aunque Linux ha tratado de hacer interfases gráficas muy similares a las de Windows, internamente funcionan de distinta manera y los comandos para ejecutar alguna aplicación también son distintos. Aunque seria de gran utilidad trabajar con ambos sistemas, pero la incompatibilidad que existe entre ellos no lo permite; aunque se puede sacar provecho de estas "incompatibilidades" ya que Linux es fuerte en algunos procesos y Windows lo es en otros. En conjunción se pueden lograr muchos beneficios.

5.1 RESEÑA DE LINUX

Unix es uno de los mejores sistemas operativos debido a su extenso soporte y distribución que, originalmente fue creado para multitareas con tiempo compartido para minicomputadoras a mediados de los 70's, y es uno de los sistemas más utilizados, aunque es confuso para el usuario y tiene problemas de estandarización. De manera que para muchos hackers, Unix, es el único sistema operativo. El desarrollo de Linux viene de un grupo de hackers de Unix que quisieron hacer su propio sistema. Existen muchas versiones de Unix, que van desde computadoras pequeñas hasta macrocomputadoras, la mayoría de las versiones existentes de Unix para computadoras personales son muy caras.

Linux es una versión de Unix pero con la diferencia de que este es libre, que fue inicialmente desarrollado por Linus Torvalds, fue desarrollado con la ayuda de programadores y expertos en Unix a lo largo de todo el mundo gracias al Internet. Cualquier persona que sepa programar puede accesar al código fuente de Linux y mejorarlo las veces que se quiera. El no utiliza ninguna línea de código de fuentes de propiedad comercial, y la mayor parte del software para Linux se desarrolla bajo las reglas del proyecto de GNU de la Free Software Fundation, Cambridge, Massachussets.

Al inicio fue solo el proyecto de Linus Torvalds, su inspiración se basaba en Minix que era un pequeño Unix desarrollado por Andy Tanenbaum, y las primeras platicas sobre Linux se dieron en el grupo News comp.os.minix, dichas platicas giraban en torno al desarrollo de un pequeño sistema basado en Unix dirigido a aquellos usuarios de Minix que querían un plus extra.

"El desarrollo inicial de Linux ya aprovechaba las características de conmutación de tareas en modo protegido del 386, y se escribió todo en ensamblador. Linus dice, Comencé a utilizar el C tras escribir algunos drivers, y ciertamente se aceleró el desarrollo. En este punto sentí que mi idea de hacer un Minix mejor que Minix se hacía más seria. Esperaba que algún día pudiese recompilar el gcc bajo Linux... Dos meses de trabajo, hasta que tuve un driver de discos (con numerosos bugs, pero que parecía funcionar en mi PC) y un pequeño sistema de ficheros. Aquí tenía

ya la versión 0.01 (al final de Agosto de 1991) no era muy agradable de usar sin el driver de disquetes, y no hacía gran cosa. No pensé que alguien compilaría esa versión."[35]

Hoy en día, Linux es un clon de Unix completo, que es capaz de ejecutar X Windows, TCP/IP, Emacs, UUCP, y software de correo y News.

5.2 LINUX Y EL AMBIENTE DE RED

En Linux se cuenta con los dos principales protocolos de red para sistemas Unix, los cuales son TCP/IP y UUCP; TCP/IP, como ya se había mencionado anteriormente es un protocolo que permite la comunicación a sistemas de todo el mundo por medio de una única red, conocida como Internet. Con Linux, TCP/IP y con tener una conexión a la red, pueden comunicarse usuarios por todo el Internet a través de correo electrónico, transferencia de datos con FTP y mucho más; en la actualidad ya hay muchos usuarios conectados al Internet usando Linux. Las redes TCP/IP implementan Ethernet como tipo de red física de transporte, pero como no todos los usuarios de Linux cuentan con una conexión Ethernet en su casa, Linux proporciona SLIP (Serial Line Internet Protocol), con este protocolo los usuarios pueden conectarse al Internet a través de un módem. Para poder utilizar el SLIP, se debe de tener un servidor SLIP también, una maquina que permita el acceso a la red por medio del teléfono; muchas empresas y campus universitarios cuentan con servidores SLIP, de manera que si el servidor cuenta con una conexión Ethernet y aparte de módem, puede configurarlo como un servidor SLIP para los demás usuarios. Lo que es NFS (Network File System), permite la compartición de archivos con otras maquinas de la red y el FTP (File Transfer Protocol), permite el intercambio de archivos entre maquinas.

Para los usuarios que tiene una experiencia previa con aplicaciones TCP/IP Unix el ambiente Linux se les hará muy familiar. El servidor Linux de X también soporta

[35] Ver: http://www.monografias.com/trabajos/redes_linux.htm

TCP/IP, lo que permite ver aplicaciones que están corriendo en otro sistema sobre la pantalla.

UUCP

UUCP (UNIX to UNIX Copy) es un mecanismo ya viejo que permite la transferencia de archivos, correo electrónico y noticias entre maquinas Unix. Anteriormente las maquinas UUCP se conectaban a través de cable telefónico y un módem, una de las funcionalidades de UUCP es que también trabajo sobre redes TCP/IP. La ventajas es que si no se tiene acceso a una red TCP/IP o en su defecto a un servidor SLIP, se puede configurar un sistema de manera que pueda enviar y recibir archivos y correo usando el UUCP.

5.3 REDES CON LINUX

Para meter a Linux en ambientes de red basados en el protocolo TCP/IP, se empezó a trabajar en 1992 cuando Ross Biro y otros programadores crearon lo que se conoce como Net-1. Des pues de varios esfuerzos más y con logros bastante buenos surgió Net-2, y la primera versión pública Net-2d salió en el verano de 1992. Esta versión han participado y ampliado diversos programadores pero en especial Alan Cox.

Tras numerosos cambios en el código nació la versión Net-3 después de que salió Linux 1.0, esta es la versión de código incluida en el kernel actualmente.

La versión Net-3 ofrece lo que son drivers de dispositivo para una gran variedad de tarjetas Ethernet que existen en el mercado hoy en día, así como SLIP (para enviar tráfico de red sobre líneas serie), y PLIP que es para líneas en paralelo. Con el Net-3 Linux tiene lo que es una implementación de TCP/IP, esta implementación ha tenido satisfactorios resultados, incluso funciona mejor que algunos de los Unix de pc comerciales. El nuevo desarrollo que se esta dando, tiene como prioridad la estabilidad necesaria para su buen funcionamiento en nodos de Internet. Además

de estas implementaciones, existen varios proyectos puestos en marcha que están mejorando la versatilidad de Linux, un driver PPP (Protocolo Punto a Punto), que tiene como función enviar el tráfico de la red sobre líneas en serie; actualmente existe una versión beta. Alan Cox también implementó un driver para lo que es el protocolo IPX de Novell, pero el desarrollo para hacer compatible un paquete de red con el de Novel se ha visto truncado, debido a la negativa de Novell para facilitar los documentos necesarios para desarrollar este tipo de aplicaciones compatibles con Linux.

5.4 PROTOCOLO IP (INTERNET PROTOCOL) EN LINUX

Linux se beneficia de este protocolo ya que su principal ventaja es que convierte redes que son físicamente distintas como si fueran una red aparentemente homogénea, a lo que se le conoce como "Internet working".

El IP necesita un esquema de direccionamiento distinto al que maneja el hardware, esto se lleva a cabo asignándole a cada estación un número de 32 bits de longitud, el cual define su dirección IP. La dirección IP se asigna como 4 números en decimal, uno por división de 8 bits y a su vez están separados por puntos, como por ejemplo 192.76.23.1. A esta forma de acomodarlos se le llama *"notación de puntos"*.

El SLIP y el PPP, son protocolos que son muy utilizados para enviar paquetes IP por medio de enlaces serie; algunas instrucciones ofrecen acceso telefónico PPP y SLIP a computadoras conectadas a Internet, eso a su vez le proporciona conectividad IP a las personas privadas. Para poder trabajar con estos dos protocolos (SLIP y PPP), no es necesario hacer modificaciones al hardware, ya que puede utilizarse cualquier puerto serie.

En el esquema de Internet están disponibles 4000 millones de direcciones IP, las direcciones son distribuidas en redes que son de distinto tipo, una red clase A, posee 16 millones de hosts, una de clase B posee 65000 y una de clase C 254.

Esta división ayudaba al enrutamiento de paquetes TCP/IP pero con la desventaja de que no utilizaba muy bien todas las direcciones IP disponibles.

5.5 WLAN CON LINUX SuSE

Al igual que en Windows, en Linux las redes se configuran de modo *Ad-Hoc*, en el cual todas las tarjetas se comunican entre sí y también con los nodos de la red cableada. Y el otro modo llamado *Managed*, en el cual todos los dispositivos se comunican con un elemento central, el ya antes mencionado **Acces Point**, que a su vez tiene la función de comunicar la parte de la red cableada con la inalámbrica.

5.5.1 PARÁMETROS WLAN A CONFIGURAR CON LINUX

Los principales parámetros que se deben de configurar en la maquina con Linux son los siguientes:

- Mode: Indica el modo de funcionamiento en el cual se va a poner la tarjeta
- ESSID: Identificador de la red, es decir, su nombre
- Nick: Identificador de alguna maquina en la red
- Nwid: Es parecido al ESSID, de alguna forma identifica la red
- Freq: Indica la frecuencia que se va a utilizar o el canal
- Channel: Los mismo que el anterior
- Key: Si se quiere cifrar la comunicación, este parámetro sirve para indicar la clave que se va a utilizar

CONFIGURACIÓN DE LA TARJETA INALÁMBRICA CON SuSE

Solo existen cuatro fabricantes de electrónica WLAN:

- Lucent
- Cisco
- Intersil
- Atmel

El driver orinoco_cs proporciona SuSE en su distribución 8.0 que sirve para las tarjetas con electrónica de Cisco e Intersil. De forma que SuSE reconoce el hardware y sólo se tienen que instalar las wireless-tools.

5.5.2 WIRELESS TOOLS

Para poder trabajar de modo inalámbrico es necesario tener instaladas estas herramientas, si no se cuenta con ellas simplemente no se podrá conectar la computadora de manera inalámbrica.

Para instalar las wireless tools, se debe de meter el siguiente código:

rpm –ga | grep wireless-tools

Para comprobar que las herramientas están instaladas saldrá algo parecido a lo siguiente:

```
admin@tux3c: ~> rpm-ga | grep wireless-tools
wireless-tools-23-31
admin@tux3c: ~>
```

5.6 COFIGURACIÓN AD-HOC

Para este tipo de funcionamiento se deben de configurar los mismos parámetros wireless para todas las estaciones de trabajo. Como ejemplo, el archivo /etc/sysconfig/network/wireless que se obtiene al configurar las wireless tools, se debe de configurar conforma lo marca el "listado Ad-hoc".

En ese archivo se indica lo siguiente:

- Modo de funcionamiento Ad-hoc
- Identificador de red
- El identificador de el equipo que se esta usando, como por ejemplo Computadora 1
- Opcionalmente la clave de cifrado, si se requiere de cifrar las comunicaciones

Ya cuando se haya modificado, se necesita reiniciar con los comandos, como el root:

Ifdown/ifup

Si es una tarjeta PCI o con la instrucción siguiente:

rcpcmcia restart

en caso de que sean pcmcia

5.6.1 CONFIGURACIÓN MODO MANAGED

Este modo de funcionamiento es en donde se especifican los parámetros de funcionamiento de el Punto de Acceso (AP), los que van a indicar el modo de configuración de la tarjeta.

Que al igual que la configuración del Ad-hoc, se configura conforme al *listado MANAGED*. Y respecto a la configuración Ad-hoc, la única diferencia estriba en el

valor del parámetro WIRELESS_MODE, que en este caso es MANAGED en vez de Ad-hoc.

5.6.1 CONFIGURACIÓN DE TARJETA 3COM WIRELESS, LAN XJACK 3CRWE62092A

Existen varias tarjetas en las cuales Linux SuSE no tiene los drivers de configuración como en caso de estas tarjetas, su configuración no es muy complicada, solo se debe de tener cuidado al momento de meter los dirvers porque al momento de meter otros de versiones distintas de la tarjeta, ocasionara problemas, incluso graves.

La tarjeta 3COM, tiene la peculiaridad de que esconde la antena dentro de la tarjeta, esto permite un fácil maneja sin necesidad de desconectarla para trasladar o guardar la computadora portátil, pero la desventaja es que el SuSE en sus versiones 8.0 y 8.1, no tiene los drivers necesarios para que funcione. Para configurarla, se accesa con la cuenta *root* o raíz y se mete el código *cardctl ident* para checar como SuSE identifica la tarjeta, esto nos debe de arrojar el siguiente resultado[36] o algo similar:

```
tux3c:/home/admin # cardctl  ident
socket 0:
product info: "3COM", "3CRWE62092A Wireless LAN pc card"
manfid: 0x0101, 0x2092
function: 6 (network)
Socket 1:
no product info available  tux3c:/home/admin #
```

Una vez que se tengan los drivers, lo que se debe de hacer es:

[36] Ver: http://sdb.sese.de/en/sdb/html/wavelan.html

- Comprobar que se tengan instaladas las fuentes del kernel
- Tener instaladas las wireless-tools
- Instalar el driver y configurar la tarjeta

COMO INSTALAR LAS FUENTES DEL KERNEL

Las fuentes del kernel se pueden instalar con *yast* desde la unidad de CD-ROM con los discos de instalación del SuSE, se encuentran como suse/d3/kernel-source-2.4.18.SuSE-35.i386.rpm

INSTALACIÓN DE LOS DRIVERS

Cuanto se cuenta con el driver y utilizando la cuenta de root se procede a realizar la siguiente configuración:

- Copiar el archivo con el driver en : /usr/scr
- Se procede a descomprimirlo
- Acceder al subdirectorio creado cd/usr/scr/poldhu
- Se ejecuta make config, make all, make install

Ya una vez instalados las Fuentes del kernel y los drivers de la tarjeta se podra trabajar en la red, solo resta que el AP identifique la computadora y listo.

5.7 HARDWARE CERTIFICADO PARA REDES WIRELESS CON LINUX

A continuación se muestra una lista de los diferentes dispositivos que se pueden implementar en una red inalámbrica utilizando el sistema operativo Linux; a su vez estos dispositivos están certificados por la Wi-Fi y la WECA.

Se mostrara una lista de tarjetas para pc portátil, antenas direccionales, puntos de acceso, gestores de acceso, antenas de largo acceso y bridges inalámbricos.

PUNTO DE ACCESO INALÁMBRICO DE 11 Mbps EZ CONNECT SMC2655W

Características:

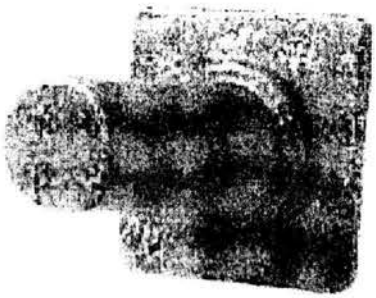
1. Compatibilidad con LAN's inalámbricas de 11 Mbps
2. 2.4 Ghz. Ethernet inalámbrico
3. Direct Sequence Spread Spectrum (DSSS). Ofrece inmunidad gracias a la interfaz.
4. Soporta hasta 64 usuarios
5. Filtrado de direcciones MAC
6. Encriptación WEP de 64/128 bits y control de acceso
7. Compatible con los estándares IEEE 802.11B e IEEE 802.3
8. Compatible con LINUX

EZ CONNECT BRIDGE SMC2682W DE 11 Mbps INALÁMBRICO

Características:

- Compatibilidad con LAN inalámbrica de 11 Mbps
- 2.4 GHz Ethernet inalámbrico
- Utiliza DSS
- Soporta 1024 usuarios
- Filtrado de direcciones MAC
- Utiliza encriptación WEP (64/128 bits)
- Compatible con LINUX
- Compatible con los estándares IEEE 802.11b e IEEE 802.3
- Certificado Wi-Fi

ANTENAS INALÁMBRICAS DE LARGO ALCANCE EZ CONNECT SMCANT-DI105, SMCANT-DI135, SMCANT-DI145, SMCANT-DI215 Y SMCANT-KIT



Características:

- El rango de frecuencia alcanzado es de 2.400 – 2.483 GHz.
- El alcance que tiene es de:

  SMCANT-DI105: 10.5dBI

  SMCANT-DI135: 13.5dBI

  SMCANT-DI145 : 14.5dBI

  SMCANT-DI215 : 21.5dBI
- Polarización elíptica y circular
- La impedancia que tiene es de 50 Ohms
- Las dimensiones van desde los 11.36 cm hasta los 31.6 cm
- Los diámetros son de 61 cm y la profundidad es de 45 cm

SERVIDOR WLAN EZ EliteConnect SMC2504W

Este servidor inalámbrico provee del servicio de protección de red, gestión de acceso y derechos, es decir, cuando algún usuario desea ingresar a la red, éste

checa el nombre de usuario y password, de manera que si concuerda con los que tiene dados de alta, automáticamente lo deja ingresar; así mismo checa los permisos que se le otorgan a dicho usuario. Los permisos son los otorgados por el administrador de la red hacia los usuarios, es decir, se pueden dar permisos de que el usuario pueda modificar archivos, que tenga acceso a la base de datos pudiéndola modificar o no, eso depende de los permisos que se le hallan otorgado como se mencionó.

Características:

- Gestión de derechos de usuario
- Soporta VPN para acceso basado en derechos
- Soporte de autentificación de usuarios
- Configuración y gestión basada en Internet
- IEEE 802.11b, 802.3, 802.3u, 802.1x
- 4x 10Base-T/100Base-TX puertos Ethernet

GESTOR DE ACCESO EZ ELITE CONNECT WLAN SMC2502W

Es un gestor de derechos para puntos de acceso adicionales en las redes inalámbricas.

Al igual que el servidor SMC2504W, el SMC2502W basa su funcionamiento en soporte de VPN para la autentificación de los usuarios, soporta hasta 4 puntos de

acceso, su configuración es basada en gestión e Internet y es compatible con los mismos estándares que el anterior.

Como se puede observar es solo para darle un apoyo extra al servidor SMC2504W, ya que a veces se satura demasiado la red por la carga excesiva de los usuarios y por los recursos que se comparten, porque como ya es sabido todo esto recae en el servidor.

Pero lo más importante es que estos productos son compatibles con LINUX, solo se deben de instalar las gíreles tools correctamente y fijarse en la versión de los controladores y con ello se podrá trabajar sin ningún problema.

Esto es algo muy breve de todo lo que puede hacer LINUX al momento de trabajar con él, se debe de tener conocimiento previo para poder configurarlo correctamente y así entender como trabaja, el hardware[37]

[37] Todas las imágenes de los dispositivos, así como su respectiva información de cómo funcionan bajo LINUX se encuentran en http://www.smc.com

CONCLUSIONES

Las redes inalámbricas están teniendo aceptación en algunas empresas y escuelas por las necesidades de movimiento que estas tienen. La finalidad de las redes inalámbricas no es sustituir a las redes tradicionales de cableado, si no ser una extensión de ellas para facilitar es desplazamiento de los usuarios, implementarlas en lugares en donde es muy difícil cablear o simplemente la estructura de el edificio no permite modificaciones.

Como se menciono anteriormente, una red híbrida nos trae muchas ventajas y es de fácil instalación; la ventaja más importante es que el segmento cableado se puede hacer compatible sin necesidad de hacer complejas instalaciones, de manera que se debe de dejar lo que ya está instalado, es decir, dejar la estructura original para poder hacerla compatible porque seguiríamos teniendo la velocidad que nos brinda la parte cableada y expandirnos con la parte inalámbrica.

Comparando una red tradicional de cableado con una red inalámbrica, se puede decir que existen ciertas desventajas de las dos, es decir, las redes tradicionales de cableado (como se ha mencionado) son de difícil implementación en espacios muy reducidos; ésta es una ventaja que tienen las redes inalámbricas sobre las redes tradicionales de cableado, a su vez las redes inalámbricas todavía no alcanzan la velocidad de transmisión de las redes cableadas.

Entonces como se puede observar, tanto las redes de cableado como las redes inalámbricas, pueden llegar a funcionar en conjunto y dar esa funcionalidad extra a la red.

Así mismo, existen varios fabricantes de los diferentes componentes para implementarse en la red inalámbrica, de manera que se debe de seleccionar cuidadosamente al fabricante al cual se le va a consumir de sus productos, tomando en cuenta lo que ofrece, velocidades de transmisión, compatibilidad, calidad, garantías, soporte técnico y sobre todo lo que en realidad se va a necesitar.

Las redes inalámbricas llaman la atención de los usuarios por la flexibilidad de éstas mismas, es decir, ofrecen una conexión continua al usuario, pudiendo éste mismo, desplazarse de un lugar a otro sin perder la conexión, pero teniendo en cuenta que el usuario debe de moverse dentro del rango de alcance de el punto de acceso o puntos de acceso.

En una empresa lo que se busca es la flexibilidad; una manera de tener esa "flexibilidad" es el implementar una red inalámbrica, ya que muchos de los usuarios se quejan de la poca movilidad que tienen, el usuario busca la manera de llevar su computadora portátil de un lado a otro y olvidarse de el estorboso cable o de tener cuidado de no jalarlo.

La tecnología óptica es la de más fácil implementación, ya que para la tecnología de radio frecuencia, se deben de sacar permisos a la S.C.T. (Secretaría de Comunicaciones y Transportes) para utilizar una banda, de lo contrario se puede violar la ley. Además se debe de tener especial cuidado en el hardware que se compre para realizar una red inalámbrica de radio frecuencia, pues se debe de asegurar que todo ese hardware este aprobado por la S.C.T.

Nos enfrentamos a la realidad de que la tecnología avanza muy rápido y sobretodo en el campo de la computación, de manera que debemos de estar preparados a estos cambios tan radicales y una manera de hacerlo es actualizándonos, y en especial me parece que las redes es en donde debemos de poner especial atención porque por ahí es por donde se mueve la información.

GLOSARIO

PCMCIA: Organización que desarrolla el estándar para pequeños dispositivos del tamaño de una tarjeta, denominados comúnmente tarjetas de PC.

10BaseT: Es un estándar IEEE 802.3, aplicado para operar en redes locales Ethernet de 10Mbps, con cable de par trenzado o UTP, con un HUB que opera con cable.

802.11: Es un grupo de especificaciones desarrolladas por IEEE para tecnologías de red local o WLAN.

802.11a: Describe el estándar de redes inalámbricas que operan a 5 GHz.

802.11b: Describe el estándar de red inalámbrica para una WLAN que opera con frecuencias de 2.4 GHz.

802.11g: Este estándar es nuevo, se encarga de describir un método de red inalámbrica que opera en una banda de radio de 2.4 GHz.

IEEE: Instituto de ingenieros eléctricos y electrónicos, este instituto se encarga de reunir a todos los ingenieros en electrónica y eléctricos, científicos etc., para llegar a un acuerdo en cuanto a las normas para las diferentes arquitecturas de red.

A

ADSL: Línea de abonados digital, es una tecnología que permite al acceso de alta velocidad al Internet, ya sea desde el hogar o de la empresa.

Ancho de Banda: El ancho de banda se refiere a la capacidad de transmisión de una red.

AUI: Unidad de Acoplamiento de Interfase (Attachment Unit Interface).

B

Banda Ancha: Término aplicado a la transmisión de datos a alta velocidad, como la conexión por cable.

BS: Estación Base (Base Station).

BIOS: Sistema básico de entra y salida, este programa es el que utiliza el procesador para arrancar la computadora cuando se enciende, al mismo tiempo gestiona el flujo de datos entre el sistema operativo y los dispositivos adjuntos.

bps: Bits por segundo, es una medida que se utiliza para medir la transmisión en la red.

Bus del sistema: Se encarga de conectar al procesador con la memoria principal, gestiona la transferencia de datos y las instrucciones entre estos dos componentes.

C

CSMA/CD: Censor de Medio de Acceso Múltiple/Con detección de Colisión

CP: Señal de Presencia de colisión (Collision Presence).

CDMA: Acceso Múltiple con División de Códigos, es una tecnología móvil digital la cual utiliza técnicas de amplio espectro, CDMA no asigna una frecuencia específica a cada usuario, de manera que cada canal utiliza el espectro disponible.

Clave de codificación (WEP): La clave de codificación es una serie de caracteres, puede ser alfanumérico, es decir, puede incluir letras y/o números, esta clave permite que los datos se codifiquen y decodifiquen en forma que se pueda compartir la información de manera segura. WEP utiliza una clave de codificación, esta clave codifica los datos que salen en las redes inalámbricas.

Codificación de Huffman: Esta es utilizada para reducir los datos.

Control de acceso al medio: La dirección de control de acceso al medio (MAC), es una dirección Ethernet única a nivel mundial grabada en un chip para un adaptador de red.

Cortafuegos (firewall): Protege al acceso a la red, bloquea a los usuarios no autorizados. El cortafuegos se puede implementar en el software o en el hardware (o ambos), evita el acceso ilimitado a la red.

Conmutador: Un conmutador es un dispositivo que conecta varios equipos en una red local para que se puedan comunicar entre sí, que a diferencia de un HUB, el

conmutador no comparte el ancho de banda, es decir, cada puerto del conmutador cuenta con el ancho de banda completo.

D

DHCP: Protocolo de configuración dinámica del host, permite a un servidor asignar de forma dinámica direcciones IP de una lista predefinida a dispositivos de una red, también limita el periodo de uso de estas direcciones de forma que se puedan reasignar.

DOS: Sistema operativo de disco.

Datagrama: Agrupamiento lógico de de información enviada como unidad de la capa de red en un medio de transmisión.

DLL: Capa de enlace de datos, Data Link Layer.

Dirección IP: Es un número de 32 bits, el cual identifica al emisor y receptor de información a través de Internet.

DNS: Sistemas de Nombre de Dominio, es un programa que traduce las direcciones URL de Internet en direcciones IP al acceder a una base de datos mantenida en un grupo de servidores de Internet. A manera de ejemplo el DNS traduce una dirección de Internet como www.doodie.com en una dirección IP 207.209.45.78.

E

Encapsulamiento: Proporciona protección hermética y no hermética, determina el formato y sirve como interconexión de primer nivel externa para el dispositivo por medio de terminales de encapsulado.

Espectro extendido de salto de frecuencia: Esta técnica de modulación es utilizada por 802.11 y funciona distribuyendo las señales de datos a través de todo el espectro de frecuencias, es una técnica bastante fuerte y segura frente a la intercepción de los datos.

ESSID: Es el nombre con el que se identifica una red inalámbrica 802.11.

Ethernet: Es una tecnología de red estándar internacional para lo que son las implementaciones cableadas. Lo que son las redes 10BaseT ofrecen un ancho de banda de 10 Mbps, también hay Fast Ethernet que ofrece velocidades de 100 Mbps y Gigabit Ethernet que ofrece 1000 Mbps.

Extensiones Internet Streaming (SIMD): Consiste en instrucciones que reducen el número total de instrucciones necesarias para ejecutar una tarea de programación determinada, de este modo puede propiciar una mejora en cuento al rendimiento se refiere al acelerar una amplia gama de aplicaciones.

I

IP: Internet Protocol, determina si la red utiliza la arquitectura de grupos de trabajo o cliente/servidor.

IPX: Este protocolo de red es utilizado por los sistemas operativos Novell Netware, IPX es un protocolo de datagramas que se utiliza para las comunicaciones sin conexión.

N

NAT: Traducción de dirección de red, permite a un grupo de equipos compartir de forma dinámica una única dirección de IP entrante desde una conexión de marcación, cable o ADSL, NAT toma la dirección entrante para crear otra dirección IP para cada equipo de la red.

NIC: Tarjeta de interfaz de red.

P

PAN: Es una red personal inalámbrica pero de muy poco alcance (10 metros).

Paquete: Es el segmento de un paquete transmitido a través de una red, dicho paquete contiene la dirección del destino y los datos.

PCI: Interconexión de Componentes Periféricos, es un estándar de bus local.

R

RDSI: Red Digital de Servicios Integrados, RDSI es un tipo de conexión de Internet la cual proporciona los servicios digitales desde las instalaciones del cliente a la red telefónica de marcación.

RF: RF o radiofrecuencia, cubre una gran variedad de frecuencias electromagnéticas de alta frecuencia que son utilizadas en las transmisiones de radio.

S

S.C.T: Secretaría de Comunicaciones y Transportes

Servidor Proxy: Este servidor es el encargado de actuar como un intermediario entre una aplicación cliente Internet, con la finalidad de mejorar las operaciones de red y de seguridad. También se utiliza para evitar lo que es la comunicación directa entre dos o más redes, especialmente al conectar la red a Internet.

SPX: Intercambio Secuencial de Paquetes; éste es un protocolo de nivel de transporte el cual es utilizado en las redes Novell Netware, es decir, el SPX se coloca encima de una capa IPX (nivel 3) y ofrece servicios orientados a la conexión de dos computadoras de la red; es utilizado fundamentalmente en las pequeñas redes cliente-servidor.

SSID: Identificador de grupos de servicio; es el nombre que identifica de forma única a una red inalámbrica.

SSL: Nivel de socket seguro; es un esquema de codificación que es utilizado por muchos sitios de compras por Internet y servicios de banco para proteger la integridad de los datos financieros en las transacciones que se van realizando.

Subred: Es una división de una red más grande. Comúnmente se divide en subredes para simplificar la utilización de direcciones entre numerosos equipos. Las subredes se conectan a la red central a través de un ruteador, hub, switch. Cada red local o WLAN se configura para que utilice la misma subred con todos los equipos locales con los que se comunique.

T

TDMA: Acceso múltiple por división de tiempo; es una tecnología que permite el envío de un servicio digital inalámbrico a través de la multiplexación por división de tiempo (TDM). Básicamente el funcionamiento de TDMA consiste en dividir la frecuencia de radio en espacios de tiempo y asignarlos después a varias llamadas.

BIBLIOGRAFIA

BLACK, Wyless, ***REDES DE COMPUTADORES, PROTOCOLOS, NORMAS E INTERPRETES,*** Editorial Grupo Alfa Omega.

TANENBOWN, Andrew, ***REDES DE COMPUTADORAS***, USA, Editorial Prentice Hill núm. 10, 1999, 9 pp.

OTRAS FUENTES

LÓPEZ RUIZ, Jorge, ***"La computadora ideal",*** en ***PC Magazine,*** año XII, vol , núm. 10, México, Editorial Televisa, junio del 2002, 35 pp.

http://www.monografias.com

http://www.proxim.com

http://www.newstuff.com

http://www.linix.com

http://www.uv.es

http://www.intel.com

http://www.techdepot.com/product?.asp/productid=107934&affid=673

http://www.orinocowireless.com

http://www.smc.com

http://www.freebaries.com

http://www.google.com

http://www.lawebdelprogramador.com

http://www.ataenea.idistrital.edu.co/cursos/teleproceso/redes/htm/cap3-html

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

http://www.geocities.com/Eureka/Plaza/2131/primeras.html

http://www.geocities.com/nicaraocalli/

http://www.ts.es/doc/area/produccion/ral/BANDA.HTM

http://ccdis.dis.ulpgc.es/ccdis/laboratorios/redes.html