Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

ANÁLISIS DE REDES INALÁMBRICAS, SUS TECNOLOGÍAS, ARQUITECTURAS FÍSICAS, LÓGICAS Y LOS DIFERENTES COMPONENTES NECESARIOS PARA SU IMPLEMENTACIÓN

Emerson Alexander Gómez Morales

Asesorado por el Ing. José Aníbal Silva de los Ángeles

Guatemala, febrero de 2012

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ANÁLISIS DE REDES INALÁMBRICAS, SUS TECNOLOGÍAS, ARQUITECTURAS FÍSICAS, LÓGICAS Y LOS DIFERENTES COMPONENTES NECESARIOS PARA SU IMPLEMENTACIÓN

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

EMERSON ALEXANDER GÓMEZ MORALES
ASESORADO POR EL ING. JOSÉ ANÍBAL SILVA DE LOS ÁNGELES

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, FEBRERO DE 2012

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Juan Carlos Molina Jiménez
VOCAL V	Br. Mario Maldonado Muralles
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Julio César Solares Peñate
EXAMINADOR	Ing. Romeo Neftalí López Orozco
EXAMINADORA	Inga. María Magdalena Puente Romero
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ANÁLISIS DE REDES INALÁMBRICAS, SUS TECNOLOGÍAS, ARQUITECTURAS FÍSICAS, LÓGICAS Y LOS DIFERENTES COMPONENTES NECESARIOS PARA SU IMPLEMENTACIÓN

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 27 de mayo de 2010.

Emerson Alexander Gómez Morales

Guatemala 07 de Abril de 2011

Señor Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería
Universidad San Carlos de Guatemala

Señor Coordinador:
Ing. Carlos Guzmán

Por medio de la presente, me permito informarle que he revisado completamente el trabajo de tesis titulado: Análisis de Redes Inalámbricas, sus Tecnologías, Arquitecturas Físicas, *Lógicas y los Diferentes Componentes Necesarios para su Implementación; desarrollado por* Emerson Alexander Gómez Morales y puedo concluir que dicho trabajo cumple con los objetivos propuestos en el anteproyecto de tesis.

Por lo tanto, el autor de esta tesis y yo, como asesor, nos hacemos responsables por el contenido y conclusiones de la misma.

Sin otro particular, me es grato suscribirme.

Atentamente,

JOSE ANIBAL SILVA DE LOS ANGELES
ING ELECTRONICO
COLEGIADO No 5067

Ing. José Aníbal Silva de los Angeles
Asesor Nombrado

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

Ref. EIME 29. 2011
Guatemala, 12 de MAYO 2011.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingeniería Mecànica Elèctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: ANÁLISIS DE REDES INALÁMBRICAS, SUS TECNOLOGÍAS ARQUITECTURAS FÍSICAS, LÓGICAS Y LOS DIFERENTES COMPONENTES NECESARIOS PARA SU IMPLEMENTACIÓN, del estudiante Emerson Alexander Gómez Morales, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

Ing. Carlos Eduardo Guzmán Salazar
Coordinador de Electrónica

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

CEGS/sro

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 40. 2011.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; EMERSON ALEXANDER GÓMEZ MORALES titulado: ANÁLISIS DE REDES INALÁMBRICAS, SUS TECNOLOGÍAS ARQUITECTURAS FÍSICAS, LÓGICAS Y LOS DIFERENTES COMPONENTES NECESARIOS PARA SU IMPLEMENTACIÓN, procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 03 DE JUNIO 2,011.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 086.2012

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **ANÁLISIS DE REDES INALÁMBRICAS, SUS TECNOLOGÍAS, ARQUITECTURAS FÍSICAS, LÓGICAS Y LOS DIFERENTES COMPONENTES NECESARIOS PARA SU IMPLEMENTACIÓN,** presentado por el estudiante universitario **Emerson Alexander Gómez Morales,** autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, 23 de febrero de 2012.

/gdech

ACTO QUE DEDICO A:

Dios	Sobre todas las cosas.
Mi madre	Susana Morales Castro, quien siempre me dio el apoyo y buenas enseñanzas en todo momento de la vida.
Mis hermanos	Rosa Gómez Morales de Chávez, Oscar Armando Gómez Morales. Por todo su apoyo.
Mi esposa	Brenda Ileana Coc Santizo de Gómez. Esposa y compañera incondicional.
Mis hijos	Jazzmine Susana y Emerson Alexander. Por su apoyo incondicional y comprensión.
Mis suegros	José Antonio Coc y Juana Santizo. Por su apoyo incondicional.
Mis cuñados y cuñadas	Con mucho cariño.
Mis amigos y compañeros	Por los momentos que estuvimos estudiando y divirtiéndonos.

AGRADECIMIENTOS A:

Dios	Fuerza creadora del universo.
Mi familia	Por todo su apoyo.
Universidad de San Carlos De Guatemala	Templo de enseñanza y sabiduría que llevaré en mi corazón por siempre.
Mis catedráticos	Por mi formación.
Mis amigos y compañeros	Por su apoyo, paciencia y amistad.
I**ngeniero José Aníbal Silva de Los Ángeles**	Asesor del presente trabajo de graduación, por su valiosa asesoría, por compartir sus conocimientos y por el apoyo brindado para la culminación de mi carrera.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Acceso nomádico Acceso a la red desde cualquier lugar; pero es necesario autenticarse nuevamente cada vez que se cambie de ubicación.

ADSL Línea de Abonado Digital Asimétrica. Es una línea digital de alta velocidad, apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando el alcance no supere los 5,5 km., medidos desde la central telefónica.

Backhaul Red de retorno, conexión de baja, media o alta velocidad. Un *Backhaul* es usado para interconectar redes entre sí, utilizando diferentes tipos de tecnologías alámbricas o inalámbricas.

Banda ancha Transmisión de datos por la cual se envían simultáneamente varias piezas de información, con el objeto de incrementar la velocidad de transmisión efectiva.

Broadcasting Es la distribución de audio y/o señales de vídeo que transmiten los programas a una audiencia.

Broadcast Servicio de la capa de transporte, que permite comunicación punto a multipunto.

BS	Radiotransmisor y receptor utilizado para transmitir y recibir voz y datos desde y hacia teléfonos móviles en una célula o celda en particular.
DSL	Es un conjunto de normas para la conectividad de red de banda ancha sobre líneas telefónicas normales.
Enlace	Es el medio por el cual se transporta información.
Firmware	Parte del *software* de un ordenador que no puede modificarse por encontrarse en la ROM. Es el código de la programación que ejecuta un dispositivo de red.
GPRS	Es una tecnología digital de telefonía móvil; comunicación basada en paquetes de datos. Los intervalos de tiempo se asignan a la conexión de paquetes, mediante un sistema basado en la demanda. Si no se envía ningún dato por el usuario, las frecuencias quedan libres para ser utilizadas por otros usuarios.
GSM	*Global System For Mobile Communications*. Es un sistema de comunicación 2G que utiliza tecnología TDMA.
GPL	Licencia pública general. Puede ser instalado sin limitación en uno o varios ordenadores. En las distribuciones de estos programas debe estar incluido el código fuente.

Handover	Sistema utilizado en comunicaciones móviles celulares con el objetivo de transferir el servicio de una estación base a otra, cuando la calidad del enlace es insuficiente.
Hardware	Componentes electrónicos y electro-mecánicos de una computadora o cualquier otro sistema. Término utilizado para distinguir componentes físicos de los datos y programas.
Host	Computadoras conectadas a una red, que proveen y utilizan servicios de ellas. Un *host* de Internet tiene una dirección de Internet única (dirección IP) y un nombre de dominio único o nombre de host.
Hiperacces	Redes de acceso fijo inalámbrico de banda ancha para aplicaciones multimedia.
Hiperman	Es un estándar de Normas de Telecomunicaciones (ETSI) dirigido principalmente para proveer DSL inalámbrica de banda ancha, cubriendo un área geográfica grande. Es una alternativa europea a Wimax y a la coreana WiBro.
Hotspots	Es una zona de cobertura Wi-Fi, en el que un punto de acceso o varios proveen servicios de red a través de un Proveedor de Servicios de Internet Inalámbrico.

HSDPA	Es la optimización de la tecnología espectral UMTS/WCDMA, incluida en las especificaciones de 3GPP release 5 y consiste en un nuevo canal compartido en el enlace descendente (*downlink*) que mejora significativamente la capacidad máxima de transferencia de información hasta alcanzar tasas de 14 Mbps. Soporta tasas de *throughput* promedio cercanas a 1 Mbps.
IEEE	Institute of Electrical and Electronics Engineers, una fuente de información, recursos y servicios técnicos y profesionales.
Infraestructura	Equipo de red e informático, actualmente instalado.
Interfaz	Conexión con un medio de transmisión por la que se envían los paquetes.
ISP	Es una empresa dedicada a conectar a Internet a los usuarios o las distintas redes que tengan, y dar el mantenimiento necesario para que el acceso funcione correctamente.
LMDS	Sistema de Distribución Local Multipunto, es una tecnología de conexión vía radio inalámbrica que permite, gracias a su ancho de banda, el despliegue de servicios fijos de voz, acceso a internet, comunicaciones de datos en redes privadas, y vídeo bajo demanda.

MAC	Dirección de control de acceso al medio, una dirección MAC es la dirección de hardware de un dispositivo conectado a un medio de red compartido. Máscara de subred, código de dirección que determina el tamaño de la red.
MPLS	(*Multiprotocol Label Switching*) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI.
Módulo *Bluetooth*	Módulo multichip que implementa en hardware y firmware las capas bajas del stack de protocolos *Bluetooth*.
Multipath fading	Término utilizado para describir el desvanecimiento que experimentan las ondas de radios al seguir durante su trayectoria de propagación, diferentes caminos. Tales caminos incluyen, la ionosfera, reflexiones debido a la superficie terrestre, etc.
OFDM	(Multiplexado por división de frecuencia ortogonal) La transmisión de frecuencia que separa la corriente de datos en un número de corrientes de datos de velocidad inferior que se transmiten en paralelo, para prevenir que se pierda información durante la transmisión.
Redes 3G	Sistemas de comunicaciones móviles de nueva generación, que habilitan servicios mejorados de

	comunicaciones, tales como acceso a Internet y la capacidad de ver material de video.
Roaming	Capacidad de un dispositivo de moverse desde una zona de cobertura hacia otra, sin pérdida de la conectividad.
Router	Dispositivo encargado de reenviar paquetes que no están dirigidos a él.
SOFDMA	Acceso de Multiplexación por División de Frecuencia Ortogonal Escalable, asigna diferentes subcanales a los diferentes abonados y soporta el acceso simultáneo a Internet de muchos abonado.
Triple DES:	En criptografía, Triple DES se le llama al algoritmo que hace triple cifrado del DES.
Timeout	Tiempo de espera excedido.
Timeslot	Ranura de tiempo. En *Bluetooth* tiene una duración de 625 us.
Token ring	El anillo de fichas *(token ring*), es una red de topología de anillo que se sirve del pase de fichas, para el control de acceso.

USB	Bus serie universal, los periféricos pueden conectarse y desconectarse con el equipo en marcha, configurándose de forma automática.
UMTS	Sistema de comunicación 3G que utiliza tecnología WCDMA.
VPN	Red privada virtual que conecta una red o, a través de una red intermedia, normalmente Internet.
WIFI	*Wireless-Fidelity* (Wi-fi, Wi-Fi, Wifi, wifi) es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11. Fue creado para ser utilizado en redes locales inalámbricas; sin embargo es frecuente que en la actualidad también se utilice para acceder a Internet.
WAP	Protocolo para aplicaciones inalámbrica.

RESUMEN

La tecnología de comunicación inalámbrica es muy importante en la masificación, despliegue y uso de Internet. Se ha impulsado el desarrollo de todo tipo de dispositivos móviles inalámbricos y al mismo tiempo se han generado nuevos modelos de negocios asociados a esta tecnología.

Actualmente en el mundo se vive una época de cambios, en la cual, los avances tecnológicos son una constante. Es posible apreciar estos adelantos en todas las áreas de las ciencias, pero especialmente, es posible verlos más claramente, en la electrónica y las comunicaciones. Utilizando herramientas como la teoría del tráfico, se ha podido brindar un mejor servicio a los usuarios. Y no sólo se mejoraron los servicios, sino, que se creó infinidad de ellos, a través del tiempo, a tal punto que en algunos de los países del mundo, ya no es necesario el dinero en efectivo, ya que todas las transacciones se realizan por medio de sistemas inalámbricos.

OBJETIVOS

General

Realizar el análisis de redes inalámbricas de acceso a Internet, sus tecnologías, arquitecturas físicas, lógicas y los diferentes componentes necesarios para su implementación.

Específicos

1. Analizar una red inalámbrica de acceso a Internet que satisfaga los requerimientos de funcionalidad, rendimiento y seguridad.

2. Describir los sistemas de protección de una red inalámbrica del acceso no autorizado, aclarando interrogantes de usuarios y dueños de servicio.

3. Analizar la seguridad de las redes inalámbricas y el uso de *software*, para detectar los diversos ataques de piratas informáticos.

4. Considerar normas nuevas que maximicen la cantidad de clientes que soportará una red inalámbrica y las tecnologías que mejoren su rapidez.

5. Analizar qué antena es la más funcional para una red inalámbrica y cuál es la mejor orientación para su adecuado funcionamiento.

INTRODUCCIÓN

El presente trabajo describe cómo una red inalámbrica sustituye el cableado tradicional para montar una red local; ya que en lugar de transmitir la información por medio de cable, se transmiten a través de ondas de radio cifradas, con lo que se elimina una costosa y problemática instalación. En sólo unos minutos, la red local inalámbrica estará lista para funcionar, transmitiendo fiablemente la información gracias a las antenas emisoras / receptoras y tarjetas decodificadoras para cada equipo.

Esto permite la perfecta movilidad de los equipos en red dentro del radio de cobertura de la red inalámbrica, radio que se extiende en las tres dimensiones y que es fácilmente ampliable con las antenas adecuadas. Esto hace de la red inalámbrica un soporte robusto, seguro y poco problemático para todo tipo de edificios.

En el capítulo inicial se incluye una reseña histórica de las redes inalámbricas, los tipos de modulación y los protocolos de enlace. Con apego a la experiencia, se ha demostrado que las ondas de la red inalámbrica no se bloquean ni se distorsionan por objetos sólidos, por lo que pasan fácilmente a través de puertas, tabiques, suelos y techos, y su señal cifrada y de frecuencia modificable por el usuario permite la total ausencia de interferencias.

En el siguiente capítulo se hace un análisis de las redes inalámbricas en los países en desarrollo, describiendo sus características, las diversas redes, capacidad y la optimización del enlace a internet.

En el capítulo tercero se analizan los requerimientos y costos de las redes inalámbricas y las soluciones comerciales de acuerdo con las tecnologías existentes.

En el capítulo cuarto se explica la tipología de una red inalámbrica, cuáles son sus amenazas y los recursos que pueden adquirirse y aplicarse en nuestro medio, para darles una protección adecuada.

Se enfatiza al final sobre las ventajas y desventajas de las redes inalámbricas frente a las redes de cableado tradicional y la función que desempeñan para el desarrollo económico y social de una institución o empresa.

1. INTRODUCCIÓN A LAS REDES INALÁMBRICAS

Las aplicaciones de las redes inalámbricas son infinitas; en un futuro se reunificarán todos aquellos dispositivos con los que hoy se cuenta para dar paso a unos nuevos que se podrán llamar terminales internet en los cuales estarán reunidas las funciones de teléfono móvil, agenda, terminal de video, reproductor multimedia, ordenador portátil etc.

La infraestructura inalámbrica puede ser construida a bajo costo en comparación con las alternativas tradicionales de cableado. Pero construir redes inalámbricas se refiere sólo en parte al ahorro de dinero, dando a su comunidad un acceso a la información más sencilla y económica, la misma se beneficiará directamente con lo que Internet tiene para ofrecer.

El tiempo y el esfuerzo ahorrado gracias a tener acceso a la red global de información, se traduce en bienestar a escala local, porque se puede hacer más trabajo en menos tiempo y con menos esfuerzo. Asimismo, la red se transforma en algo valioso cuanta más gente esté conectada a ella. Las comunidades que se conectan a Internet a una alta velocidad, participan en el mercado global, donde las transacciones suceden alrededor del mundo a la velocidad de la luz. Las personas están encontrando en que el acceso a internet les brinda una voz para discutir sus problemas, políticas, y cualquier cosa que sea importante en sus vidas, de una forma en la cual el teléfono y la televisión no pueden competir. Lo que se creía ciencia ficción se está transformando en realidad, y esta realidad se está construyendo sobre redes inalámbricas.

Es necesario tener un cierto conocimiento sobre la tecnología que va a ser la base de estas aplicaciones. Para ello debe conocerse el mundo de las redes inalámbricas, clasificándolas para centrar la atención en las diferentes variantes que se encuentre.

1.1. Reseña histórica

En realidad, la historia de la red se da al principio del siglo XIX. El primer intento, de establecer una red amplia estable de comunicaciones, que abarcara al menos un territorio nacional, se produjo en Suecia y Francia a principios del siglo XIX. Estos primeros sistemas se denominaban de telégrafo óptico y consistían en torres, similares a los molinos, con una serie de brazos o bien persianas. Estos brazos o persianas codificaban la información por sus distintas posiciones. Estas redes permanecieron hasta mediados del siglo XIX, cuando fueron sustituidas por el telégrafo. Cada torre, evidentemente, debía de estar a distancia visual de las siguientes; cada torre repetía la información hasta llegar a su destino.

El origen de las LAN inalámbricas se publicó en 1979, de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología. Las investigaciones siguieron adelante tanto con infrarrojos como con microondas. En mayo de 1985 el FCC3 (*Federal Communications Comission*) asignó las bandas IMS4 (*Industrial, Scientific and Medical*) 902-928 MHz, 2,400-2,483-5 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en *spread spectrum* (frecuencias altas).

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria, ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado.

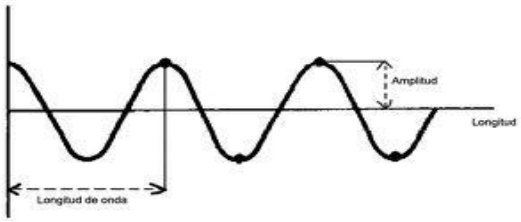
1.2. Fundamentos de las redes inalámbricas

Los fundamentos de las redes inalámbricas se encuentran en las ondas electromagnéticas, ya que estas tienen una característica en la forma de propagación de la radiación electromagnética a través del espacio. Estas ondas son producidas por el movimiento de una carga eléctrica. Son disturbios ondulatorios que se repiten en una distancia determinada, llamada longitud de onda. A diferencia de las ondas mecánicas, las ondas electromagnéticas no necesitan de un medio físico para propagarse, se propagan libremente por el aire alcanzando velocidades de 300,000 Km/s. Estas ondas electromagnéticas forman parte de nuestra vida, estando presentes en la luz, las microondas, los rayos-X y las transmisiones de radio y televisión etc.

- Componentes de una onda electromagnética**:**

La amplitud es la distancia máxima vertical entre la base y la onda. La forma de la variación de amplitud es llamada la envolvente de la onda; las unidades de la amplitud dependen de la onda. En las ondas electromagnéticas la amplitud del campo eléctrico esta expresado en metros.

Figura 1**. Componentes de una onda electromagnética**



Fuente: http://www.someprani.org/drupal-6.20/node/4. Consulta 22/08/10.

Período es el tiempo para un ciclo completo de oscilación de la onda.

Frecuencia se refiere a cuántos periodos por unidad de tiempo (segundos) se repite la onda y es medida en hertz.

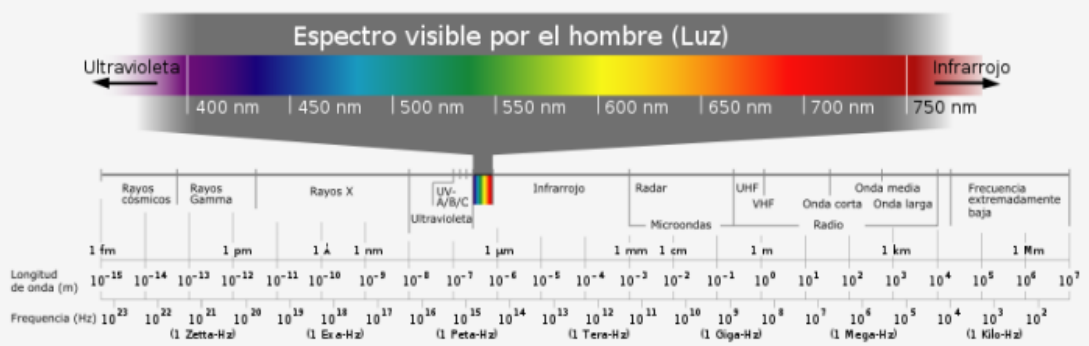
La frecuencia y el período de una onda son recíprocas entre sí y están representadas por la siguiente fórmula: f=1/T.

Longitud de onda es la distancia entre dos montes o valles seguidos. Suele medirse en metros.

Es importante la siguiente relación: a mayor frecuencia mayor longitud de onda, teniendo mayor alcance las de mayor longitud de onda ya que traspasan, atraviesan obstáculos, pero tienen bajas velocidades; por el contrario, menor frecuencia menor longitud de onda, mayor velocidad, menor alcance y no atraviesan obstáculos a grandes distancias.

El espectro electromagnético es la distribución energética del conjunto de las ondas electromagnéticas. Agrupadas bajo distintas denominaciones según su rango de frecuencias, aunque no existe un límite muy preciso para cada grupo. Los espectros se pueden observar mediante espectroscopios que además de permitir observarlo, permiten realizar medidas sobre este, como la longitud de onda, la frecuencia y la intensidad de la radiación.

Figura 2. **Espectro electromagnético**



Fuente: http://es.wikipedia.org/wiki/Espectro_electromagn%C3%A9tico. Consulta 22/08/10.

En el espectro electromagnético se puede encontrar:

Luz visible es la clase de energía electromagnetíca radiante, capaz de ser percibida por el ojo humano.

Infrarrojos es la radiación infrarroja, radiación térmica o radiación IR es un tipo de radiación electromagnética de mayor longitud de onda que la luz visible, pero menor que la de las microondas. La radiación infrarrojo es emitida por cualquier cuerpo cuya temperatura sea mayor que 0^{o} Kelvin, es decir -273^{o} C (cero absoluto).

Rayos Gamma, este tipo de radiación electromagnétíca producida generalmente por los elementos radiactivos o procesos subátomicos como la aniquilación de un par positron-electrón.

Radiación ultravioleta se denomina tambien radiación UV. Ya que su rango empieza de longitudes de onda más cortas, de lo que los humanos identificamos como el color violeta. La exposición constante a esta radiacion produce daños en la piel.

Rayos X designada a una radiación electromagnética, invisible, capaz de atravesar los cuerpos opacos y de impresionar las películas fotográficas.

1.2.1. Concepto de las redes inalámbricas

El término genérico "red" hace referencia a un conjunto de entidades (objetos, computadores, etc.) conectadas entre sí. Por lo tanto, una red permite que circulen elementos materiales o inmateriales entre estas entidades, según reglas bien definidas.

Una red inalámbrica es, como su nombre lo indica, una red en la que dos o más terminales (por ejemplo, ordenadores portátiles, agendas electrónicas, etc.) se pueden comunicar sin la necesidad de una conexión por cable.

Las redes inalámbricas son aquellas que se comunican por medio de transmisión no guiada (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas.

Las redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en

oficinas que se encuentren en varios pisos. No se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas. Estas ofrecen, velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps.

Los sistemas de cable de fibra óptica logran velocidades aún mayores, se espera que las redes inalámbricas alcancen velocidades de más de 10 Mbps. Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.

Las tecnologías de interconexión inalámbrica van desde redes de voz y datos globales, que permiten a los usuarios establecer conexiones inalámbricas a través de largas distancias, hasta las tecnologías de luz infrarroja y radiofrecuencia que están optimizadas para conexiones inalámbricas a distancias cortas. Entre los dispositivos comúnmente utilizados para la interconexión inalámbrica se encuentran los equipos portátiles, equipos de escritorio, asistentes digitales personales (PDA), teléfonos celulares, equipos con lápiz y localizadores. Las tecnologías inalámbricas tienen muchos usos prácticos. Por ejemplo, los usuarios de móviles pueden usar su teléfono celular para tener acceso al correo electrónico.

1.2.2. Bandas utilizadas

Las bandas más importantes con aplicaciones inalámbricas, del rango de frecuencias que abarcan las ondas de radio, son la VLF(comunicación en navegación y submarinos), LF (radio AM de onda larga), MF (radio AM de onda media), HF (radio AM de onda corta), VHF (radio FM y TV), HF (TV). Las bandas utilizadas son del espectro electromagnético y se pueden diversificar en otras.

Tabla I. **Tabla Espectro electromagnético**

Banda	Longitud de onda (m)	Frecuencia (Hz)	Energía (J)
Rayos gamma	< 10 pm	> 30,0 EHz	$> 20 \cdot 10^{-15}$ J
Rayos X	< 10 nm	> 30,0 PHz	$> 20 \cdot 10^{-18}$ J
Ultravioleta extremo	< 200 nm	> 1,5 PHz	$> 993 \cdot 10^{-21}$ J
Ultravioleta cercano	< 380 nm	> 789 THz	$> 523 \cdot 10^{-21}$ J
Luz Visible	< 780 nm	> 384 THz	$> 255 \cdot 10^{-21}$ J
Infrarrojo cercano	< 2,5 µm	> 120 THz	$> 79 \cdot 10^{-21}$ J
Infrarrojo medio	< 50 µm	> 6,00 THz	$> 4 \cdot 10^{-21}$ J
Infrarrojo lejano/submilimétrico	< 1 mm	> 300 GHz	$> 200 \cdot 10^{-24}$ J
Microondas	< 30 cm	> 1 GHz	$> 2 \cdot 10^{-24}$ J
Ultra Alta Frecuencia - Radio	< 1 m	> 300 MHz	$> 19.8 \cdot 10^{-26}$ J
Muy Alta Frecuencia - Radio	< 10 m	> 30 MHz	$> 19.8 \cdot 10^{-28}$ J
Onda Corta - Radio	< 180 m	> 1,7 MHz	$> 11.22 \cdot 10^{-28}$ J
Onda Media - Radio	< 650 m	> 650 kHz	$> 42.9 \cdot 10^{-29}$ J
Onda Larga - Radio	< 10 km	> 30 kHz	$> 19.8 \cdot 10^{-30}$ J
Muy Baja Frecuencia - Radio	> 10 km	< 30 kHz	$< 19.8 \cdot 10^{-30}$ J

Fuente: http://es.wikipedia.org/wiki/Espectro_electromagn%C3%A9tico. Consulta 23/08/10.

Radio Frecuencia es también denominado espectro de radiofrecuencias o RF, se aplica a la porción menos energética del espectro electromagnético, situada entre unos 3 Hz y unos 300 GHz. Las ondas electromagnéticas de esta región del espectro se pueden transmitir aplicando la corriente alterna originada en un generador a una antena.

Tabla II. **Bandas del espectro electromagnético**

Nombre	Abreviatura inglesa	Banda ITU	Frecuencias	Longitud de onda
			Inferior a 3 Hz	> 100.000 km
Extra baja frecuencia	ELF	1	3-30 Hz	100.000–10.000 km
Super baja frecuencia	SLF	2	30-300 Hz	10.000–1000 km
Ultra baja frecuencia	ULF	3	300–3000 Hz	1000–100 km
Muy baja frecuencia	VLF	4	3–30 kHz	100–10 km
Baja frecuencia	LF	5	30–300 kHz	10–1 km
Media frecuencia	MF	6	300–3000 kHz	1 km – 100 m
Alta frecuencia	HF	7	3–30 MHz	100–10 m
Muy alta frecuencia	VHF	8	30–300 MHz	10–1 m
Ultra alta frecuencia	UHF	9	300–3000 MHz	1 m – 100 mm
Super alta frecuencia	SHF	10	3-30 GHz	100-10 mm
Extra alta frecuencia	EHF	11	30-300 GHz	10–1 mm
			Por encima de los 300 GHz	< 1 mm

Fuente: http://es.wikipedia.org/wiki/Espectro_electromagn%C3%A9tico. Consulta 22/08/10.

Para el interés de la presente investigación, las bandas de radiofrecuencias utilizadas en redes inalámbricas son:

900 MHz su tasa fiable de transmisión es de 1 Mbps pero permite recorrer distancias mayores que las bandas 2.4 y 2.5 GHz. Llegando hasta

100 Km. Esta frecuencia no es útil para transmisiones de datos; en nuestro medio se utilizan para transmisión de voz.

2.4 GHz corresponde con la norma 802.11b y 802.11g: Wi-Fi, entrega una señal con una tasa máxima de 11 a 22 Mbps (en modo b), 54 a 108 Mbps (en modo g).

3.2 a 4.8 GHz: en esta frecuencia opera Wimax con velocidades de transferencia de 75 Mbps. Con alcance de hasta 48 Km. de radio.

5 GHz corresponde con la norma 802.11a; dispone de compatibilidad "hacia atrás", es decir, es una tecnología de banda dual para dar soporte a dispositivos de 2.4 GHz de la norma 802.11b y 802.11g; su tasa máxima de transmisión es de 108 Mbps.

1.2.3. Tecnologías inalámbricas

La tecnología sin cables permite conectar varias máquinas o dispositivos entre sí.

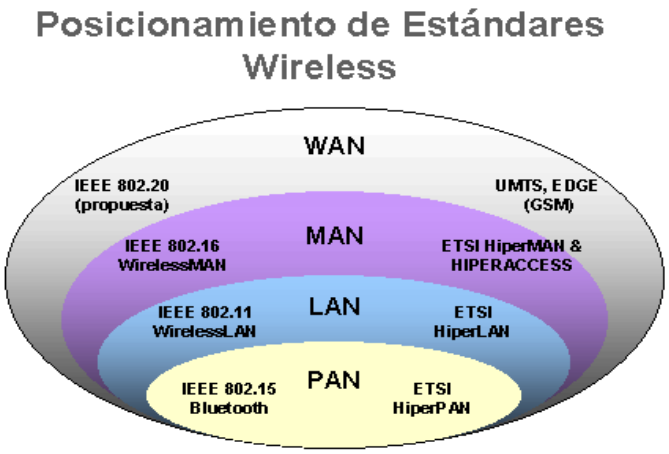
Las redes inalámbricas se clasifican en cuatro categorías según su alcance:

- WAN (*Worl Area Network*)
- MAN (*Metropolitan Area Network*)
- LAN (*Local Area Network*)
- PAN (*Personal Area Network*)

En la primera y segunda categoría WAN/MAN, se ubica a las redes que cubren desde decenas hasta miles de kilómetros. En la tercera categoría LAN, las redes que comprenden desde varios metros hasta decena de metros. Y en la última y nueva categoría PAN, son redes que comprenden desde 1 metro hasta 30 metros. En el caso de la categoría LAN, la norma IEEE 802.11 estableció en junio de 1997 el estándar para redes inalámbricas.

Una red de área local inalámbrica puede definirse como: una red de alcance local que tiene como medio de transmisión el aire. A este tipo de red inalámbrica se le conoce como Wi-Fi. El estándar 802.11 es muy similar al 802.3 (Ethernet). En este estándar se encuentran las especificaciones tanto físicas como a nivel MAC.

Figura 3. **Diferentes tecnologías inalámbricas**



Fuente**:** http://www.monografias.com/trabajos16/wimax/wimax.shtml. Consulta 26/08/10.

Tabla III. **Rango de frecuencias utilizadas por las tecnologías inalámbricas**

Tecnología	IrDA	Bluetooth	DS/SS	FH/SS	802.11b	802.11a	802.11g
Data Rate(bps)	9.6K-4M	3M	11M	1-2M	11M	54M	54M
Mobility	v	v	v	v	v	V	v
Range(m)	1-2	20	20-100 indoors	20-100	100	100	100
Frequency wav length	850-900nm	2.4GHz ISM	2.4GHz ISM	2.4GHz ISM	2.4GHz ISM	5 GHz U-NII	2.4GHz ISM
WEP	option	yes	option	option	option	yes	yes
802.11	x	x	v	v	v	v	v

Fuente: http://medtransnoguifabymarcos.blogspot.com/2010_05_01_archive,html. Consulta 26/08/10.

- Diferentes tipos de tecnologías inalámbricas

Infrarrojo en esta forma especial de transmisión de radio, un haz enfocado de luz en el espectro de frecuencia infrarrojo, medido en Terahertz o billones de hertzios (ciclos por segundo) se modula con información y se envía de un transmisor a un receptor a una distancia relativamente corta. La radiación infrarroja (IR) es la misma tecnología usada para controlar un televisor con un mando a distancia.

Estas redes son muy limitadas debido a su corto alcance; necesitan visión sin obstáculos entre los dispositivos que se comunican y su baja velocidad (hasta 115 Kbps, 4Mbps en el IRDA 1.1). Se encuentran principalmente en ordenadores portátiles, PDAs (agendas electrónicas personales), teléfonos móviles y algunas impresoras.

El rojo es el color de longitud de onda más larga de la luz visible, comprendida entre 700 nanómetros y un milímetro. Los infrarrojos son a menudo subdivididos en infrarrojos cortos (0.7-5 µm). Sin embargo, esta clasificación no es precisa porque en cada área de su utilización, se tiene una idea de los límites de los diferentes tipos.

Existe una organización denominada IRDA (*infrared data association*), fundada para crear las normas internacionales para el hardware y el software usado en enlaces de comunicación por rayos infrarrojos. La IRDA publica varios estándares, pero el estándar original de IRDA, conocida como IRDA 1.0, permitía la transferencia de datos a una velocidad de hasta 115.2 Kbps en un radio de acción de 1 metro y un ángulo de 15 grados. En 1996 se adoptó una extensión estándar, el IRDA 1.1 que permitía transferencias 35 veces superiores al IRDA. En el estándar IRDA-1.1, el máximo tamaño de datos que se puede transmitir es de 2 Mbps y la tasa máxima de transmisión es de 4 Mbps. La radiación infrarroja, también puede usarse para interconexiones un tanto más largas y es una posibilidad para las interconexiones en redes de área local (LAN), la distancia efectiva máxima es algo menor a los ocho kilómetros y el máximo ancho de banda proyectado es de 16 Mbps dado que la radiación infrarroja es transmisión en línea visual (ambos dispositivos deben de poder verse entre sí), sensible a la niebla y otras condiciones atmosféricas.

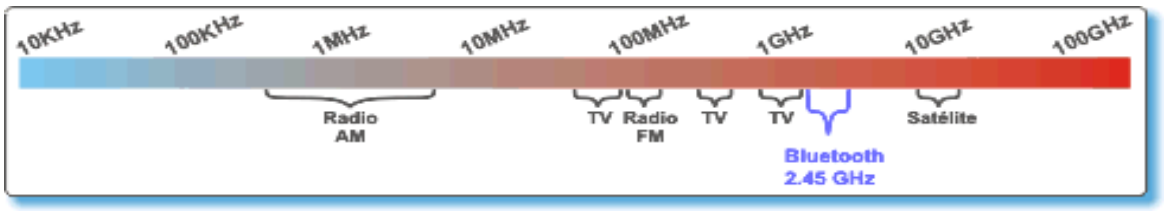
Bluetooth es una tecnología orientada a la conectividad inalámbrica entre dispositivos; estos pueden ser computadoras de escritorio, PDAs, teléfonos móviles, auriculares, manos libres (*hands free)*, inclusive impresoras y en fin las posibilidades pueden considerarse muchas. Esta tecnología revoluciona el mercado de la conectividad personal, proveyendo ínterconectividad entre cualquier tipo de dispositivo que cumpla con las especificaciones inalámbricas Bluetooth. Además este es un estándar libre, lo

que simplifica su uso para diseñar y sacar al mercado nuevos productos innovadores que se beneficien de la conectividad inalámbrica.

Los dispositivos de radio que soportan la tecnología no requieren de licencia y deben tener un espectro de 2.4 GHz para asegurar la compatibilidad en todo el mundo. Cada dispositivo Bluetooth está equipado con un *transceiver* que transmite y recibe a una frecuencia de 2.4 GHz, la cual está disponible en todo el mundo. Las conexiones son una a una, con un rango máximo de 10 metros. Pero si se utilizan repetidores se puede alcanzar hasta 100 metros, con algo de distorsión.

El ancho de banda que se alcanza entre los dispositivos *bluetooth* es 1 a 3 Mbps, pero está proyectada para alcanzar 53 a 480 Mbps. con alcances de 1 a 100 metros.

Figura 4. **Localidad de radiofrecuencias internacionales**

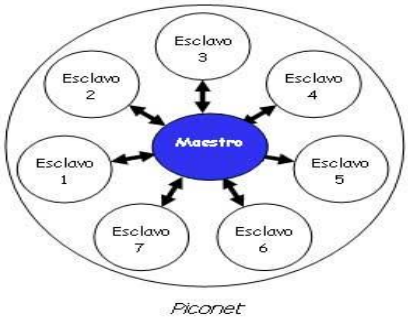


Fuente: http://www.monografias.com/trabajos16/wimax/wimax.shtml. Consulta 26/08/10.

Los dispositivos pueden comunicarse entre sí e intercambiar datos de una forma transparente para el usuario. Hasta 8 usuarios pueden formar parte de una piconet y pueden coexistir hasta 10 piconets en la misma área de

cobertura. En una piconet habrá siempre un máster y los demás serán esclavos.

Figura 5. **Diagrama de un piconet**



Fuente: http://www.monografias.com/trabajos16/wimax/piconet.shtml. Consulta 26/08/10.

GSM, GPRS y UMTS**:** las tecnologías inalámbricas han tenido mucho auge y desarrollo en estos últimos años. Una de las tecnologías que ha tenido un gran desarrollo ha sido la telefonía celular.

A pesar de que la telefonía celular fue concebida estrictamente para la voz, la tecnología celular hoy es capaz de brindar otro tipo de servicio, como: datos, audio y vídeo, con algunas limitaciones.

La tecnología celular tuvo gran aceptación, por lo que a los pocos años de implantarse se empezó a saturar el servicio. En este sentido, hubo la necesidad de desarrollar e implementar otras formas de acceso múltiple al canal y transformar los sistemas analógicos a digitales, con el objeto de dar cabida a más usuarios. Para separar una etapa de la otra, la telefonía celular

se ha caracterizado por contar con diferentes generaciones. A continuación se describe una de ellas.

La primera generación (1G) de la telefonía móvil hizo su aparición en 1979 y se caracterizó por ser analógica y estrictamente para voz. Tenían baja velocidad (2400 bauds). En cuanto a la transferencia entre celdas, era muy imprecisa ya que contaba con una baja capacidad (basadas en FDMA, *Frequency Division Multiple Access*) y además la seguridad no existía. La tecnología predominante de esta generación es AMPS (*Advanced Mobile Phone System*).

La segunda generación (2G) arribó hasta 1990 y a diferencia de la primera se caracterizó por ser digital. El sistema 2G utiliza protocolos de codificación más sofisticados y se emplea en los sistemas de telefonía celular actuales. Las tecnologías predominantes son GSM (*Global System por mobile communications)*; IS-136 (conocido también como TIAIEIAI36 o ANSI-136) y CDMA (*Code Division Multiple Access*) y PDC (*personal Digital communications*), este utilizado en Japón.

Los protocolos utilizados en los sistemas 2G soportan velocidades de información más altas por voz, pero limitados en comunicación de datos. Se puede ofrecer servicios auxiliares, como datos, fax y 8MS (*Short Massage Service*). La mayoría de los protocolos de 2G ofrecen diferentes niveles de encriptación.

La generación 2.5G apareció ofreciendo características extendidas, ya que cuenta con más capacidades adicionales que los sistemas 2G, como GPRS (*General Packet Radio System*), HSCSD (*High Speed Circuit Switched*), EDGE (*Enhanced Data Rates for Global Evolution*), IS-1368 e IS-95Bm entre

otros. Por último se tiene en estos momentos la tercera generación (3G), que se caracteriza por contener a la convergencia de voz y datos con acceso inalámbrico a internet; en otras palabras, es apta para aplicaciones multimedia y altas transmisiones de datos.

Los protocolos empleados en los sistemas 3G soportan altas velocidades de información y están enfocados para aplicaciones mas allá de la voz como audio (mp3), video en movimiento, video conferencias y acceso rápido a internet, solo por nombrar algunos.

Los sistemas de telefonía digital están basados en dos tecnologías distintas: TDMA (*Time Division Multiple Access*) y CDMA (*Code Division Multiple Access*). Es decir por división de tiempos y por códigos. El sistema de telefonía GSM está basado en TDMA. Una vez saturada la frecuencia original de 900 MHz se implantó el estándar GSM de segunda generación en la banda del 1800 MHz. Con el aumento de usuarios, las bandas se quedan cortas. Las frecuencias de transmisión son un bien escaso. No se puede asignar a cada usuario una frecuencia diferente, han de compartirlas. Con TMDA se utiliza una sola frecuencia, que se divide en casillas de tiempo, las llamadas se reparten entre las casillas.

En el sistema CDMA las llamadas se reparten entre varias frecuencias. En la actualidad el sistema CDMA ha demostrado ser el mejor, teniendo mayor capacidad, calidad de sonido y de transmisión de datos que TDMA, y por tanto, que GSM. El sistema UMTS utiliza CDMA. La tecnología UMTS (*Universal Mobile Telecommunications System*) es el sistema de telecomunicaciones móviles de tercera generación, que evoluciona desde GSM pasando por GPRS.

El principal avance es la tecnología WCDMA (*Wide Code Division Multiple Access*), a diferencia de GSM y GPRS que utilizan una mezcla de FDMA (*Frecuency Division Multiple Access*) y TDMA (*Time Division, Multiple Access*). La principal ventaja de WCDMA consiste en que la señal va dando saltos por todo el espectro de frecuencias, y la sincronización de esos saltos solo la conocen emisor y receptor.

Esta original forma de modulación tiene numerosas ventajas como altas velocidades de transmisión de hasta 2 Mbps al usar todo el espectro, alta seguridad y confidencialidad debido a que la señal va saltando de unas frecuencias a otras, tiene acceso múltiple de eficacia mientras no coincidan las secuencias de saltos, alta resistencia a las interferencias, posibilidad de trabajar con dos antenas simultáneamente debido a que siempre se usa todo el espectro y lo importante es la secuencia de salto, lo que facilita el handover (proceso de traspaso de la señal de una a antena a otra), donde GSM falla mucho. UTMS ofrece otra serie de ventajas como roaming y cobertura a nivel mundial ya sea vía enlace radio terrestre o vía satélite, y está altamente estandarizado con una interfaz única para cualquier red.

Wimax interoperabilidad mundial para el acceso por microondas, es considerado hoy en día como el futuro de las redes Wi-Fi. Es el nombre comercial del estándar 802.16, un protocolo de transmisión de datos inalámbrico que va un paso más allá de Wi-Fi. Wimax promete una velocidad de 70 megabits por segundo (siete veces el ancho de banda de Wi-Fi), que con una sola antena cubrirá un área de 50 kilómetros a la redonda, frente a los 300 metros de Wi-Fi. Es decir, Wimax será a una ciudad entera lo que Wi-Fi es para los hogares: conexión a Internet a alta velocidad sin cables.

El nuevo estándar está respaldado por importantes fabricantes de equipos y proveedores de servicios. El Wimax Forum está formado por más de 230 miembros entre los que destacan nombres como Intel, Nokia, Siemens, *Motorola, Samsung o Fujitsu*, y donde no faltan operadores de telefonía como Deutsche Telekom, France Telecom, Telecom Italia o Euskaltel. Intel es el gran impulsor de esta nueva tecnología; ya produce los primeros *chips* Wimax que los fabricantes venderán integrados en sus equipos en años futuros.

El estándar Wimax establece el uso de canales de 25 MHz en el rango de frecuencias entre 10 y 66 GHz. Asimismo, se está en proceso de definir los canales en el rango de frecuencias entre los 2 y 11 GHz, actualmente, las frecuencias usadas en nuestro país son las de 3.2 y 4.8 GHz.

El primer rango de frecuencias requiere una línea de vista directa entre antena y antena, por lo que se planea usarla para la transmisión entre antenas y no para distribución a usuarios finales. El segundo rango no requiere una línea de vista directa a la antena, por lo que puede ser usado para distribuir contenido a los usuarios finales. Una desventaja de las frecuencias más bajas radica en que la velocidad máxima se ve disminuida por defecto de los protocolos de corrección de errores. Sin embargo, la velocidad máxima compartida es de alrededor de 100 Mbps, lo que significa que tienen la misma velocidad que la red local (LAN) de cualquier compañía.

Debido a que esta es una velocidad compartida, la velocidad real observada dependerá del número de usuarios conectados simultáneamente y de los requerimientos de ancho de banda de cada usuario. Es por eso que Wimax está dado a reemplazar o a competir directamente con el internet por cable, así como con el ADSL (*Asymmetric Digital Subscriber Line*). A diferencia del ADSL, la torre de distribución de Wimax se puede encontrar ubicada a

kilómetros del usuario, haciendo que sea innecesario tener múltiples estaciones para distribuir la señal. Una misma torre puede manejar múltiples antenas en diferentes canales cubriendo a múltiples usuarios con necesidades de ancho de banda diferente.

Wimax ofrece flexibilidad en la localización de las torres, gran alcance, un ancho de banda de hasta 50 veces el proporcionado por 3G, así como una reducción de costos fijos en cableado y antenas repetidoras. Todo esto hace posible pensar que Wimax puede ayudar a Latinoamérica a alcanzar la adopción de banda ancha de los países desarrollados a una fracción de costo. La nueva tecnología, conocida como Wimax, podría llevar Internet a millones de hogares y empresas donde no llegan ni el cable ni líneas de suscripción digital (DSL, por sus siglas en inglés). La tecnología puede cubrir un área de 48 kilómetros, con capacidad para transmitir datos a 75 Mbps.

Wimax utiliza antenas que pueden recibir la señal en casas y oficinas. Allí, un *router* tomaría la señal Wimax y daría conexiones de Internet. Finalmente, las computadoras y los móviles podrán conectarse directamente a la señal Wimax. Actualmente Wimax está en sus etapas iníciales, y es solo una de varias soluciones de banda ancha inalámbrica rivales ofrecidas por las grandes compañías tecnológicas.

El estándar 802.16 puede alcanzar una velocidad de comunicación de más de 100 Mbit/s en un canal con un ancho de banda de 28 MHz (en la banda de 10 a 66 GHz), mientras que el 802.16a puede llegar a los 70 Mbit/s, operando en un rango de frecuencias más bajo (<11 GHz). Es un claro competidor de LMDS.

Tabla IV. **Comparaciones Wimax frente a otras tecnologías**

	WiMAX - 802.16	Wi-Fi -802.11	Mobile-Fi - 802.20	UMTS y cdma2000
Velocidad	124 Mbit/s	11-54 Mbit/s	16 Mbit/s	2 Mbit/s
Cobertura	40-70 km	300 m	20 km	10 km
Licencia	Si/No	No	Si	Si
Ventajas	Velocidad y Alcance	Velocidad y Precio	Velocidad y Movilidad	Rango y Movilidad
Desventajas	Interferencias	Bajo alcance	Precio alto	Lento y caro

Fuente: http://www.monografias.com/trabajos16/wimax/wimax.html. Consulta 30/08/10.

Estas velocidades tan elevadas se consiguen gracias a utilizar la modulación OFDM (*Orthogonal Frequency División Multiplexing*) con 256 subportadoras, la cual puede ser implementada de diferentes formas, según cada operador, siendo la variante empleada de OFDM, un factor diferenciador del servicio ofrecido.

Otra característica de Wimax es que soporta las llamadas antenas inteligentes (*smart* antenas), propias de las redes celulares de 3G, lo cual mejora la eficiencia espectral, llegando a conseguir 5 bps/Hz, el doble que 802.11a. Estas antenas inteligentes emiten un haz muy estrecho que se puede ir moviendo, electrónicamente, para enfocar siempre al receptor, con lo que se evitan las interferencias entre canales adyacentes y se consume menos potencia al ser un haz más concentrado.

También se contempla la posibilidad de formar redes malladas (*mesh networks*) para que los distintos usuarios se puedan comunicar entres sí, sin necesidad de tener visión directa entre ellos. Ello permite, por ejemplo, la

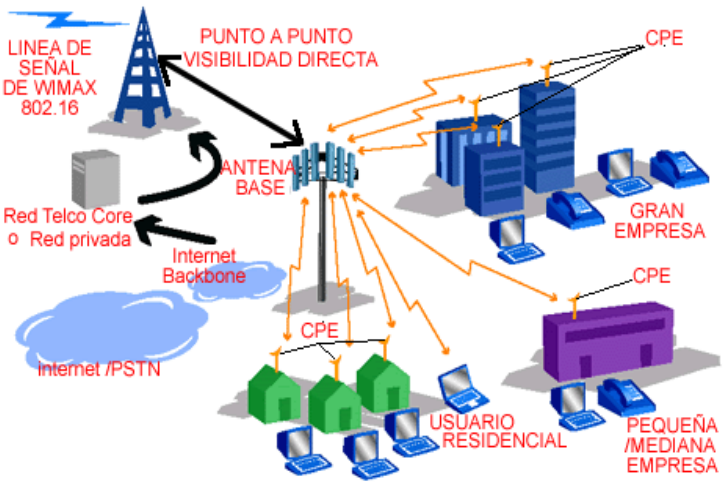
comunicación entre una comunidad de usuarios dispersos a un coste muy bajo y con una gran seguridad al disponerse de rutas alternativas entre ellos.

En cuanto a seguridad, incluye medidas para la autenticación de usuarios y la encriptación de los datos mediante los algoritmos Triple DES. (128 bits) y RSA (1.024 bits).

Una de las principales limitaciones en los enlaces a larga distancia vía radio es la limitación de potencia, para prever interferencias con otros sistemas, y el alto consumo de batería que se requiere. Sin embargo, los más recientes avances en los procesadores digitales de señal hacen que señales muy débiles (que llegan con poca potencia al receptor) puedan ser interpretadas sin errores, un hecho del que se aprovecha Wimax. Con los avances que se logren en el diseño de baterías podrá haber terminales móviles Wimax, compitiendo con los tradicionales de GSM, GPRS y de UMTS.

Componentes de los sistemas Wimax: la arquitectura de la tecnología Wimax está constituida por 2 bloques principales, la estación base y el receptor Wimax utilizado por los usuarios. Este último generalmente es denominado bajo la sigla CPE (*Customer Premise Equipment*). Se consideran sólo estos bloques ya que los estándares 802.16 no especifican alguna tecnología en especial para la conexión con el núcleo de la red, no es parte del sistema Wimax.

Figura 6. **Componentes sistemas Wimax**



Fuente: http://observatorio.cnice.mec.es. Consulta 30/08/10.

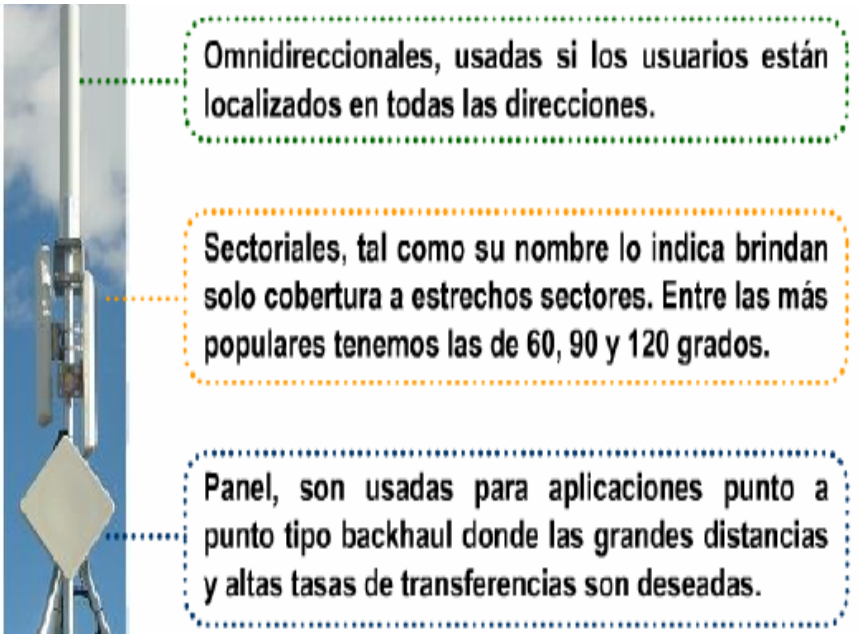
BS Estación Base Wimax la estación base Wimax corresponde a los equipos, que generalmente son ubicados en casetas, con los resguardos de clima y energía necesarios, en la mayoría de los equipos de telecomunicaciones.

Una estación base teóricamente puede cubrir hasta 50 kilómetros, pero en la práctica se consideran alrededor de 10 kilómetros. Una estación base también se denomina torre Wimax. Pero una estación base no necesariamente tiene que residir en una torre, también puede estar localizada en edificios terrazas o estructuras elevadas, tales como torres para tanques de agua.

Una estación base (BS) puede conectarse directamente a un proveedor de servicios de Internet (ISP) utilizando una conexión alámbrica de alta velocidad (por ejemplo una línea T3) o también puede conectarse al sistema mediante otra BS o mediante un enlace microondas. Así como las antenas de

las estaciones base de las redes celulares, las antenas Wimax pueden ser omnidireccionales o direccionales.

Figura 7. **Antenas de los sistemas Wimax**

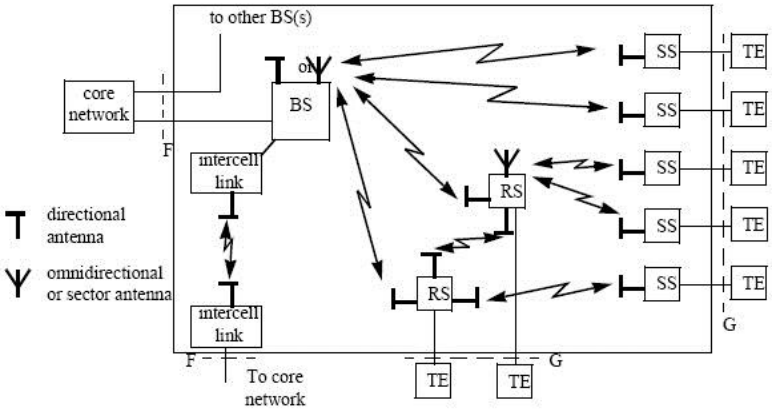


Fuente: www.ola.com.co/formas/13140/Wi-Max-Orbitel.pdf. Consulta 30/08/10.

CPE Wimax el equipo Local del cliente – CPE, consiste en una unidad localizada en cada emplazamiento del usuario; en cada hogar para el caso residencial y en cada oficina para el caso empresarial. Dicha unidad constituye el último segmento de la red Wimax pues es la que permite todo el proceso de transferencia de información entre el usuario y la estación base – BS. El CPE, podría ser una pequeña caja con una antena, una tarjeta PCMCIA o PCI, o un módulo USB o incluso un chip integrado a un equipo portátil. Algunos ejemplos según el tipo de servicio.

Arquitectura del sistema los sistemas FBWA (*Fixed Broadband Wireless Access*) a menudo emplean arquitecturas del tipo multipunto (MP). La arquitectura MP incluye punto-multipunto (PMP) y *mesh* (Multi Punto a Multi Punto). El grupo de trabajo IEEE 802.16 ha desarrollado estándares en los cuales se especifican la interfaz de aire para los sistemas PMP y *mesh*. Para la interconexión entre estaciones base se puede utilizar enlaces inalámbricos, de fibra o par de cobre.

Figura 8. **Diagrama Sistema Internet Banda Ancha Inalámbrica**



Fuente: Marco Antonio Muñoz. Metodologías, criterios y herramientas para la planificación de redes inalámbricas. Santiago de Chile: Universidad de Chile. 2007, p.13. Consulta 03/09/10.

En un sistema PMP, los RSs son generalmente usados para mejorar la cobertura en lugares donde no se tiene línea de vista (LOS), dentro del área normal de cobertura o alternativamente para extender la cobertura de una BS en particular.

Una estación repetidora retransmite la información desde la BS a uno o más SSs. También puede proporcionar conexión a SS locales.

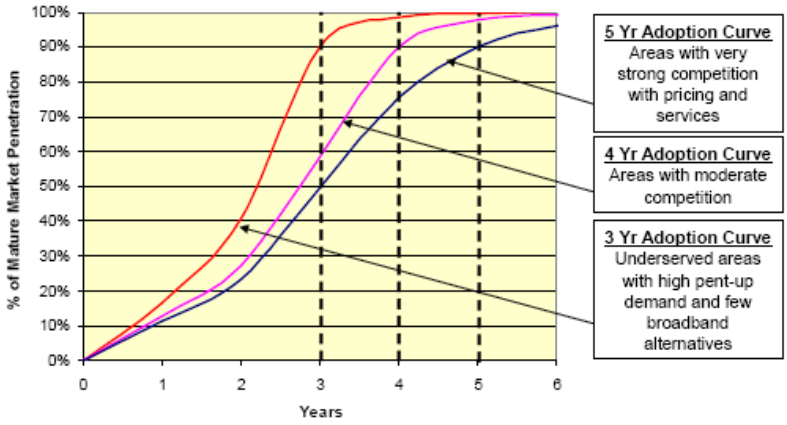
Modelo económico Wimax: un modelo económico para una red Wimax debe tener en cuenta los siguientes parámetros:

Demografía juega un papel determinante en la viabilidad de un negocio en torno a cualquier red de telecomunicaciones. Tradicionalmente las regiones son clasificadas en urbanas, suburbanas y rurales. Cada una de éstas con características diferenciales en cuanto a la capacidad económica, densidad poblacional y la tasa de penetración de los servicios de telecomunicaciones.

Servicios se refiere a los tipos de servicios ofrecidos durante la vigencia del negocio, generalmente pueden tenerse servicios de tipo residencial, comercial, PYMES, entre otros. Las proyecciones que se hagan en este aspecto, tienen radical importancia en la viabilidad económica del proyecto.

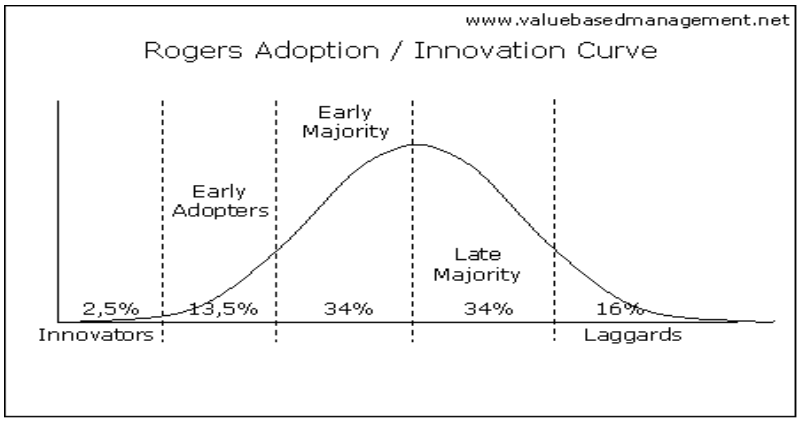
Rata de adopción del mercado generalmente toma un tiempo para que los consumidores adopten una nueva tecnología o servicio. Para los consumidores la percepción que se tiene de nuevos productos varía de acuerdo con múltiples factores, sin embargo para una tecnología como Wimax se espera que la aceptación sea muy favorable debido a que se tienen servicios similares como el Wi-Fi y la telefonía celular, y por ende se confía en que se tendrá una aceptación equivalente. Como puede observarse en la siguiente gráfica se proponen diferentes curvas para prever la aceptación por parte del mercado de las nuevas redes Wimax.

Figura 9. **Curvas de Porcentaje del Mercado de una red Wimax**



Fuente**:** http://www.hkwtia.org/wtia/WiMAX%20-%20Business%20Case%20Rev2%2031.pdf. Consulta 03/09/10.

Figura 10. **Curva de Adopción de tecnologías nuevas**



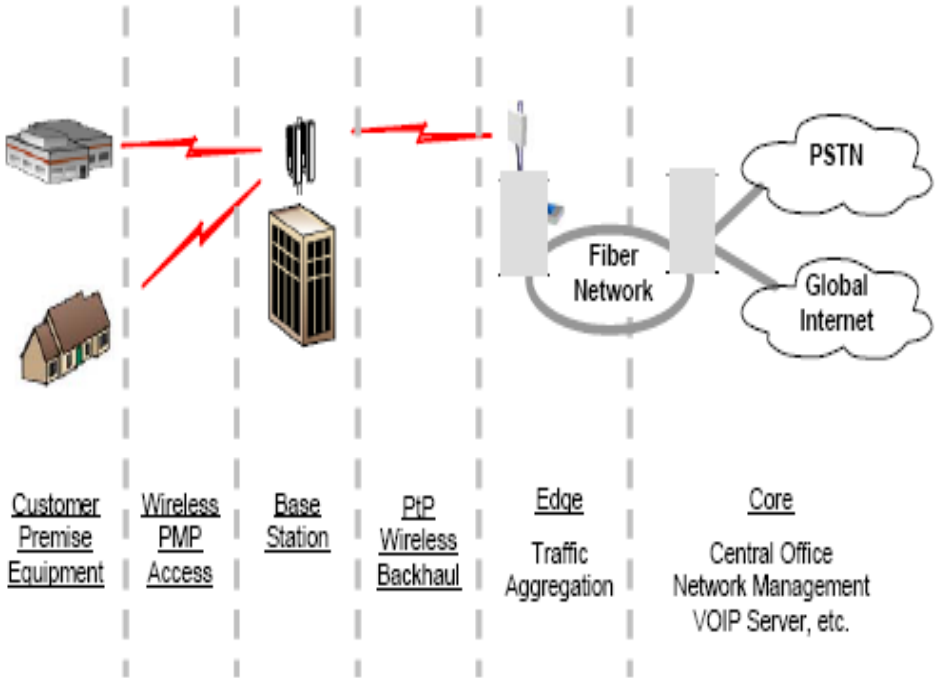
Fuente: www.valuebasedmanagemen.net. Consulta 03/09/10.

Estaciones base (*Base Station*), Interfaces y elementos de red, el análisis económico de un proyecto Wimax parte de determinar los requerimientos de equipos de radio (estaciones base), espacios físicos para montar la

infraestructura, y de gestión de la red, los cuales están condicionados a las inversiones, cobertura geográfica y tasas de penetración que se tengan presupuestadas en el tiempo de desarrollo del proyecto.

Generalmente, es necesario llevar a cabo obras de ingeniería para soportar la infraestructura. Y en algunos casos es necesario tender redes de fibra para realizar los *Backhaul* entre las estaciones base.

Figura 11. **Arquitectura de inversiones de capital en la red Wimax**



Fuente: http://www.hkwtia.org/wtia/WiMAX%20-%20Business%20Case%20Rev2%2031.pdf. Consulta 07/09/10.

A continuación se resumen las principales inversiones en esta materia, que son necesarias considerar en un proyecto Wimax:

Tabla V. **Resumen costo equipos para una red Wimax**

Descripción	Costo	Comentarios
Equipos Wimax	USD 35.000	Costo de las estaciones Base de la red Wimax
Enlaces *Backhaul*	USD 25.000	Realiza la interconexión entre estaciones Base
Equipos de Red	USD 100.000	Incluye los elementos necesarios para realizar la administración e interconexión de la red con otras.
Licenciamiento del Espectro	USD 0	Gastos que deben pagar los operadores por las licencias que les permitan prestar el servicio Wimax
Obras civiles, e instalación de Estaciones Base	USD 20.000	Incluye la adquisición de terrenos y las adecuaciones que se deben realizar por Estación Base, necesarias para dar funcionamiento a la red

Fuente: http://www.hkwtia.org/wtia/WiMAX%20-%20Business%20Case%20Rev2%2031.pdf. Consulta 10/09/10.

La primera empresa en instalar Wimax en Guatemala (2005) fue Telgua (América Móvil).

Wi-Fi es una aplicación de la comunicación inalámbrica en una red de área local, lo cual ha venido a denominarse WLNA; dentro de esta se hará un enfoque en el estudio de Wi-Fi.

Las redes WLAN (*Wireless LAN*) utilizan ondas electromagnéticas de radio para enlazar (mediante un adaptador) los equipos conectados a la red, en lugar de los cables coaxiales o, de fibra óptica que se utilizan en las LAN convencionales cableadas (*Ethernet, Teken Ring*).

La función principal de este tipo de redes es proporcionar conectividad y acceso a las tradicionales redes cableadas, como si de una extensión de estas últimas se tratara, pero con la flexibilidad y movilidad que ofrecen las comunicaciones inalámbricas. El momento decisivo para la consolidación de estos sistemas fue la conclusión del estándar IEEE 802.11 en junio del 1997. En este estándar se encuentran las especificaciones tanto físicas como a nivel MAC que hay que tener en cuenta a la hora de implementar una red de área local inalámbrica. Otro de los estándares definidos y que trabajan en este mismo sentido, es el ETSI *HIPERLAN*.

Los primeros sistemas LAN inalámbricos datan de 1986. Eran lentos y toda la infraestructura de radio tenía que ser suministrada por el mismo fabricante. En 1993 aparecieron sistemas de mayor capacidad que funcionaban en la banda de 2.4 GHz, IEEE aprobó la norma 802.11 en junio de 1997. En ella se especificaba el funcionamiento de LANs inalámbricas de 1 y 2 Mbps en la banda de 2.4 GHz (Wi-Fi) y mediante infrarrojos.

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (*Ethernet*). Esto quiere decir que en lo único que se diferencia una red Wi-Fi de una red *Ethernet* es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico; por lo tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (*Ethernet*).

En 1998 aparecieron en el mercado los primeros sistemas que funcionaban a 11 Mbps, siguiendo el borrador de la norma 802.11 b, que fue finalmente aprobada en septiembre de 1999, junto con la 802.11 a, que especifica el funcionamiento en la banda de 5 GHz a velocidades de hasta 54 Mbps.

En el 2001 destaca el 802.11e, que especifica mecanismos de calidad de servicio en WLANs, y en el 2003 el 802.11g, que describe el funcionamiento de velocidades de hasta 54 Mbps en la banda de 2.4 GHz.

Nokia y *Symbol Technologies* crearon en 1999 una asociación conocida como WECA (*Wireless Ethernet Compatibility Alliance*, alianza de compatibilidad *Ethernet* Inalámbrica). Esta asociación pasó a denominarse Wi-Fi Alliance en 2003. El objetivo de la misma fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos. De esta forma, en abril de 2000 WECA certifica la interoperabilidad de equipos según la norma IEEE 802.11b bajo la marca Wi-Fi (el término no tiene un significado en sí).

Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problema, independientemente del fabricante de cada uno de ellos. Se puede obtener un listado completo de equipos que tienen la certificación Wi-Fi en *Alliance certified products*. En el año 2002 la asociación WECA estaba formada ya por casi 150 miembros.

- Variaciones de la norma 802.11

La norma 802.11 ha sufrido diferentes extensiones sobre la norma para obtener modificaciones y mejoras. De esta manera, se tienen las siguientes especificaciones: 802.11 a.

El estándar 802.11 a: fue la primera aproximación a las redes Wi-Fi y llega a alcanzar velocidades de hasta 54 Mbps. Esta variante opera dentro del

rango de los 5 GHz. Inicialmente se soportan hasta 64 usuarios por punto de acceso.

Sus principales ventajas son su velocidad, la base instalada de dispositivos de este tipo, y la ausencia de interferencias en la misma.

Sus principales desventajas son su incompatibilidad con los estándares 802.11b y g, la no incorporación a la misma de QoS (posibilidades de asegurar calidad de servicio, lo que en principio impediría ofrecer transmisión de voz y contenidos multimedia *online*), el hecho de no está disponible en Europa prácticamente se descarta de todas las posibilidades de elección para instalaciones en este continente.

802.11b este estándar es la segunda aproximación de redes Wi-Fi, alcanza una velocidad de 11 Mbps (22 Mbps en modo turbo). Opera dentro de las frecuencias de los 2.4 GHz.

Inicialmente se soportan hasta 32 usuarios por AP. Este estándar no tiene varios de los inconvenientes que tiene el 802.11a, como la falta de QoS, además de otros problemas como la masificación de la frecuencia en la que transmite y recibe, pues a los 2.4 GHz funcionan teléfonos inalámbricos, teclados y ratones inalámbricos, hornos microondas, dispositivos Bluetooth, lo cual puede provocar interferencias. En el lado positivo está su rápida adopción por parte de una gran comunidad de usuarios, debido principalmente a unos muy bajos precios de sus dispositivos, la gratuidad de la banda que usa y su disponibilidad gratuita alrededor de todo el mundo.

802.11g este estándar es la tercera aproximación a las redes Wi-fi, se basa en la compatibilidad con los dispositivos 802.11b y en el ofrecer unas velocidades de hasta 54 Mbps (108 Mbps en modo turbo).

Las unidades 802.11g podrán trabajar también a velocidades de 11 Mbs, de modo que los dispositivos 802.11b y 802.11g pueden coexistir bajo la misma red. Ambos estándares aplicarán para la banda de frecuencia de 2.4 GHz. Las ventajas de las que dispone son las mismas que las del 802.11b, además de su mayor velocidad.

802.11n, es la cuarta generación en los sistemas inalámbricos Wi-fi, compatible en gran parte con los estándares anteriores es el 802.11n, trabaja en la frecuencia de 2.4 y 5 GHz. La mejora respecto de los anteriores en el uso de varias antenas de transmisión y recepción (MIMO=Multiple *IN*, Multiple *Out*) se refiere a las características de la señal pues permite anchos de banda de 300 Mbps propuesto a 540 Mbps; una característica importante es la capacidad de poder usar una antena exclusivamente para transmitir y otra para recibir, a diferencia de sus predecesoras que usaban la misma antena para ambas acciones, debiendo el transmisor cambiar a modo receptor cada cierto tiempo o usar filtros adicionales. Esto hace que el 802.11n sea ideal para altas velocidades.

El gran éxito de Wi-Fi es que utiliza frecuencias de uso libre, es decir no es necesario pedir autorización o algún permiso para utilizarlas. Aunque la normatividad acerca de la administración del espectro varía de país a país. La desventaja de utilizar este tipo de banda de frecuencia es que las comunicaciones son propensas a interferencias y errores de transmisión. Estos errores ocasionan que sean reenviados una u otra vez los paquetes de información. Una razón de error del 50 % ocasiona que se reduzca la velocidad

eficaz real (*throughput*) dos terceras partes, aproximadamente. Por eso la velocidad máxima especificada teóricamente no es la realidad.

La velocidad real en las Wi-Fi está muy por debajo que la especificada por las normas, trabajando a largas distancias; ya que depende de diversos factores tales como el ambiente de interferencias, la distancia o área de cobertura, la potencia de transmisión, el tipo de modulación empleada, etc. La mayoría de las redes 802.11 g, pueden alcanzar oficialmente distancias hasta de 200 metros interiores. Con una mayor potencia se pueden extender esa longitud, aunque en interiores al limitarse la potencia de transmisión; paredes y otros objetos pueden interferir la señal. En la realidad una Wi-Fi en ambientes exteriores en comunicación punto a punto puede alcanzar varios kilómetros mientras exista línea de vista y libre de interferencia.

En este sentido, el objetivo fundamental de las redes inalámbricas locales es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas.

1.3. Tipos de modulaciones

Modulación, es un efecto no lineal en el cual varias señales interactúan unas con otras para producir nuevas señales con frecuencias que no estaban presentes en las señales originales. La modulación nace de la necesidad de transportar una información a través de un canal de comunicación a la mayor distancia y menor costo posible. Este es un proceso mediante el cual dicha información (onda moduladora) se inserta a un soporte de transmisión.

Son tres los parámetros de la señal portadora afectados por la señal de información o señal moduladora: la amplitud, la frecuencia y la fase.

Son múltiples las razones para modular, facilita la propagación de la señal, ordena el espectro radioeléctrico, optimiza el ancho de banda, evita interferencias entre canales, protege de la degradación del ruido y define la calidad de la información.

1.3.1. Modulación de amplitud ASK

Una portadora puede modularse de diferentes modos dependiendo del parámetro de la misma sobre el que actúe. Se modula en amplitud una onda que se llamará portadora, cuando la distancia que existe entre el punto de la misma en el que la onda vale cero y los puntos en que toma el valor máximo ó mínimo, se altera.

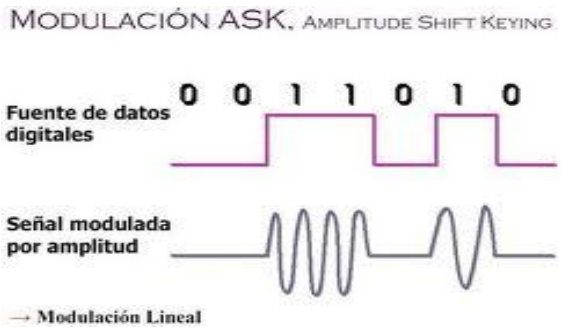
Es la amplitud (intensidad) de la información a transmitir la que varía la amplitud de la onda portadora. Y resulta que, al añadir esta información se obtiene tres frecuencias: la frecuencia de la portadora fp; la frecuencia suma de la portadora y la información fp + fm y la frecuencia diferencia de la portadora y la información fp – fm.

El análisis lleva a pensar que, como normalmente la información no la compone la única onda, sino varias dentro de una banda, sería necesario hacer uso de un gran ancho de banda para transmitir una información cuyas frecuencias estuvieran comprendidas entre los 20 Hz y 20 000 Hz (límites de la banda de frecuencias audibles por el oído humano) con buena calidad.

Por otro lado, como el ancho de banda permitido para una emisora está limitado, este tipo de modulación se aplica a usos que no requieren gran cantidad de sonido o en los que la información sea de frecuencias próximas entre sí.

Otra característica de la modulación de amplitud es que, en su recepción, los desvanecimientos de señal no provocan demasiado ruido, por lo que es usada en algunas de comunicaciones móviles, como ocurre en buena parte de las comunicaciones entre un avión y la torre de control, debido que la posible lejanía y el movimiento del avión puede dar lugar a desvanecimientos. Sin embargo, la modulación en amplitud tiene un inconveniente y es la vulnerabilidad a las interferencias atmosféricas.

Figura 12. **Modulación ASK**



Fuente: http://jfergar.wordpress.com/2010/12/01/tipos-de-modulacion/. Consulta 15/09/10.

Entonces la modulación ASK consiste en establecer una variación de la amplitud de la frecuencia portadora, según los estados significativos de la señal de datos. Sin embargo este método no se emplea en las técnicas de construcción de los módems puesto que no permiten implementar técnicas que permitan elevar la velocidad de transmisión.

1.3.2. Modulación de amplitud FSK

Este tipo de modulación consiste en asignar una frecuencia diferente a cada estado significativo de la señal de datos. Para ello existen dos tipos de modulación FSK**:** FSK Coherente y FSK No Coherente.

FSK coherente esta se refiere a cuando en el instante de asignar la frecuencia se mantiene la fase de la señal.

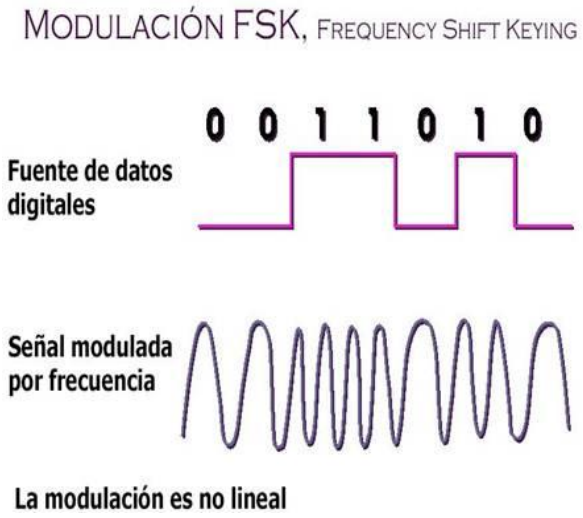
FSK no coherente aquí la fase no se mantiene al momento de asignar la frecuencia, independiente para la generación de las distintas frecuencias. La modulación FSK se emplea en los módem en forma general hasta velocidades de 2400 baudios. Sobre velocidades mayores se emplea la modulación PSK.

La modulación de amplitud tiene en la práctica dos inconvenientes: no siempre se transmite la información con la suficiente calidad, ya que el ancho de banda en las emisiones está limitado; en la recepción es difícil eliminar las interferencias producidas por descargas atmosféricas, motores, etc. La modulación de frecuencias consiste en variar la frecuencia de la onda portadora de acuerdo con la intensidad de la onda de información. La amplitud de la onda modulada es constante e igual que la de la onda portadora.

La frecuencia de la portadora oscila más o menos rápidamente, según la onda moduladora, esto es, si se aplica una moduladora de 100 Hz, la onda modulada se desplaza arriba y abajo cien veces en un segundo respecto de su frecuencia central, que es la portadora; además el grado de esta variación dependerá del volumen con que se module la portadora, a lo que se denomina índice de modulación.

Debido a que los ruidos o interferencias que se mencionaron anteriormente alteran la amplitud de la onda, no afecta a la información transmitida en FM, puesto que dicha información se extrae de la variación de frecuencias y no de la amplitud, que es constante. Como consecuencia de estas características de modulación se puede observar cómo la calidad de sonido o imagen es mayor cuando se modula en frecuencia que cuando se hace en amplitud. Además al no alterar la frecuencia de la portadora en la medida que se aplica la información, se pueden transmitir señales sonoras o información de otro tipo (datos o imágenes), que comprenden mayor abanico de frecuencias moduladoras, sin por ello abarcar mayor ancho de banda.

Figura 13. **Modulación FSK**



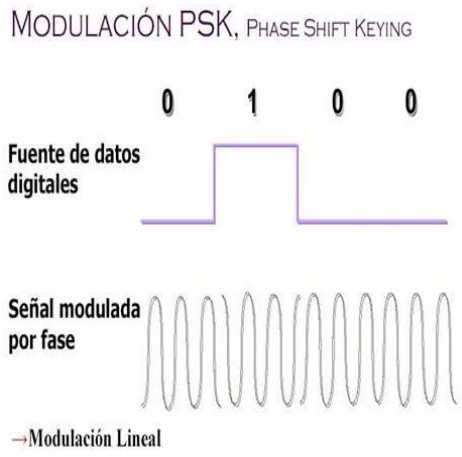
Fuente: http://jfergar.wordpress.com/2010/12/01/tipos-de-modulacion/. Consulta 17/09/10.

1.3.3. Modulación de amplitud y frecuencia PSK

PSK (*Phase-shift keying*), es una modulación de fase donde la señal moduladora (datos) es digital. Existen dos alternativas de modulación PSK: PSK convencional, donde se tienen en cuenta los desplazamientos de fase y PSK diferencial, en la cual se consideran las transiciones. La modulación PSK asigna una fase distinta a la portadora, según el estado de la señal de datos. Un ejemplo de este tipo de modulación digital podría ser la modulación BPSK 31. .

A la modulación PSK binaria se la denomina BPSK (*Binary PSK*). Si la modulación PSK introduce cambios de fase en la portadora respecto de la fase original, se trata de una modulación PSK pura; sin embargo, si la modulación introduce en la portadora saltos de fase respecto del estado anterior, se conoce entonces como modulación PSK Diferencial o DPSK. Este tipo de modulación tiene la ventaja de permitir una sincronización más rápida en el receptor.

Figura 14. **Modulación PSK**



Fuente: http://jfergar.wordpress.com/2010/12/01/tipos-de-modulacion/. Consulta 17/09/10.

1.4 Tipo de protocolos de enlace

Un protocolo es un conjunto de normas o reglas que permiten el intercambio de información entre 2 dispositivos de un mismo nivel. Estos ayudan no sólo a la comunicación, sino que permiten entre varias cosas la corrección de errores.

Para comunicarse, se ha dicho que se necesitan elementos físicos y lógicos y así lograr un mejor entendimiento. Pero también estos elementos deben ser estructurados de algún modo, y la mejor forma para hacerlo se denomina modularización, que se basa en dividir el conjunto de elementos en subconjuntos independientes uno del otro, para trabajar más fácilmente. Pero estos subconjuntos pueden ser cambiados por otros ya que debido a los avances tecnológicos se necesita modernizar el equipo.

Para realizar una comunicación mediante un sistema tele informático se requieren varios factores:

El lenguaje que se usa está compuesto por el código de los datos y si no se logra comprender al mismo, se utilizan las funciones de traducción para pasar un código a otro más fácil.

Se necesitan normas para controlar la información que se pasa y se establecen los turnos de intervención y turnos de espera de cada persona.

Se controlan las conexiones y el movimiento de los datos.

Todo este sistema tele informático debe ser bien estructurado y se deben dividir las funciones en niveles; estos tienen que estar controlados para que se resuelvan las necesidades de la comunicación.

Las redes que hay actualmente para la comunicación de datos se deben organizar en un conjunto, de capas o niveles para simplificar las tareas. Cada nivel se desarrolla sobre el anterior y el número de ellos varían en cada red. En general, al conjunto de los niveles (con sus protocolos ya determinados) se denomina arquitectura de la red. Una red teleinformática permite comunicar aplicaciones que se ejecutan en distintos sistemas y lugares. Por ejemplo: enviar un archivo de un sistema a otro, transmitir un mensaje de un usuario a otro. El nivel superior de la arquitectura se denomina nivel de aplicación, ya que proporciona los servicios necesarios para la comunicación.

El *Internet Protocol version* 6 (IPv6) (en español: *Protocolo de Internet versión 6*) es una versión del protocolo *Internet Protocol* (IP), definida en el RFC 2460 y diseñada para reemplazar a *Internet Protocol version* 4 (IPv4) RFC 791, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

IPv6 está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles, está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. El nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes.

A principios de 2010, quedaba menos del 11 % de IPs sin asignar. En la semana del 3 al 7 de febrero del 2011, la IANA (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó el último

bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IPs en Asia, un mercado que está en auge y no tardará en consumirlas todas.

IPv4 posibilita 4.294.967.296 (2^{32}) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada vehículo, teléfono, PDA, etcétera. En cambio, IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (2^{128} o 340 sextillones de direcciones) —cerca de $6{,}7 \times 10^{17}$ (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de la Tierra.

Otra vía para la popularización del protocolo es la adopción de este por parte de instituciones. El gobierno de los Estados Unidos ordenó el despliegue de IPv6 por todas sus agencias federales en el año 2008.

Las direcciones IPv6 se representan en el Sistema de Nombres de Dominio (DNS) mediante registros AAAA (también llamados registros de Qua-A, por tener una longitud cuatro veces la de los registros A para IPv4)

El concepto de AAAA fue una de las dos propuestas al tiempo que se estaba diseñando la arquitectura IPv6. La otra propuesta utilizaba registros A6 y otras innovaciones como las etiquetas de cadena de bits (*bit-string labels*) y los registros DNAME.

Mientras que la idea de AAAA es una simple generalización del DNS IPv4, la A6 fue una revisión y puesta a punto del DNS para ser más genérico, y de ahí su complejidad.

La RFC 3363 recomienda utilizar registros AAAA hasta tanto se pruebe y estudie exhaustivamente el uso de registros A6. La RFC 3364 realiza una comparación de las ventajas y desventajas de cada tipo de registro.

Ante el agotamiento de las direcciones IPv4, el cambio a IPv6 ya ha comenzado. Se espera que convivan ambos protocolos durante 20 años y que la implantación de IPv6 sea paulatina. Existe una serie de mecanismos que permitirán la convivencia y la migración progresiva tanto de las redes como de los equipos de usuario. En general, los mecanismos de transición pueden clasificarse en tres grupos:

- Doble pila
- Túneles
- Traducción

La doble pila hace referencia a una solución de nivel IP con doble pila (RFC 4213), que implementa las pilas de ambos protocolos, IPv4 e IPv6, en cada nodo de la red. Cada nodo con doble pila en la red tendrá dos direcciones de red, una IPv4 y otra IPv6.

A favor: fácil de desplegar y extensamente soportado.

En contra: la topología de red requiere dos tablas de encaminamiento y dos procesos de encaminamiento. Cada nodo en la red necesita tener actualizadas las dos pilas.

Los túneles permiten conectarse a redes IPv6 "saltando" sobre redes IPv4. Estos túneles trabajan encapsulando los paquetes IPv6 en paquetes IPv4 teniendo como siguiente capa IP el protocolo número 41, y de ahí el nombre proto-41. De esta manera, se pueden enviar paquetes IPv6 sobre una infraestructura IPv4. Hay muchas tecnologías de túneles disponibles. La principal diferencia está en el método que usan los nodos encapsuladores para determinar la dirección a la salida del túnel.

La traducción es necesaria cuando un nodo que sólo soporta IPv4 intenta comunicar con otro que sólo soporta IPv6. Los mecanismos de traducción se pueden dividir en dos grupos basados en si la información de estado está guardada o no

- Con estado: NAT-PT (RFC 2766), TCP-UDP *Relay* (RFC 3142), *Socks_based Gateway* (RFC 3089).

- Sin estado: *Bump-in-the-Stack, Bump-in-the-API* (RFC 276)

1.4.1 Capa de enlace – protocolo Mac 802.11

El estándar IEEE 802.11 define nueve servicios MAC (*Medium Access Control*). Seis de estos servicios están destinados a la transmisión de paquetes (MSDUs) entre STA (estaciones). Los tres servicios restantes se utilizan para controlar el acceso a la LAN 802.11 y proporcionar confidencialidad a la transacción de datos. Los servicios son: entrega de MSDUs (*MSDU delivery*), distribución, integración, asociación, reasociación, desasociación, autentificación, desautentificación y privacidad. Algunos de estos servicios van ligados a la funcionalidad de las STA mientras que el resto está asociado a la funcionalidad del DS. Cada uno de estos servicios está soportado por una o más tramas de tipo MAC. Algunos de ellos son soportados por tramas MAC de gestión y otros por tramas MAC de datos.

El protocolo MAC del estándar IEEE 802.11 distingue tres tipos de tramas: tramas de control, de datos y de gestión. Los mensajes de gestión se utilizan para soportar los servicios de 802.11; los de control, para la correcta entrega de tramas y los de datos, transportan la información de los usuarios.

El algoritmo básico de acceso a este nivel es muy similar al implementado en el estándar IEEE 802.3 y es el llamado CSMA/CA (*Carrier Sense Multiple Access / Collision Advoidance*). Este protocolo evita colisiones en lugar de descubrir una colisión, como el algoritmo usado en la 802.3.

En una red inalámbrica es difícil descubrir colisiones. Es por ello que se utiliza el CSMA/CA y no el CSMA/CD debido a que entre el final y el principio de una transmisión suelen provocarse colisiones en el medio. En CSMA/CA, cuando una estación identifica el fin de una transmisión, espera un tiempo aleatorio antes de transmitir su información, disminuyendo así la posibilidad de colisiones. Sin embargo, CSMA/CA es un entorno inalámbrico y celular que presenta una serie de problemas que se intentará resolver con alguna modificación. Los dos principales problemas que se pueden detectar son:

Nodos ocultos: una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no oye.

Nodos expuestos: una estación cree que el canal está ocupado, pero en realidad está libre, pues el nodo al que oye no le interferiría para transmitir a otro destino.

La solución que propone 802.11 es MACA (*MultiAccess Collision Avoidance)*. Según este protocolo, antes de transmitir, el emisor envía una trama RTS (*request to Send*), indicando la longitud de datos que quiere enviar.

El receptor le contesta con una trama CTS (*Clear to Send*), repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos. Los nodos seguirán una serie de normas para evitar los nodos. Ocultos y expuestos.

- Al escuchar un RTS, hay que esperar un tiempo por el CTS.
- Al escuchar un CTS, hay que esperar según la longitud.

La solución final de 802.11 utiliza MACA con CSMA/CA para evitar los RTS y CTS. Las características de la arquitectura MAC del estándar 802.11 se pueden resumir en estos puntos:

- Determina cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo a nivel MAC a través del medio inalámbrico.

- Utiliza MACA (CSMA/CA con RTS/CTS) como protocolo de acceso al medio.

- Necesita el reconocimiento ACKs, provocando retransmisiones si no se recibe.

- Usa campo *Duration*/ID que contiene el tiempo de reserva para transmisión y ACK.

- Esto quiere decir que todos los nodos conocerán al escuchar cuándo el canal volverá quedar libre.

- Implementa fragmentación de datos.

- Concede prioridad a tramas mediante el espacio entre tramas (IFS).

- Soporta *Broadcast* y *Multicast* sin ACKs.

1.4.2. Protocolo CSMA/CA

CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) o *Distributed Coordination Function* (DCF). CSMA/CA intenta evitar colisiones utilizando un paquete explícito de reconocimiento (ACK), en donde un paquete ACK es enviado por la estación receptora confirmando que el paquete de datos llegó intacto. CSMA/CA trabaja de la siguiente manera: una estación que quiere transmitir censa el aire, y si no se detecta actividad, la estación espera un tiempo adicional, seleccionado aleatoriamente y entonces transmite si el medio continúa libre.

Si el paquete es recibido intacto, la estación receptora envía un *frame* ACK una vez que el proceso de recepción termina. Si el *frame* ACK no es detectado por la estación transmisora, se asume que hubo una colisión y el paquete es transmitido de nuevo después de esperar otra cantidad de tiempo aleatoria. CSMA/CA además provee un camino para compartir el acceso sobre el aire. Este mecanismo explícito de ACK también maneja de manera efectiva la interferencia y otros problemas relacionados con radio.

Cuando una estación quiere enviar una trama escucha primero para ver si alguien está transmitiendo. Si el canal está libre la estación transmite. Si está ocupado se espera a que el emisor termine y reciba su ACK, después se espera un tiempo aleatorio y transmite. El tiempo en espera se mide por intervalos de duración constante.

Al terminar espera a que el receptor le envíe una confirmación (ACK). Si esta no se produce dentro de un tiempo prefijado considera que se ha producido una colisión; en cuyo caso repite el proceso desde el principio.

Las redes basadas en el estándar IEEE 802.3 son las más usadas. Consisten en un Bus donde se conectan las distintas estaciones, donde se usa un protocolo MAC llamado CSMA-CD (*Carrier Sense Multiple Access with Collision Detection*). El protocolo CSMA-CD funciona de la siguiente manera: un nodo que desea transmitir espera a que el canal esté aislado, una vez que se encuentra en este estado, empieza la transmisión. Si otro nodo empezara también a transmitir, en este instante se produciría colisión, por lo tanto se detiene la transmisión y se retransmite tras un retraso aleatorio.

Las estaciones en una LAN CSMA/CD pueden acceder a la red en cualquier momento y, antes de enviar los datos, las estaciones CSMA/CD "escuchan" la red para ver si ya es operativa. Si lo está, la estación que desea transmitir espera. Si la red no está en uso, la estación transmite. Se produce una colisión cuando dos estaciones que escuchan el tráfico en la red no "oyen" nada y transmiten simultáneamente. En este caso, ambas transmisiones quedan desbaratadas y las estaciones deben transmitir de nuevo en otro momento. Los algoritmos *Backoff* determinan cuándo deben retransmitir las estaciones que han colisionado. Las estaciones CSMA/CD pueden detectar colisiones y determinar cuándo retransmitir.

Las colisiones pueden producirse porque dos estaciones a la espera elijan el mismo número de intervalos (mismo tiempo aleatorio) para transmitir después de la emisión en curso. En ese caso reintentan ampliando exponencialmente el rango de intervalos y vuelven a elegir. Es similar a Ethernet, salvo que las estaciones no detecten la colisión, infieren que se ha producido cuando no reciben el ACK esperado.

También se produce una colisión cuando dos estaciones deciden transmitir a la vez, o casi a la vez. Pero el riesgo es mínimo. Para una distancia

entre estaciones de 70 metros en el tiempo que tarda en llegar, la señal es de 0.23 µs.

Fragmentación: en el nivel MAC de 802.11 se prevé la posibilidad de que el emisor fragmente una trama para enviarla en trozos más pequeños; por cada fragmento se devuelve un ACK, por lo menos en caso necesario es retransmitido por separado. Si el emisor ve que las tramas no están llegando bien puede decidir fragmentar las tramas grandes para enviarla en trozos más pequeños. Por cada fragmento se devuelve un ACK por lo que en caso necesario es retransmitido por separado. Todas las estaciones están obligadas a soportar la fragmentación en recepción, pero no en transmisión.

1.4.3. Protocolo RTS/CTS

RTS/CTS (Petición de enviar/claro enviar) es el mecanismo usado por 802.11 protocolo de establecimiento de una red sin hilos para reducir las colisiones del marco introducidas por problema terminal ocultado. El protocolo fijó originalmente problema terminal expuesto también, pero RTS/CTS moderno incluye ACKs y no soluciona problema terminal expuesto.

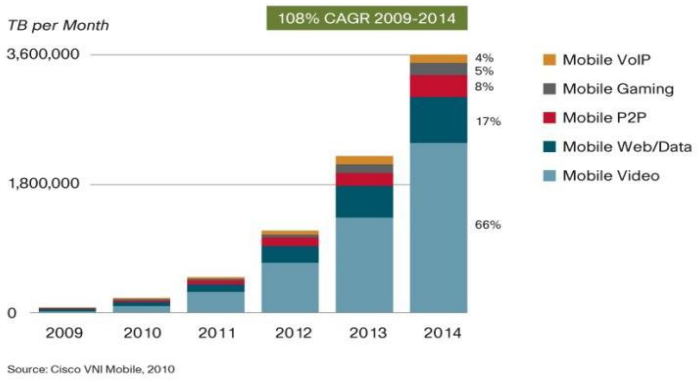
El uso de mensajes RTS/CTS se denomina a veces *Virtual Carrier Sense*. Emite a una estación reservar el medio durante una trama para su uso exclusivo. Si todas las estaciones se escuchan directamente entre sí, el uso de RTS/CTS no aporta nada y supone un *overead* importante, sobre todo en tramas pequeñas.

No todos los equipos soportan el uso de RTS/CTS. Los que lo soportan permiten indicar en un parámetro de configuración, a partir de qué tamaño de trama se quieren utilizar RTS/CTS.

2. ANÁLISIS SITUACIÓN ACTUAL REDES INALÁMBRICAS EN LOS PAISES EN DESARROLLO

La masiva popularidad de las redes inalámbricas ha llevado a una disminución continua del costo del equipamiento, mientras que la capacidad del mismo continua incrementándose. Como se ha podido observar con el desarrollo de las comunicaciones y la necesidad de movilidad con anchura de banda cada día más grande, ha nacido la necesidad de encontrar soluciones de diseño eficiente, fiable y sobre todo a bajo costo. En la siguiente gráfica se encuentra una previsión de la cantidad de datos por mes, de las comunicaciones móviles para el período 2009 – 2014 hechas por Cisco.

Figura 15. **Comunicaciones móviles 2009 – 2014**



Fuente: http://abra360.blogspot.com/2010/06/homo-digitalis-vi.html. Consulta 22/09/10.

La técnica Radio *over Fiber*, permite transmitir directamente en fibra óptica la señal a microondas o a frecuencia intermedia, permitiendo aprovechar las ventajas de las fibras (como por ejemplo bajas pérdidas, gran anchura de

banda, inmunidad a interferencias electromagnéticas y seguridad de la privacidad de los datos y de los usuarios) y de las de un sistema de acceso inalámbrico con estaciones radio de bajo coste (en cuanto si no se transmite en banda base, a lo máximo se necesita un oscilador local o un interferómetro para regenerar la frecuencia a microondas, que de todas formas son componentes muy baratos y con muy buenas características a nivel de prestaciones).

La estación base, que es el corazón del sistema, es el equipo que más se diferencia a lo largo de la empresas. Esta diferencia no se limita sólo a las características electro-ópticas (frecuencias de trabajo, sistemas suportados, potencia de entrada y salida, cifra de ruido, etc.) y físicas (peso, dimensiones), sino también a nivel de medios de transportes suportados (fibra mono, multi-modo, coaxial), conectores, arquitectura (necesidad de concentradores hub intermedios, como el sistema de ADC) y gestión, aunque sí parece que el protocolo de gestión basado en web y SNMP sobretodo, parecen ser los más preferidos, con la ventaja de una grande posibilidad de escalabilidad del sistema especialmente en entornos web.

2.1. Historia

La primera red experimental de conmutación de paquetes se usó en el Reino Unido, en los *National Physics Laboratories*; otro experimento similar lo llevó a cabo en Francia la *Societe Internationale de Telecommunications Aeronautiques*. Hasta el año 1969 esta tecnología no llegó a los Estados Unidos de América (USA), donde comenzó a utilizarla el ARPA, o agencia de proyectos avanzados de investigación para la defensa.

El ancestro de la Internet, pues, fue creado por la ARPA y se denomina ARPANET. El plan inicial se distribuyó en 1967. Los dispositivos necesarios para conectar ordenadores entre sí se llamaron IMP (*Information Message*

Processor), y eran un potente miniordenador fabricado por *Honeywell,* con 12 Ks de memoria principal. El primero se instaló en la UCLA, y posteriormente se instalaron otros en Santa Bárbara, *Stanford* y *Utah*. Curiosamente, estos nodos iníciales de la Internet todavía siguen activos, aunque sus nombres han cambiado. Los demás nodos que se fueron añadiendo a la red correspondían principalmente a empresas y universidades que trabajaban con contratos de defensa.

Internet viene de interconexión de redes, y el origen real de la Internet se sitúa en 1972, cuando, en una conferencia internacional, representantes de Francia, Reino Unido, Canadá, Noruega, Japón y Suecia, discutieron la necesidad de empezar a ponerse de acuerdo sobre protocolos, es decir, sobre la forma de enviar información por la red, de forma que todo el mundo la entendiera.

La primera red comercial fue la *TransCanada Telephone Systemas Dataroute*, a la que posteriormente sigue el *Digital Data System* de *AT&T*. Estas dos redes, para beneficio de sus usuarios, redujeron el costo y aumentaron la flexibilidad y funcionalidad.

El concepto de redes públicas de datos emergió simultáneamente. Algunas razones para favorecer el desarrollo de redes públicas de datos es que el enfoque de redes privadas es muchas veces insuficiente para satisfacer las necesidades de comunicación de un usuario dado. La falta de interconectabilidad entre redes privadas y la demanda potencial de información entre ellas, en un futuro cercano, favorecen el desarrollo de las redes públicas.

Aparecen las redes inalámbricas, el problema principal que pretendía resolver la normalización es la compatibilidad. No obstante, existen distintos

estándares que definen diferentes tipos de redes inalámbricas. Para resolver este problema, los principales vendedores de soluciones inalámbricas crearon en 1999 una asociación conocida como WECA *(Wireless Ethernet Compability Alliance*, "Alianza de Compatibilidad Ethernet Inalámbrica"). El objetivo fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurarse la compatibilidad de equipos.

En abril del 2000, WECA certificó la interoperatividad de equipos según la norma IEEE 802.11b bajo la marca WI-FI (Fidelidad Inalámbrica). Esto confirma que todo lo del sello WI-FI puede trabajar junto sin problemas, independientemente del fabricante de cada uno de ellos.

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

Con el sistema WI-FI se pueden establecer comunicaciones a una velocidad máxima de 11 Mbps, alcanzándose distancia de hasta cientos de metros. No obstante, versiones más recientes de esta tecnología permiten alcanzar los 22, 54 y hasta los 100 Mbps.

En 1990, en el seno de IEEE 802, se formó el comité IEEE 802.11, que empezó a trabajar para tratar de generar una norma para las WLAN. Pero no fue sino hasta 1994 cuando aparece el primer borrador.

En 1992 se crea *Winforum*, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (*Personal Communications Systems*). En ese mismo año, la ETSI (*European*

Telecommunications Standards Institute), a través del comité ETSI-RES 10, inició actuaciones para crear una norma a la que denominó HiperLAN (*High Performance LAN*) para, asignar las bandas de 5,2 y 17,1 GHz. En 1993 también se constituyó la IRDA (*Infrared Data Association*) para promover el desarrollo de las WLAN, basadas en enlaces por infrarrojos.

En 1996, finalmente, un grupo de empresas del sector de informática móvil (*mobile computing*) y de servicios formaron el *Wireless* LAN *Interoperability Forum (WLI Forum*) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos. Entre los miembros fundadores de WLI *Forum* se encuentran empresas como ALPS *Electronic*, AMP, *Data General, Contron, Seiko Epson y Zenith Data Systems*.

Del Comité de Normalización de Redes Locales (IEEE 802) del Instituto de Ingenieros Eléctricos, IEEE de Estados Unidos se puede entonces destacar las normas siguientes: · 802.3 CSMA/CD (*ETHERNET*) · 802.4 *TOKEN BUS* · 802.5 *TOKEN RING*·

En las redes metropolitanas por otro lado, el Instituto Americano de Normalización, (ANSI), ha desarrollado unas especificaciones para redes locales con fibra óptica, las cuales se conocen con el nombre de FDDI, y es obre del Comité X3T9.5 del ANSI. La última revisión del estándar FDDI, llamada FDDI-II, ha adecuado la norma para soportar no sólo comunicaciones de datos, sino también de voz y vídeo.

Para las aplicaciones de las redes locales en el entorno de la automatización Industrial, ha surgido el MAP (*Manufacturing Automation Protocol*), apoyado en la recomendación 802.4 y para las aplicaciones en el entorno de oficina surgió el TOP (*Technical and Office Protocol*), basado en la norma 802.3.

2.2. Características de una red inalámbrica

Un sistema de comunicación inalámbrico flexible y de bajo costo, utilizado como alternativa de la red cableada o como extensión de esta, utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizarse las conexiones cableadas.

Características:

- Movilidad**:** permite transmitir información en tiempo real en cualquier lugar de la organización o empresa a cualquier usuario. Esto supone mayor productividad y posibilidades de servicio.

- Facilidad de instalación: al no usar cables, se evitan obras para tirar cable por muros y techos, mejorando así el aspecto y la habitabilidad de los locales, y reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios temporales de la red.

- Flexibilidad: puede llegar donde el cable no puede, superando mayor número de obstáculos, llegando a atravesar paredes. Así, es útil en zonas donde el cableado no es posible o es muy costoso. Como por ejemplo, parques naturales, reservas o zonas escarpadas.

2.3. La red lógica

Una red lógica se refiere en sí a todos los protocolos que requiere una red para estar en funcionamiento,

La red lógica en sí, es la planeación y diseño de la implementación de la red, también se refiere a la forma en que estos van a poder compartir datos, es

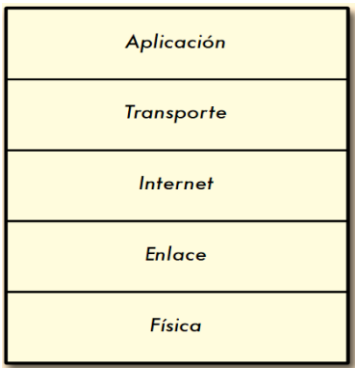
decir, aunque dos computadoras estén conectadas físicamente, hace falta establecer una conexión lógica entre ellas para que se lleve a cabo la comunicación y esto se hace asignando direcciones conocidas como direcciones IP. (En el protocolo TCP/IP) la comunicación es posible solo cuando los participantes hablan un lenguaje común. Los protocolos se vuelven tan importantes como el lenguaje. Sin un conjunto común de protocolos de comunicación que regulen cuándo y cómo cada computador puede hablar.

Estos son los protocolos que son importantes en la red lógica:

TCP/IP, comprende el conjunto de protocolos que permiten que sucedan las conversaciones en Internet entendiendo TCP/IP, usted puede construir redes que virtualmente pueden crecer a cualquier tamaño, y en última instancia formar parte de la Internet global.

El Modelo TCP/IP**,** las redes de datos se describen a menudo como construidas en muchas capas. Cada capa depende de la operación de todas las capas subyacentes antes de que la comunicación pueda ocurrir, pero sólo necesita intercambiar datos con la capa superior o la inferior. El modelo de redes TCP/IP2 comprende 5 capas, como se muestra en este diagrama:

Figura 16. **Modelo de redes TCP/IP**



Fuente: http://www.alfinal.com/Temas/tcpip.php. Consulta 07/10/10.

La capa física, este es el medio físico donde ocurre la comunicación. Puede ser un cable de cobre CAT5, un cable de fibra óptica, ondas de radio, o cualquier otro medio.

Capa de enlace, cuando dos o más nodos comparten el mismo medio físico (por ejemplo, varias computadoras conectadas a un concentrador (*hub*), o un cuarto lleno de computadoras portátiles usando el mismo canal de radio) la capa de enlace establece quién tiene el turno para transmitir en el medio. La comunicación sobre esta capa se llama de enlace local, ya que todos los nodos pueden comunicarse unos con otros directamente. En redes tipo Ethernet, cada nodo tiene su propia dirección MAC (*Media Access Control*), que es un número único de 48 bits asignado a cada dispositivo de red cuando es fabricado. Justo sobre la capa enlace está la capa Internet.

Capa Internet, para TCP/IP, está constituido por el Protocolo Internet (IP). En la capa Internet, los paquetes pueden salir del enlace local de red y ser retransmitidos a otras redes. Los enrutadores realizan esta función teniendo por lo menos dos interfaces de red, una en cada una de las redes a ser

interconectadas. Los nodos en Internet son especificados por su única dirección IP global. Una vez establecido el enrutamiento en Internet, se necesita un método para alcanzar un servicio particular en una dirección IP dada. Esta función es realizada por la próxima capa.

Capa de transporte, TCP y UDP son ejemplos comunes de protocolos de la capa de transporte. Algunos protocolos de la capa de transporte (como el TCP) aseguran que todos los datos han llegado a su destino, y son reensamblados y entregados a la próxima capa en el orden correcto.

Capa de aplicación, esta es la capa con la que la mayoría de los usuarios tienen contacto, y es el nivel en el que ocurre la comunicación humana. HTTP, FTP, y SMTP son todos protocolos de la capa de aplicación. Las personas están por encima de todas estas capas, y necesitan poco o ningún conocimiento de las subyacentes para usar efectivamente la red.

En las redes inalámbricas 802.11 antes de que los paquetes puedan ser reenviados y enrutados en Internet, la capa uno (física) y dos (enlace) necesitan estar conectadas. Sin conectividad de enlace local, los nodos no pueden hablarse y enrutar paquetes.

Para proveer conectividad física, los dispositivos de redes inalámbricas deben operar en la misma porción del espectro de radio. Esto significa que los radios 802.11a se comunican con otro radio 802.11a en frecuencias de 5GHz, y que los radios 802.11b/g hablan con otros 802.11b/g en 2,4GHz, pero un dispositivo 802.11a no puede interoperar con uno 802.11b/g, puesto que usan porciones completamente diferentes del espectro electromagnético.

Más específicamente, las tarjetas inalámbricas deben concordar en un canal común. Si a una tarjeta de radio 802.11b se le asigna el canal 2 mientras que otra el canal 11, no podrán comunicarse. Cuando dos tarjetas inalámbricas son configuradas para usar el mismo protocolo en el mismo canal de radio, están prontas para negociar conectividad al nivel de la capa de enlace. Cada dispositivo 802.11a/b/g puede operar en uno de los cuatro modos posibles:

El modo maestro, (también llamado AP o modo de infraestructura) se utiliza para crear un servicio que parece un punto de acceso tradicional. La tarjeta de red crea una red con un canal y un nombre específico (llamado SSID), para ofrecer sus servicios. En el modo maestro, las tarjetas inalámbricas administran todas las comunicaciones de la red (autentificación de clientes inalámbricos, control de acceso al canal, repetición de paquetes, etc.). Las tarjetas inalámbricas en modo maestro sólo pueden comunicarse con tarjetas asociadas a ella en modo administrado.

El modo administrado, es denominado algunas veces modo cliente. Las tarjetas inalámbricas en modo administrado sólo pueden unirse a una red creada por una tarjeta en modo maestro, y automáticamente cambiarán su canal para que corresponda con el de ésta. Luego ellas presentan las credenciales necesarias al maestro, y si estas son aceptadas, se dice que están asociadas con la tarjeta en modo maestro. Las tarjetas en modo administrado no se comunican unas con otras directamente, y sólo se van a comunicar con una tarjeta asociada en modo maestro.

El modo ad hoc crea una red multipunto a multipunto donde no hay un único nodo maestro o AP. En el modo ad hoc, cada tarjeta inalámbrica se comunica directamente con sus vecinas. Cada nodo debe estar dentro del

alcance de los otros para comunicarse, y concordar en un nombre y un canal de red.

El modo monitor es utilizado por algunas herramientas (tales como *Kismet*) para escuchar pasivamente todo el tráfico de radio en un canal dado. En el modo monitor, las tarjetas inalámbricas no trasmiten datos. Se utiliza para analizar problemas en un enlace inalámbrico o para observar el uso del espectro en el área local. El modo monitor no es usado para las comunicaciones normales.

Cuando se implementa un enlace punto a punto, o punto a multipunto, un radio opera en modo maestro, mientras que los otros operan en modo administrado. En una red *mesh* multipunto a multipunto, todos los radios operan en modo ad hoc, de manera que puedan comunicarse directamente.

Ahora que las tarjetas inalámbricas proveen conectividad física y de enlace, están listas para comenzar a pasar paquetes a la capa 3 la capa Internet.

2.4. Redes Internet/*Mesh* con OLSR

Redes Internet direcciones IP, direccionamiento de redes, enrutamiento y reenvío son conceptos relacionados e importantes en redes Internet. Una dirección IP es un identificador para un nodo de red como un PC, un servidor, un enrutador o un puente. El direccionamiento de redes es un sistema usado para asignar estos identificadores en grupos convenientes. El enrutamiento mantiene un registro del lugar en la red donde están ubicados esos grupos.

Los resultados del proceso de enrutamiento se guardan en una lista llamada tabla de enrutamiento. El reenvío es la acción de usar la tabla de enrutamiento para mandar un paquete al destino final o al "próximo salto" en dirección a ese destino.

Direcciones IP en una red IP3, la dirección es un número de 32 bits, usualmente escrito como 4 números de 8 bits expresados en forma decimal, separados por puntos. Algunos ejemplos de direcciones IP son 10.0.17.1, 192.168.1.1 ó 172.16.5.23

Direccionamiento de redes, las redes interconectadas deben ponerse de acuerdo sobre un plan de direccionamiento IP. En Internet, hay comités de personas que asignan las direcciones IP con un método consistente y coherente para garantizar que no se dupliquen las direcciones, y establecen nombres que representan a grupos de direcciones. Esos grupos de direcciones son denominados subredes, o *subnets*. Grandes *subnets* pueden ser subdivididas en *subnets* más pequeñas. Algunas veces un grupo de direcciones relacionadas se denomina espacio de direcciones.

Mediante acuerdos, las direcciones son asignadas a organizaciones en relación con sus necesidades y tamaño. Una organización a la cual se le ha asignado un rango de direcciones, puede también asignar una porción de ese rango a otra organización como parte de un contrato de servicio. Las direcciones que han sido asignadas de esta manera, comenzando con comités reconocidos internacionalmente, y luego repartidas jerárquicamente por comités nacionales o regionales, son denominadas direcciones IP enrutadas globalmente.

Algunas veces es inconveniente o imposible obtener más de una dirección IP enrutada globalmente para un individuo u organización. En este caso, se puede usar una técnica conocida como Traducción de Direcciones de Red o NAT (*Network Address Translation*). Un dispositivo NAT es un enrutador con dos puertos de red. El puerto externo utiliza una dirección IP enrutada globalmente, mientras que el puerto interno utiliza una dirección IP de un rango especial conocido como direcciones privadas. El enrutador NAT permite que una única dirección global sea compartida por todos los usuarios internos, los cuales usan direcciones privadas. A medida que los paquetes pasan por él, los convierte de una forma de direccionamiento a otra. Al usuario le parece que está conectado directamente a Internet y que no requieren software o controladores especiales para compartir una única dirección IP enrutada globalmente.

Enrutamiento, Internet está cambiando y creciendo constantemente. Continuamente se agregan nuevas redes, se añaden y remueven enlaces entre redes, que fallan y vuelven a funcionar. El trabajo del enrutamiento es determinar la mejor ruta al destino, y crear una tabla que liste el mejor camino para todos los diferentes destinos.

Enrutamiento estático, es el término utilizado cuando la tabla de enrutamiento es creada por configuración manual. Algunas veces esto es conveniente para redes pequeñas, pero puede transformarse rápidamente en algo muy dificultoso y propenso al error en redes grandes. Peor aún, si la mejor ruta para una red se torna inutilizable por una falla en el equipo u otras razones, el enrutamiento estático no podrá hacer uso de otro camino.

Enrutamiento dinámico, es un método en el cual los elementos de la red, en particular los enrutadores, intercambian información acerca de su estado y el

estado de sus vecinos en la red, y luego utilizan esta información para automáticamente tomar la mejor ruta y crear la tabla de enrutamiento. Si algo cambia, como un enrutador que falla, o uno nuevo que se pone en servicio, los protocolos de enrutamiento dinámico realizan los ajustes a la tabla de enrutamiento. El sistema de intercambio de paquetes y toma de decisiones es conocido como protocolo de enrutamiento. Hay muchos protocolos de enrutamiento usados en Internet hoy en día, incluyendo OSPF, BGP, RIP, y EIGRP.

Reenvío, es más sencillo que el direccionamiento y el enrutamiento. Cada vez que un enrutador recibe un paquete, consulta su tabla de enrutamiento interna. Comenzando con el bit más significativo (de mayor orden), escudriña la tabla de enrutamiento hasta encontrar la entrada que tenga el mayor número de bits coincidentes con la dirección destinataria. A esto se le llama prefijo de la dirección. Si en la tabla se encuentra una entrada que coincide con el prefijo, el campo *hop count* (cuenta de salto) o TTL (tiempo de vida) se decrementa. Si el resultado es cero, el paquete se descarta y se envía una notificación de error al emisor del mismo. De lo contrario, el paquete se envía al nodo o interfaz especificado en la tabla de enrutamiento.

Una vez que todos los nodos de la red tienen una dirección IP, pueden enviar paquetes de datos a cualquier otro nodo. Mediante el enrutamiento y el reenvío, esos paquetes pueden llegar a nodos en redes que no están conectadas físicamente con el nodo original.

Redes *mesh* con OLSR: la mayoría de las redes Wi-Fi operan en el modo de infraestructura, consisten en un punto de acceso en un lugar (con un radio operando en el modo maestro), conectado a una línea DSL u otra red cableada de larga distancia. En un "*hot spot*" el punto de acceso generalmente actúa

como una estación máster que distribuye el acceso a Internet a sus clientes, que operan en el modo administrado. Esta topología es similar al servicio GSM de teléfonos móviles. Los teléfonos móviles se conectan a una estación base; si no existe, se pueden comunicar entre sí.

Las tarjetas Wi-Fi en el modo administrado tampoco pueden comunicarse directamente. Los clientes por ejemplo, dos computadoras portátiles en la misma mesa, tienen que usar un punto de acceso como intermediario. Todo el tráfico entre dos clientes conectados a un punto de acceso debe ser enviado dos veces. Si los clientes A y C se comunican, el cliente A envía datos al punto de acceso B, y luego el punto de acceso va a retransmitir los datos al cliente C. Una transmisión puede tener una velocidad de 600 Kbyte/segundo (que es prácticamente la máxima velocidad que se puede obtener con 802.11b). En el ejemplo señalado, puesto que los datos deben ser repetidos por el punto de acceso antes de que lleguen a su objetivo, la velocidad real entre ambos clientes va a ser de sólo 300 Kbyte/segundo.

En el modo ad hoc no hay una relación jerárquica entre maestro-cliente. Los nodos pueden comunicarse directamente si están dentro del rango de su interfaz inalámbrica. Por lo tanto, en el ejemplo, ambas computadoras podrían conectarse a la velocidad máxima cuando operan en ad hoc, bajo circunstancias ideales.

La desventaja del modo ad hoc es que los clientes no repiten el tráfico destinado a otros clientes. En el ejemplo del punto de acceso, si dos clientes A y C no pueden “verse” directamente con su interfaz inalámbrica, todavía se pueden comunicar si el AP está dentro del rango inalámbrico de ambos clientes.

Los nodos ad hoc no repiten datos por omisión, pero pueden hacerlo si se aplica el enrutamiento. Las redes malladas (*mesh*) están basadas en la estrategia de que cada nodo actúa como un relevo para extender la cobertura de la red inalámbrica. Cuantos más nodos, mejor será la cobertura de radio y rango de la nube mallada.

Hay un tema importante que debe ser mencionado en este punto. Si el dispositivo utiliza solamente una interfaz de radio, el ancho de banda disponible se ve reducido significativamente cada vez que el tráfico es repetido por los nodos intermedios en el camino desde A hasta B. Además, va a haber interferencia en la transmisión de esos nodos compartiendo el mismo canal. Por lo tanto, las económicas redes malladas ad hoc pueden suministrar muy buena cobertura de radio a una red inalámbrica comunitaria a expensas de la velocidad, especialmente si la densidad de los nodos y la potencia de transmisión son elevadas.

Si una red ad hoc consiste sólo en unos pocos nodos que están funcionando simultáneamente, si no se mueven y siempre tienen radioenlaces estables y una larga lista de otras condicionantes es posible escribir a mano una tabla de enrutamiento individual para todos los nodos. Desafortunadamente, esas condiciones raramente se encuentran en el mundo real. Los nodos pueden fallar, los dispositivos Wi-Fi pueden cambiar de lugar, y la interferencia puede hacer que los radioenlaces estén inutilizados en cualquier momento. Además nadie quiere actualizar varias tablas de enrutamiento a mano si se adiciona un nodo a la red.

Mediante la utilización de protocolos que mantienen automáticamente las tablas de enrutamiento individuales de cada nodo involucrado, pueden olvidarse esos temas.

Enrutamiento mallado con *olsrd*, el Demonio de Enrutamiento de Estado de Enlace de olsr.org es una aplicación desarrollada para el enrutamiento de redes inalámbricas. Habrá más concentración en este software de enrutamiento por varias razones. Es un proyecto fuente abierta que soporta Mac OS X, Windows 98, 2000, XP, Linux*, FreeBSD*, *OpenBSD y NetBSD*. Olsrd está disponible para puntos de acceso que corren Linux como Linksys WRT54G, Asus Wl500g, *AccessCube* o *Pocket PCs* que corren Linux Familiar, y viene incluido en los equipos *Metrix* que corren *Metrix Pebble*. Olsrd puede manejar interfaces múltiples; puede extenderse con diferentes plug-ins. Soporta IPv6 y está siendo desarrollado y utilizado activamente en redes comunitarias alrededor del mundo.

El *olsrd* actual difiere significativamente del borrador original porque incluye un mecanismo denominado *Link Quality Extension* (Extensión de la Calidad del Enlace) que mide la cantidad de paquetes perdidos entre nodos y calcula las rutas de acuerdo con esta información. Esta extensión rompe la compatibilidad con los demonios de enrutamiento que adhieren al borrador del INRIA.

El *olsrd* disponible en olsr.org puede ser configurado para comportarse de acuerdo con el borrador del IETF que carece de esta característica pero no hay una razón para deshabilitar el *Link Quality Extension* (Extensión de la Calidad del Enlace), a menos que se requiera la compatibilidad con otras implementaciones. Después de haber corrido olsrd por un rato, cada nodo adquiere conocimiento acerca de la existencia de los otros nodos en la nube mallada; los nodos pueden ser utilizados para enrutar el tráfico hacia ellos. Cada nodo mantiene una tabla de enrutamiento que cubre la totalidad de la nube mesh. Este enfoque de enrutamiento mallado es denominado

enrutamiento proactivo. En contraste, los algoritmos de enrutamiento reactivo buscan rutas sólo cuando es necesario enviar datos a un nodo específico.

La ventaja más grande del enrutamiento proactivo es que se sabe quién está dentro o fuera de la red y no se debe esperar hasta que se encuentre una ruta. El alto tráfico de protocolo y la mayor cantidad de carga de CPU son algunas de las desventajas. Hay un límite al grado hasta el cual la extensión de un protocolo proactivo puede escalar, dependiendo de cuántas interfaces estén involucradas y cuán a menudo se actualizan las tablas de enrutamiento. Mantener rutas en una nube mallada con nodos estáticos toma menos esfuerzo que hacerlo en una *mesh* compuesta de nodos que están en constante movimiento, ya que la tabla de enrutamiento no necesita ser actualizada tan a menudo.

2.5. Estimando capacidad

Los enlaces inalámbricos pueden proveer a los usuarios un rendimiento real significantemente mayor que las conexiones tradicionales a Internet, tales como VSAT, discado, o DSL. El rendimiento también se denomina capacidad del canal, o simplemente ancho de banda (aunque este término no está relacionado con el ancho de banda de las ondas de radio).

Es importante comprender que la velocidad listada de los dispositivos inalámbricos (la tasa de datos) se refiere a la tasa a la cual los radios pueden intercambiar símbolos, no al rendimiento que va a observar el usuario. Como se mencionó antes, un enlace 802.11g puede utilizar 54Mbps en el radio, pero el rendimiento real será de unos 22Mbps. El resto es la tasa (*overhead*) que necesitan los radios 802.11g para coordinar sus señales.

El rendimiento es una medida de bits por tiempo: 22 Mbps significa que en un segundo dado pueden ser enviados hasta 22 megabits desde un extremo del enlace al otro. Si los usuarios intentan enviar más de 22 megabits a través del enlace, va a demorar más de un segundo. Si los datos no pueden ser enviados inmediatamente, son puestos en una cola de espera, y transmitidos tan pronto como sea posible. Esta cola de datos incrementa el tiempo que se necesita para que los bits puestos en la cola más recientemente atraviesen el enlace. El tiempo que le toma a los datos atravesar el enlace es denominado latencia, y una latencia muy grande es denominada comúnmente demora (*lag*). El enlace va a enviar todo el tráfico en espera, pero sus clientes seguramente se quejen al incrementar la demora.

Las diversas aplicaciones de Internet requieren diferentes cantidades de rendimiento, esto depende de cuántos usuarios existen y de cómo usan su enlace inalámbrico.

Para estimar el rendimiento necesario para cada red, debe multiplicarse el número esperado de usuarios por el tipo de aplicación que probablemente vayan a usar. Por ejemplo, 50 usuarios quienes están principalmente navegando en la web, en los momentos pico van a consumir entre 2.5 a 5Mbps o más de rendimiento, y se va a tolerar algo de latencia. Por otro lado, 50 usuarios simultáneos de VoIP van a requerir de 5Mbps o más de rendimiento en ambas direcciones sin absolutamente nada de latencia.

Debido a que el equipamiento inalámbrico 802.11g es *half duplex* (esto es, sólo transmite o recibe, nunca las dos cosas a la vez) debe duplicar el rendimiento requerido por un total de 10Mbps. Sus enlaces deben proveer esa capacidad cada segundo, o las conversaciones van a tener demora.

Ya que es poco probable que todos sus usuarios utilicen la conexión precisamente al mismo momento, una práctica normal es la de sobresuscribir, el rendimiento disponible por algún factor (esto es, permitir más usuarios de los que el máximo de ancho de banda disponible puede soportar). La sobre subscripción en un factor que va desde 2 a 5, es bastante normal. Probablemente se utilice sobresuscripción cuando se construya la infraestructura de red. Si se es cuidadoso en el monitoreo del rendimiento real de la red, se va a poder planificar cuándo actualizar diferentes partes de la red, y cuántos recursos adicionales se van a necesitar.

Es de esperar que, sin importar cuánta capacidad provea, sus usuarios encuentren aplicaciones que utilicen la totalidad de la misma. Como podrá verse, las técnicas de conformación del ancho de banda pueden ayudar a mitigar algunos problemas de latencia. Mediante la conformación de ancho de banda, almacenamiento temporal (*caching*) web, así como otras técnicas, se puede reducir significativamente la latencia e incrementar el rendimiento global de la red.

2.6. Planificar enlaces

Un sistema básico de comunicación consiste de dos radios, cada uno con su antena asociada, separados por la trayectoria que se va a cubrir. Para tener una comunicación entre ambos, los radios requieren que la señal proveniente de la antena tenga un valor por encima de cierto mínimo.

El proceso de determinar si el enlace es viable se denomina cálculo del presupuesto de potencia. Que las señales puedan o no ser enviadas entre los radios dependerá de la calidad del equipamiento que se esté utilizando y de la

disminución de la señal debido a la distancia, denominada pérdida en la trayectoria.

Cálculo del presupuesto del enlace, la potencia disponible en un sistema 802.11 puede caracterizarse por los siguientes factores:

Potencia de transmisión, se expresa en mili vatios o en dBm. La potencia de transmisión tiene un rango de 30mW a 200mW o más. La potencia TX a menudo depende de la tasa de transmisión. La potencia TX de un dispositivo dado debe ser especificada en los manuales provistos por el fabricante, pero algunas veces puede ser difícil de encontrar.

Ganancia de las antenas, las antenas son dispositivos pasivos que crean el efecto de amplificación debido a su forma física. Las antenas tienen las mismas características cuando reciben que cuando transmiten. Por lo tanto, una antena de 12 dBi simplemente es una antena de 12 dBi, sin especificar si esto es en el modo de transmisión o de recepción. Las antenas parabólicas tienen una ganancia de 19-24 dBi, las antenas omnidireccionales de 5-12 dBi, y las antenas sectoriales, de 12-15 dBi. El mínimo nivel de señal recibida, o simplemente, la sensibilidad del receptor. El RSL (por su sigla en inglés) mínimo es expresado siempre como dBm negativos (- dBm) y es el nivel más bajo de señal que la red inalámbrica puede distinguir. El RSL mínimo depende de la tasa de transmisión, y como regla general la tasa más baja (1 Mbps) tiene la mayor sensibilidad. El mínimo va a estar generalmente, en el rango de -75 a -95 dBm. Al igual que la potencia TX, las especificaciones RSL deben ser provistas por el fabricante del equipo.

Pérdidas en los cables, parte de la energía de la señal se pierde en los cables, conectores y otros dispositivos entre los radios y las antenas. La pérdida

depende del tipo de cable utilizado y de su longitud. La pérdida de señal para cables coaxiales cortos incluyendo los conectores, es bastante baja; está en el rango de 2-3 dB. Lo mejor es tener cables lo más cortos, como sea posible.

Cuando se calcula la pérdida en la trayectoria, se deben considerar varios efectos. Algunos de ellos son pérdida en el espacio libre, atenuación y dispersión. La potencia de la señal se ve disminuida por la dispersión geométrica del frente de onda, conocida comúnmente como pérdida en el espacio libre. Ignorando todo lo demás, cuanto más lejanos los dos radios, más pequeña la señal recibida debido a la pérdida en el espacio libre. Esto es independiente del medio ambiente, se debe solamente a la distancia. Esta pérdida se da porque la energía de la señal radiada se expande en función de la distancia, desde el transmisor.

Utilizando los decibeles para expresar la pérdida y utilizando 2,45 GHz como la frecuencia de la señal, la ecuación para la pérdida en el espacio libre es: Lfsl = 40 + 20*log(r). Donde Lfsl (pérdida de señal en el espacio libre, por su sigla en inglés) es expresada en dB y r es la distancia en metros entre el transmisor y el receptor.

Para evaluar si un enlace es viable, se deben conocer las características del equipamiento que se está utilizando y evaluar la pérdida en el trayecto. Cuando se hace este cálculo, la potencia TX debe ser sumada sólo en uno de los lados del enlace. Si está utilizando diferentes radios en cada lado del enlace, se debe calcular la pérdida para cada dirección (utilizando la potencia TX adecuada para cada cálculo). Sumar todas las ganancias y restar las pérdidas resulta en: TX potencia de radio 1, más ganancia de la antena de radio 1 menos pérdida en los cables de radio 1, más ganancia de la antena de radio 2, menos pérdida en los cables de radio 2, es igual a ganancia total.

Restar la pérdida en el trayecto de la ganancia total da como resultado la ganancia total menos pérdida en el trayecto, igual nivel de señal en un lado del enlace.

Si el nivel de señal resultante es mayor que el nivel mínimo de señal recibido, entonces ¡el enlace es viable! La señal recibida es suficientemente potente para que los radios la utilicen. Recordar que el RSL mínimo se expresa siempre como dBm negativos, por lo tanto -56dBm es mayor que -70dBm.

En un trayecto dado, la variación en un período de tiempo de la pérdida en el trayecto puede ser grande, por lo que se debe considerar un margen (diferencia entre el nivel de señal recibida y el nivel mínimo de señal recibida). Este margen es la cantidad de señal por encima de la sensibilidad del radio que debe ser recibida para asegurar un enlace estable y de buena calidad durante malas situaciones climáticas y otras anomalías atmosféricas.

Un margen de 10 - 15 dB está bien. Para brindar algo de espacio para la atenuación y el multitrayecto en la señal de radio recibida, se debe tener un margen de 20dB.

Radio Mobile es una herramienta para el diseño y simulación de sistemas inalámbricos. Predice las prestaciones de radio enlaces utilizando información acerca del equipamiento y un mapa digital del área. Es un software de dominio público que corre con Windows, pero puede utilizarse en Linux con el emulador Wine.

Radio Mobile usa el modelo digital de elevación del terreno para el cálculo de la cobertura, indica la intensidad de la señal recibida en varios puntos

a lo largo del trayecto. Construye automáticamente un perfil entre dos puntos en el mapa digital mostrando el área de cobertura y la primera zona de Fresnel.

Durante la simulación chequea la línea visual y calcula la pérdida en el trayecto, incluyendo pérdidas debido a los obstáculos. Es posible crear redes de diferentes topologías, incluyendo máster/Slave (maestro/esclavo), punto a punto y punto a multipunto.

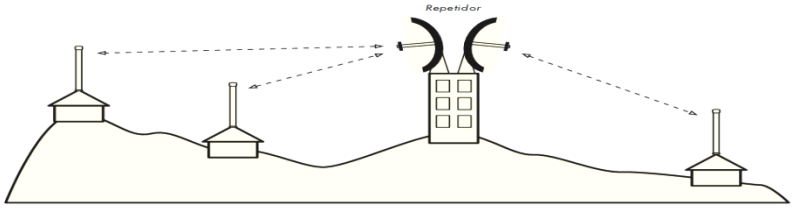
Repetidores, el componente más crítico para construir un enlace de red a larga distancia es la existencia de línea visual (a menudo abreviada como LOS). Los sistemas de microondas terrestres simplemente no pueden tolerar colinas altas, árboles, u otros obstáculos en el camino de un enlace a larga distancia. Es necesario que se tenga una idea del relieve de la tierra entre dos puntos antes de poder determinar si un enlace es posible.

Pero aún si hay una montaña entre dos puntos, se debe tener presente que los obstáculos pueden ser transformados en activos. Las montañas pueden bloquear la señal, pero suponiendo que se pueda proveer energía, también pueden actuar como muy buenos repetidores.

Los repetidores son nodos que están configurados para transmitir el tráfico que no es destinado al nodo. En una red mallada, cada nodo es un repetidor.

En una red de infraestructura tradicional, los nodos deben ser configurados específicamente para poder pasar el tráfico a otros nodos.

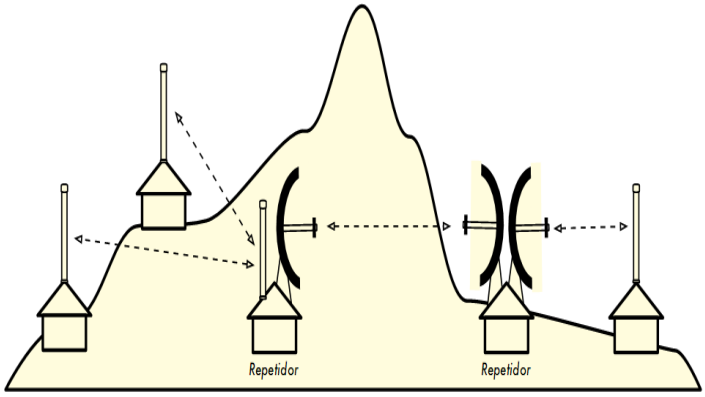
Figura 17. **Repetidor con línea visual directa**



Fuente: www.telebajar.com/redes-inalambricas. Consulta 28/10/10.

Muchas veces no puede pasar sobre, o a través de un obstáculo, a menudo lo puede rodear. En lugar de usar un enlace directo, se debe intentar hacer un salto múltiple para eludir el obstáculo.

Figura 18. **Múltiples repetidoras**



Fuente: www.telebajar.com/redes-inalambricas. Consulta 22/10/10.

Finalmente, podría necesitar ir hacia atrás para poder avanzar. Si se tiene un lugar alto en una dirección diferente, y ese lugar puede ver más allá del obstáculo, se puede hacer un enlace estable a través de una ruta indirecta.

2.7. Optimización del tráfico

El ancho de banda se mide como un cociente de número de bits transmitidos en un segundo. Esto significa que dado suficiente tiempo, la cantidad de información transmisible en cualquier enlace se acerca al infinito. Desafortunadamente, para un período de tiempo finito, el ancho de banda provisto por una conexión de red cualquiera, no es infinito. Siempre se puede descargar (o cargar) tanto tráfico como se desee; sólo que debe esperarse todo lo que sea necesario. Por supuesto que los usuarios humanos no son tan pacientes como las computadoras, y no están dispuestos a esperar una infinita cantidad de tiempo para que su información atraviese la red. Por esta razón, el ancho de banda debe ser gestionado y priorizado como cualquier otro recurso limitado.

Se puede mejorar significativamente el tiempo de respuesta y maximizar el rendimiento disponible mediante la eliminación del tráfico indeseado y redundante de la red.

Almacenamiento *Web* temporal, un servidor *web proxy* es un servidor en la red local que mantiene copias de lo que se ha leído recientemente, páginas web que son utilizadas a menudo, o partes de esas páginas, cuando la siguiente persona las busque; las mismas se recuperan desde el servidor *proxy* local sin ir hasta Internet. Esto resulta, en la mayoría de los casos en un acceso al web más rápido, al mismo tiempo que se reduce significativamente, la utilización del ancho de banda con Internet. Cuando se implementa un servidor proxy, el administrador debe saber que existen algunas páginas que no son almacenables, por ejemplo, páginas que son el resultado de programas del lado del servidor, u otros contenidos generados dinámicamente.

Otra cosa que también se ve afectada es la manera como se descargan las páginas web. Con un enlace a Internet lento, una página normal comienza a cargarse lentamente, primero mostrando algo de texto y luego desplegando los gráficos uno por uno. En una red con un servidor *proxy*, puede haber un retraso durante el cual parece que nada sucede, y luego la página se carga por completo rápidamente. Esto sucede porque la información es enviada a la computadora tan rápido que para el rearmado de la página se toma una cantidad de tiempo perceptible. El tiempo global que toma este procedimiento puede ser sólo de diez segundos (mientras que sin un servidor *proxy*, puede tomar 30 segundos cargar la página gradualmente).

Pero a menos que esto se explique a algunos usuarios impacientes, estos pueden decir que el servidor *proxy* está haciendo las cosas más lentamente.

Generalmente es tarea del administrador lidiar con la percepción de los usuarios acerca de temas como este.

Servidores *proxy***,** existen varios servidores *proxy* disponibles los que siguen son los paquetes de software utilizados más comúnmente:

Squid, el software libre *Squid* es el estándar de facto en las universidades. Es gratuito, confiable, sencillo de utilizar y puede ser mejorado (por ejemplo, añadiendo filtros de contenido y bloqueos de publicidad). *Squid* produce bitácoras (logs) que pueden ser analizadas utilizando software como *Awstats*, o *Webalizer*, los cuales son de fuente libre y producen buenos reportes gráficos. En la mayoría de los casos, es más fácil instalarlo como parte de la distribución (la mayoría de las distribuciones Linux como *Debian*, así como otras versiones de Unix como *NetBSD* y *FreeBSD* vienen con *Squid*).

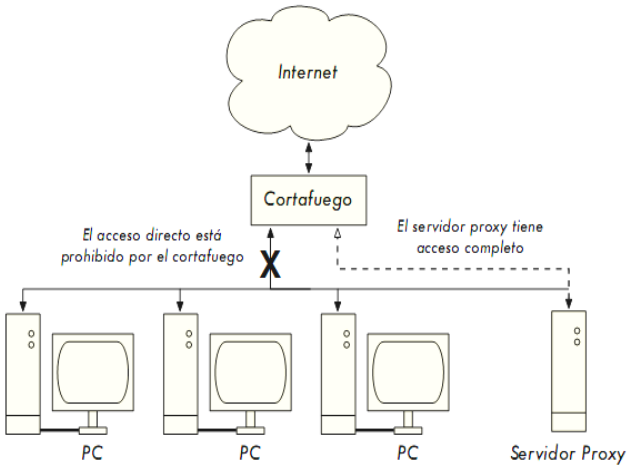
Servidor *Proxy Microsoft* 2.0, no está disponible para instalaciones nuevas porque ha sido reemplazado por el servidor *Microsoft* ISA y ha dejado de tener soporte. Si bien es utilizado por algunas instituciones es mejor no considerarlo para instalaciones nuevas.

Servidor *Microsoft* ISA, es un muy buen programa de servidor *proxy*, pero demasiado caro para lo que hace. Sin embargo, con descuentos académicos puede ser accesible para algunas instituciones.

Produce sus propios reportes gráficos, pero sus archivos de bitácora (*log*) también pueden ser analizados con el popular *software Sawmill*. Los administradores de un sitio con un Servidor MS ISA deben dedicar tiempo suficiente para obtener la configuración adecuada; por otra parte, el Servidor MS ISA *Server* puede utilizar gran cantidad de ancho de banda. Por ejemplo, una instalación por omisión puede consumir fácilmente más ancho de banda que lo que el sitio ha utilizado anteriormente, porque las páginas comunes con fechas de expiración cortas (tales como los sitios de noticias) se actualizan continuamente. Por lo tanto, es importante que la captura preliminar (pre-f*etching*) se configure correctamente, para que sea realizada durante la noche. El servidor ISA también puede ser asociado a productos de filtrado de contenidos tales como *WebSense.*

Cortafuego (*Firewall*), una de las maneras más confiable para asegurarse que las PC no van a eludir el proxy puede ser implementada utilizando un cortafuego. El cortafuego puede configurarse para que solamente pueda pasar el servidor *proxy*, por ejemplo, para hacer solicitudes de HTTP a Internet.

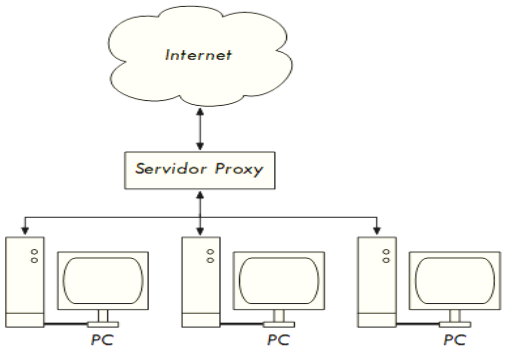
Figura 19. **Temporal *proxy***



Fuente: www.telebajar.com/redes-inalambricas. Consulta 30/10/10.

Dos tarjetas de red, posiblemente, el método más confiable es el de instalar dos tarjetas de red en el servidor *proxy* y conectar la red del campus a Internet como se muestra en la siguiente figura. De esta forma, el diseño de red hace físicamente imposible alcanzar la Internet sin pasar a través del servidor *proxy*.

Figura 20. **Servidor *Proxy***



Fuente: www.telebajar.com/redes-inalambricas. Consulta 30/10/10.

El servidor *proxy* en este diagrama no debe tener habilitado IP *forwarding*, a menos que los administradores conozcan exactamente qué es lo que quieren dejar pasar.

Una gran ventaja de este diseño es que puede utilizarse una técnica conocida como *transparent proxying*. Utilizar *proxy transparente* significa que las solicitudes *web* de los usuarios son reenviadas automáticamente al servidor *proxy*, sin ninguna necesidad de configurar manualmente los navegadores *web* para que lo utilicen. Esto fuerza efectivamente a que todo el tráfico *web* sea almacenado localmente, lo que elimina muchas posibilidades de error de los usuarios, y va a trabajar incluso con dispositivos que no soportan el uso de un *proxy* manual. Una forma de prevenir la circunvalación del *proxy* utilizando equipamiento Cisco es con una política de enrutamiento. El enrutador Cisco dirige transparentemente las solicitudes *web* al servidor *proxy*.

La ventaja de este método es que, si el servidor *proxy* está caído, las políticas de enrutamiento pueden ser removidas temporalmente permitiéndoles a los clientes conectarse directamente a Internet.

Sitio *web* espejo (*mirror*), con el permiso del dueño o del administrador del sitio web, el sitio completo puede ser copiado durante la noche al servidor local, siempre que el mismo no sea demasiado grande. Esto es algo que se debe tener en cuenta para sitios *web* importantes, que son de interés particular para la organización, o que son muy populares entre los usuarios de la *web*. Si bien esto puede ser útil, tiene algunas fallas potenciales. Por ejemplo, si el sitio que es duplicado contiene programas CGI u otros contenidos dinámicos que requieren de interacción con el usuario, va a haber problemas. Un ejemplo es el sitio *web* que requiere que la gente se registre en línea para una conferencia. Si alguien se registra en línea en un servidor duplicado (y el programa de

duplicado funciona bien), los organizadores del sitio no van a tener la información de que la persona se registró.

Pre-poblar la memoria intermedia (cache) utilizando *wget*, en lugar de instalar un sitio *web* duplicado como se describió en la sección anterior, un mejor enfoque es el de poblar la cache de la *proxy* utilizando un proceso automatizado "Un proceso automatizado recupera la página inicial del sitio y especifica el número de páginas extra (siguiendo recursivamente los enlaces HTML en las páginas recuperadas) a través del uso de un *proxy*. En lugar de copiar las páginas recuperadas en el disco local, el proceso de duplicación descarta las páginas recuperadas. Esto se hace para conservar los recursos del sistema, así como para evitar posibles problemas de *copyright*. Mediante el uso del *proxy* como intermediario, se garantiza que las páginas recuperadas están en el cache del *proxy* como si un cliente hubiera accedido a esa página. Cuando un cliente accede a la página recuperada, le es brindada desde el cache y no desde el enlace internacional congestionado. Este proceso puede ser corrido en momentos de poco uso de la red, para maximizar la utilización del ancho de banda y no competir con otras actividades de acceso.

Jerarquías de memoria temporal (cache), cuando una organización tiene más de un servidor *proxy*, los mismos pueden compartir información cache entre ellos. Por ejemplo, si una página *web* está en el cache del servidor A, pero no en el del servidor B, un usuario conectado a través del servidor B puede acceder a la página *web* en el servidor A, a través del servidor B. El Protocolo de Inter-Cache (*Inter-Cache Protocol (ICP*)) y el (*Cache Array Routing Protocol (CARP)*) pueden compartir información del cache. De estos, el protocolo CARP es considerado el mejor. *Squid* soporta ambos protocolos, y el servidor MS ISA soporta CARP.

El compartir información cache reduce el uso de ancho de banda en organizaciones donde se utiliza más de un *proxy*.

Almacenamiento intermedio (cache) y optimización de DNS, los servidores DNS con sólo la función de cache no son autoridades de ningún dominio, sólo almacenan los resultados de solicitudes pedidas por los clientes, tal como un servidor *prox*y que almacena páginas web populares por cierto tiempo. Las direcciones DNS son almacenadas hasta que su tiempo de vida (TTL por su sigla en inglés) expira. Esto va a reducir la cantidad de tráfico DNS en su conexión a Internet, porque el cache DNS puede ser capaz de satisfacer muchas de las preguntas localmente. Por supuesto que las computadoras de los clientes deben ser configuradas para utilizar el nombre del servidor solo de cache como su servidor DNS. Cuando todos los clientes utilicen ese servidor DNS como su servidor principal, se poblará rápidamente el cache de direcciones IP a nombres, por lo tanto los nombres solicitados previamente pueden ser resueltos rápidamente. Los servidores DNS que son autoridades para un dominio también actúan como cache de la conversión de nombres y direcciones de *hosts* de ese dominio.

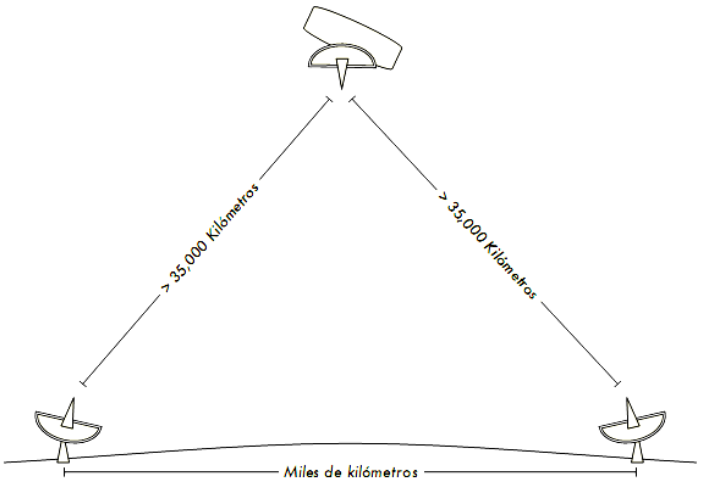
2.8. Optimización del enlace a Internet

Como se ha mencionado anteriormente, se pueden alcanzar rendimientos superiores a 22Mbps mediante la utilización de equipamiento 802.11g estándar para redes inalámbricas. Este valor de ancho de banda probablemente sea al menos un orden de magnitud mayor que la que le ofrece su enlace a Internet, y es capaz de soportar cómodamente muchos usuarios simultáneos de Internet. Pero si su conexión principal a Internet es a través de un enlace VSAT, se va a encontrar con algunos problemas de desempeño si utiliza los parámetros por omisión de TCP/IP. Optimizando su enlace VSAT, se

pueden mejorar significativamente los tiempos de respuesta cuando se accede a *hosts* de Internet.

Factores TCP/IP en una conexión por satélite, un VSAT es concebido a menudo como una tubería de datos larga y gruesa. Este término se refiere a los factores que afectan el desempeño de TCP/IP en cualquier red que tenga un ancho de banda relativamente grande, pero mucha latencia. La mayoría de las conexiones a Internet en África y otras partes del mundo en desarrollo son vía VSAT. Por lo tanto, aún si una universidad tiene su conexión a través de un ISP, esta sección puede ser aplicable si la conexión del ISP es a través de VSAT. La alta latencia en las redes por satélite se debe a la gran distancia del satélite y la velocidad constante de la luz. Esta distancia añade aproximadamente 520 mili segundos al tiempo de ida y retorno de un paquete (RTT *round trip time*), comparado con un RTT entre Europa y Estados Unidos de alrededor de 140 ms.

Figura 21. **Conexiones por satélite**



Fuente: www.telebajar.com/redes-inalambricas. Consulta 05/11/10.

Los factores que impactan más significativamente el rendimiento de TCP/IP son tiempos de propagación largos, grandes productos de ancho de banda por retardo y errores de transmisión. Generalmente, en una red satelital se deben utilizar sistemas operativos que soportan las implementaciones TCP/IP modernas. Estas, a la vez, soportan las extensiones RFC 1323: La opción de escalado de ventana para soportar ventanas TCP de gran tamaño (mayores que 64KB). Recepción selectiva (*SACK*) para permitir una recuperación más rápida de los errores de transmisión.

Matasellos (*Timestamps*) para calcular los valores de RTT y la expiración del tiempo de retransmisión para el enlace en uso. Tiempos de ida y vuelta largos (RTT). Los enlaces por satélite tienen un promedio de RTT de alrededor de 520 mili segundos hasta el primer salto. TCP utiliza el mecanismo de comienzo lento al inicio de la conexión para encontrar los parámetros de TCP/IP apropiados para la misma.

El tiempo perdido en la etapa de comienzo lento es proporcional al RTT, y para los enlaces por satélite significa que TCP se encuentra en el modo de comienzo lento por más tiempo de lo que debiera. Esto disminuye drásticamente el rendimiento de las conexiones TCP de corta duración; puede verse cuando al descargar un sitio web pequeño, sorprendentemente toma mucho tiempo, mientras que cuando se transfiere un archivo grande, se obtienen velocidades de datos aceptables luego de un rato. Además, cuando se pierden paquetes, TCP entra en la fase de control de congestión y, debido al alto RTT, permanece en esta fase por largo tiempo, reduciendo así el rendimiento de las conexiones TCP, sean de larga o corta duración. Deben tomarse en cuenta las siguientes condiciones:

Producto ancho de banda-retardo elevado, la cantidad de datos en tránsito en un enlace en un momento dado es el producto del ancho de banda por el RTT. Debido a la gran latencia del enlace satelital, este producto es grande. TCP/IP le permite a los *hosts* remotos enviar cierta cantidad de datos previamente sin esperar la confirmación. Normalmente en una conexión TCP/IP se requiere una confirmación (ACK) para cada transmisión. Sin embargo el *host* remoto siempre puede enviar cierta cantidad de datos sin confirmación, lo que es importante para lograr una buena tasa de transferencia en conexiones con productos anchos de banda-retardo de propagación elevados. Esta cantidad de datos es denominada tamaño de la ventana TCP. En las implementaciones TCP/IP modernas el tamaño de la ventana generalmente es de 64KB.

Errores de transmisión, en las implementaciones de TCP/IP más viejas, siempre se consideraba que la pérdida de paquetes era causada por la congestión (en lugar de errores de enlace). Cuando esto sucede, TCP adopta una defensiva contra la congestión, requiriendo tres confirmaciones duplicadas (ACK), o ejecutando un inicio lento (*slow start*) en el caso de que el tiempo de espera haya expirado. Debido al alto valor de RTT, una vez que esta fase de control de la congestión ha comenzado, toma un largo rato para que el enlace satelital TCP/IP vuelva al nivel de rendimiento anterior. Por consiguiente, los errores en un enlace satelital tienen un efecto más serio en las prestaciones de TCP que sobre los enlaces de latencia baja. Para solucionar esta limitación, se han desarrollado mecanismos como la Confirmación Selectiva (SACK por su sigla en inglés). SACK especifica exactamente aquellos paquetes que se han recibido, permitiendo que el emisor retransmita solamente aquellos segmentos que se perdieron debido a errores de enlace.

3. ANÁLISIS DE REQUERIMIENTOS

Debe realizarse el análisis de requerimiento para el diseño de una red que permita brindar acceso a internet de forma inalámbrica y que cumpla con los requerimientos básicos de: rendimiento, disponibilidad y seguridad.

Una vez que se está listo para instalar la red de área local, es necesario considerar algunos requerimientos por parte del personal que se encargará de instalar la red en el lugar previsto. Estos requerimientos se harán al cliente o al encargado del lugar donde se instalará la red. Se tienen que marcar algunos requerimientos hacia sus clientes para poder prestar sus servicios, y que se puedan aplicar como requerimientos de sistemas cuando se instala una LAN:

- Suministrar el espacio físico requerido para la instalación de los equipos.
- Permisos para la instalación de equipo y materiales en dicho espacio.
- Permisos para trabajar en la instalación y configuración de los equipos en cada oficina y edificio donde se instala, o permisos para realizar obras civiles si llega a ser necesario.

Suministro de energía eléctrica 110 Volts CA. Estos requerimientos proporcionan y garantizan en cierta medida la libertad de instalar adecuadamente la LAN, ya que se debe tomar en cuenta que la red local puede ser implementada en instalaciones que requieren de ciertos cuidados especiales por parte de la institución a la que se le instalará la red, y por razones de seguridad dicha institución puede tener algunas restricciones de acceso hacia ciertos puntos de la misma.

Dependencia de *software*: la dependencia de *software* se refiere al hecho de instalar ciertas aplicaciones o paquetes en las computadoras de la red, y que estos pueden necesitar de algunos componentes de *software* adicionales para su correcto funcionamiento, lo que conlleva a la instalación de paquetes o *software* adicional. Un ejemplo de lo anterior se puede apreciar en algunas aplicaciones de Internet, que requieren que la computadora cliente tenga instalado un pequeño programa para poder visualizar objetos realizados con la aplicación multimedia *Flash*. Otro claro ejemplo se puede notar cuando se utiliza alguna versión del sistema operativo Linux, y se requiere compilar algún código fuente válido para este sistema operativo, ya que para llevar a cabo esta acción, se debe tener instalados en la computadora los paquetes que contienen a los compiladores.

Mobiliario especial y equipo adicional: es natural que se deba contar con el espacio físico necesario para colocar todos los equipos de cómputo y componentes de la red, así como contar con el mobiliario para contener a dichos elementos.

Es necesario contar con algunas herramientas básicas para la instalación de la red, las cuales se mencionan a continuación:

- Taladro eléctrico
- Brocas para perforar metal y concreto
- Destornilladores plano y de cruz
- Pinzas ponchadoras RJ-45
- Flexómetro o metro
- Pinzas de corte y de punta

- *Cutter* o navaja
- Multímetro
- Conectores extra RJ-45 (o los necesarios dependiendo del tipo red)
- Cinta aislante
- Martillo
- Cautín y soldadura
- Escalera
- Grapas sujetadoras

Estas herramientas se pueden considerar básicas para la instalación de una red local, aunque dependiendo del medio de transmisión utilizado y los componentes de la red, pueden requerirse algunas herramientas adicionales. ¿Por qué siempre se consideran los conectores RJ-45 y la ponchadora?; bueno resulta que muchas instalaciones son redes híbridas y estas tienen una instalación cableada, entonces después de dicha instalación, quizás solo se tenga que poner alguna repetidora en un punto específico para cubrir todo el edificio o casa.

Análisis de tráfico: se implementará un computador con la aplicación MRTG, que permita sondear diferentes dispositivos y verificar el tráfico que está cursando por ellos. Para tener una idea real de las capacidades requeridas se ha tomado en cuenta a usuarios actuales en la red y con estos datos se verifica cuál es el uso efectivo de canal que el cliente realiza.

Protocolos requeridos: entre los protocolos requeridos para los usuarios está el uso de casilleros de correos usando POP en el puerto 110 y SMPT en el

puerto 25, además el ISP proveerá el servicio de alojamiento *WEB* para los usuarios y dará acceso al servidor para actualizar sus páginas mediante FPT. El tráfico Http es el más utilizado para navegar en la WEB.

3.1. Costos de accesorios para el desarrollo de una red inalámbrica en Guatemala

Las empresas tienen equipos de diferentes fabricantes de los cuales se destacan:

Smart Bridges, que son específicos para enlaces punto a punto y *Senao*, que pueden ser utilizados para enlaces punto a punto o multipunto. Empezando desde distribuidoras que venden señal satelital, presentan varias opciones como:

Oficina pequeña: esta opción permite la navegación de un máximo de cinco computadoras con un ancho de banda de 700 Kbps de descarga y 128 Kbps de subida. Este tipo de conexión le permite una descarga diaria de 200 Megas.

Oficina pequeña 2: esta opción le permite la navegación de diez computadoras con un ancho de banda de 1 Mega de descarga y 200 Kbps de subida. Este tipo de conexión le permite una descarga diaria de 375 megas.

Oficina pequeña 3: esta opción le permite navegación de un máximo de quince computadoras con un ancho de banda de 1.5 Mbps de descarga y 300 Kbps de subida. Este tipo de conexión le permite una descarga diaria de 425 megas.

Figura 22. **Antena de proveedores de servicio internet**

Fuente: http://www.siboneysatelital.com, http://www.satservicesolutions.galeon.com/index.html. Consulta 15/11/10.

Empresa mediana: esta opción le permite navegación de un máximo de veinticinco computadoras con un ancho de banda de 1.5 Mbps de descarga y 300 Kbps de subida. Este tipo de conexión le permite una descarga diaria de 500 megas.

Empresas grandes: esta opción le permite navegación de un máximo de cuarenta computadoras con un ancho de banda de 2 Mbps de descarga y 500 Kbps de subida. Este tipo de conexión le permite una descarga diaria de 1250 megas.

El equipo que se instala es una antena de 1.20 metros; con radio de 2 *watts* y se instala en cualquier parte de Guatemala, El Salvador y Belice. El servicio se puede instalar en hoteles, casa, fincas, proyectos móviles, etc.

Otras empresas se dedican a la distribución de Internet vía satelital desde cualquier punto geográfico, a velocidades desde 700 Kbps hasta 2 Mbps

de bajada y desde 128 Kbps hasta 500 Kbps de subida. Sus planes mensuales varían de $60.00 a $80.00 dólares.

Otros proveedores de servicio de internet comparan los precios que estos cobran por la instalación; también los beneficios que incluyen sus planes.

Tabla VI. **Tabla de proveedores de servicio de internet**

Proveedor	Tipo de servicio	Velocidad Kbps	Tarifa
Convergence	Internet por Cable	512	$50.00
RedInter	Internet por Cable	512	$50.00
Telecomunic (empresa actual)	Conexión Internet DSL	768	$65.00
Telefónica	Internet Satelital Inalámbrico	1Mbps	$45.00
Telgua - Turbonett	ADSL	512 Kbps	$58.00
		128 Kbps	$15.00
		256 Kbps	$28.00
		2 Mbps	$75.00
		5 Mbps	$100.00
Yego	Wireless	512 Kbps	$58.00
TIGO	Wireless	128	$15.00

Fuente: http://es.wikipedia.org/wiki/Comunicaciones_en_Guatemala. Consulta 15/11/10.

3.2. Comparación de tecnologías existentes en el mercado guatemalteco

Los productos más usados para los enlaces son los equipos punto a punto.

Todos los costos están en dólares y las marcas más utilizadas por su funcionamiento y precio son las siguientes:

Tabla VII. **Tabla productos más usados para enlaces**

Marca	**MTI BR58-11b**	**PROXIM Tsunami 45 & 100**
Interfaces	Fasth Ethernet, 802.3u Wireless: 802.11a	
Seguridad	WEP/WPA/Mac filtering	WEP
Administración	http, Telnet, SNMP	http, telnet SNMP
Frecuencia de trabajo	5.15-5.85 GHz	5250-5350 MHz
Sensibilidad	-68dBm@54Mbps -76dBm@36Mbps -84dBm@18Mbps -87dBm@9Mbps -88dBm@6Mbps	-79dBm
Modo de trabajo	Bridge	Bridge
Potencia de transmisión	17dBm@54Mbps 18dBm@48Mbps 20dBm@36Mbps – 6Mbps	13dBm mínimo
Antena	Tipo panel de 23 dBi, Flat panel Frecuencias: 5.3-5.8GHz Angulo de apertura: 11º tanto en horizontal como vertical	
Costo	1450	2300

Fuente: http://www.*proxim*.com/learn/library/datasheets/Tsunami_100.pdf. Consulta 15/11/10.

Tomando las características especiales y precios bajos se recomiendan los equipos MTI; su alta confiabilidad permite elegir uno de los catorce canales disponibles en el equipo.

Los equipos *proxim* sólo tienen un canal para conectarse, eso hace que tengan limitaciones para sortear interferencias.

Tabla VIII. **Comparación de equipo multipunto**

Características	SENAO-NOC-3220	NETkROM AIR-BR500G
Potencia	25dBm@1-24Mbps 23dBm@36Mbps 21dBm@48Mbps 20dBm@54Mbps	AIR-BR500G: 20dBm AIR-BR500GH: 23dBm AIR-BR500AG: 20dBm
Sensibilidad	-88dBm@6Mbps -70dBm@54Mbps	-90dB@ 6Mbps -89dB@ 9Mbps -87dB@12Mbps -85dB@18Mbps -82dB@24Mbps -79dB@36Mbps -76dB@48Mbps -74dB@54Mbps
Velocidades	5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	54, 48, 36, 24, 18, 12, 11, 5.5, 2, 1 Mbps
Rango de cobertura	5 Kilómetros	16 Kilómetros
Seguridad	IEEE 802.1x WEP, WAP/Pre Share Key(PSK)/TKIP Filtro de MAC	WEP 64/128/152 – bit Filtrado de MAC IEEE 802.1x TLS, TTLS, PEAP WAP-EAP, WPA2
Frecuencia	2.400 – 2.497 GHz	2.400- 2.497 GHz
Administración	WEB	SNMP, WEB
Costo	202.36	299

Fuente: http://www.solwise.co.uk/wireless-outdoor-bridging-noc-3220.htm
http://www.netkrom.com/support/manual/AIR-BR500X_manual.pdf. Consulta 17/11/10.

Los equipos recomendados son los *Netkrom*; los mismos funcionan en ambientes de un ISP; además, cumplen con los requerimientos, y el desempeño compensa el alto costo, aparte la garantía ofrecida por parte del fabricante.

Los equipos que se utilizaran para los clientes son de varios tipos:

- Tarjetas PCCARD
- USB
- PCI
- AP en modo cliente

Tabla IX. **Comparación de equipos para cliente**

MARCA	DLINK DWL-G132	NETGEAR WG111
Estándar	802.11b 802.11g	802.11b 802.11g
Velocidad	802.11b: 1, 2, 5.5, 11 Mbps 802.11g: 6, 9, 12, 18, 24, 36, 48, 54, 108, Mbps	.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Seguridad	WEP 64/128 bit WPA-Personal WPA-Enterprise (incluidos 802.1x)	WEP, WAP, 802.11x
Cobertura	Indoors: 100 metros Outdoors: 400 metros	Indoors: 100 metros Outdoors: 450 metros
Sensibilidad	-82dBm, 11Mbps -87dBm, 2Mbps -88dBm, 6Mbps -86dBm, 9Mbps -84dBm, 12Mbps -82dBm, 18Mbps -78dBm, 24Mbps -74dBm, 36Mbps -69dBm, 48Mbps -66dBm, 54Mbps	82dBm
Potencia de	15dBM@ 8Mbps	
Transmisión	16dBm @36Mbps 17dBm @24, 18, 12, 9, 6 Mbps	
Costo	79.99	

Fuente: http://www.dlink.com/products/?pid=358, ftp://ftp10.dlink.com/pdfs/products/DWL-G132/DWL-G132_ds.pdf. Consulta 17/11/10.

La conexión a la red podrá hacerse con cualquier tipo de tarjeta inalámbrica tomando en cuenta que las laptops ya vienen provistas de ellas, esto reduce el costo de instalación del servicio. En el caso que el usuario necesite instalación de un equipo externo para conectarse a la red, lo puede hacer mediante una AP en modo cliente.

Los controladores de Ancho de Banda pueden ser controlados desde sistemas operativos como Linux, controladores mediante plataforma CISCO. *Hardware* y *software* como *PACKETEER* o Linux.

La ayuda que ofrece Linux en el control de ancho de banda es mediante técnicas de encolamiento tales como CBQ, que presenta la capacidad de otorgar el ancho de banda requerido por cada clase, en un intervalo de tiempo especificado, si hubiera demanda del mismo. Esto se logra mediante un mecanismo que aplica esperas entre las transferencias de paquetes. En segunda instancia CBQ permite que las clases tomen prestado ancho de banda no utilizada por otras clases.

El QoS es implementado por un mecanismo de encolamiento. Este encolamiento maneja la manera en que los paquetes están esperando por su turno para salir de la interface, siempre trabaja sobre la interface de salida, las disciplinas de encolamiento controlan el orden y velocidad de los paquetes que están saliendo a través de la interface; adicionalmente, define cuáles paquetes deben de esperar por su turno para ser enviados fuera y cuáles serán descartados. Los encolamientos pueden ser clasificados dentro de dos grupos por su influencia en el flujo de datos:

- *Schedulers*
- *Shapers*

Tipo *Scheduler*: reordena el flujo de paquetes. Este tipo de disciplinas limita los números de paquetes sin degradar la velocidad. Se pueden hacer colas tipo FIFO, RED, SFQ PFIFO y BFIFO son del tipo FIFO con un buffer pequeño. La disciplina FIFO no cambia el orden del paquete, ellos justamente acumulan los paquetes hasta que un límite definido es sobrepasado.

Tipo *Shaper*: controla la velocidad del flujo de datos. Adicionalmente puede hacer un trabajo programado. La cola que se utiliza en esta caso es el PCQ (*Per Connection Queue*), la cual permite escoger clasificadores.

Entre los productos existentes en el mercado, basados en Linux se tienen los siguientes:

Tabla X. **Comparación de controladores de ancho de banda**

Marca	Características	Costo
Stick Gate	Control de ancho de banda por IP, MAC, reporte de clientes, Firewall incluido.	USD 585
Mikrotik	Controlador de ancho de banda, router, hotspot. Control de flujo tanto inbound como outbound, clasificación por IP, MAC o sub redes, manejo de tráfico WAN y LAN, manejo de redes ATM *Frame Relay.*	USD 265

Fuente: http://*www/*guatemala.internetmovil.com/banda-ancha/. Consulta 22/11/10.

Routers Cisco, este tipo de *routers* permite realizar la clasificación de ancho de banda mediante los siguientes mecanismos:

Shaping and *Policing*, este mecanismo permite tomar acciones sobre violaciones a la regla de tráfico, si se aplica *Shaping,* este retarda el tráfico mediante el encolamiento y *Policing* permite tomar acciones como el descarte de paquetes.

Traffic Policing, trabaja en una interfaz controlando el ancho de banda tanto de subida como de bajada, usando *Tocken Buckent*; esta técnica se podría utilizar para limitar los enlaces de la red de distribución.

Traffic Shaping, únicamente controla el tráfico saliente de una interfaz, los routers CISCO que permiten tener esta funcionalidad son los de las series 7500 y actualizado el IOS de los routers, se pueden implementar las series 2500 y 3500.

El *router* CISCO 2500 cuenta con dos interfaces seriales y dos interfaces *Fast Ethernet*, incluye versión de IOS 12.3 (8r) T8, tiene la funcionalidad de controlar el ancho de banda de acuerdo con los mecanismos anteriores.

Packeeter, este sistema es muy importante y se especializa en el control de ancho de banda, además permite realizar reportes, priorizar, clasificar y bloquear tráfico. Puede trabajar ya sea sobre redes 802.3 o sobres redes ATM, frame relay. Permite realizar clasificación de tráfico mediante puertos ya sean UDP o TCP, asignar ancho de banda por IP, MAC-Address, subred, host. Además maneja calidad de servicio para priorizar el tráfico. En la actualidad se utiliza este dispositivo para realizar el control de ancho de banda de los clientes. El problema de este dispositivo es que la capacidad de manejo de ancho de banda está limitada a 6 Mbps, para la expansión de la capacidad es necesario adquirir una licencia cuyo costo es de USD$1000; este rubro es muy alto para las empresas.

Selección del producto: al hacer comparaciones en tanto a funcionamiento y costos, se recomiendan las opciones, *Packeeter* o Linux-*Mikrotik.* Con respecto al CISCO no es muy recomendable debido a que su funcionamiento es limitado para controlar el ancho de banda y además su

costo es elevado respecto de las otras soluciones. En cuestiones de costos es recomendable utilizar *Mickotik* ya que permite adquirir las licencias según las necesidades, controla el ancho de banda e implementa un *firewall* y clasificador de tráfico. Su administración es mediante herramientas gráficas que permiten visualizar tráfico por clases. También se permite incorporar un *hotspot* que trabaja con un portal cautivo y un servidor *Radius* interno. Se detallan los costos de todo el *hardwar*e requerido, incluyendo los de configuración de los puntos de red; para la puesta en marcha de la WLAN. En el costo del punto de acceso está incluido el *software* de administración y seguridad.

Tabla XI. **Costo de implementación WLAN**

Cantidad	Descripción	Costo Unitario	Costo Total
2	PA-1000 802.11 a/b Punto de Acceso (incluye herramienta de gestión)	648.00	1296.00
2	802.11a/b USB Adapter GOLD	89.00	178.00
5	802.11a/b Cardbus GOLD	105.80	529.00
15	802.11a/b PCI Card GOLD	121.00	1815.00
2	20" IEEE Pigtail Assembly	66.00	132.00
2	Range Extender Antenna	81.00	162.00
	Total costo de Hardware		$ 4,112.00
20	Configuración de puntos de red	35.00	700.00
		Total general	$ 4,812.00

Fuente: http://www*l*biblioteca.meducation.edu.gt/tesis/08/08_0178_EO. Consulta 23/11/10.

3.3. Cableado inalámbrico

Lo sorprendente de un sistema inalámbrico es la cantidad de cables que están involucrados en el desarrollo de un simple enlace punto a punto. Un nodo inalámbrico está conformado por varios componentes que deben de estar conectados entre sí con el cableado apropiado.

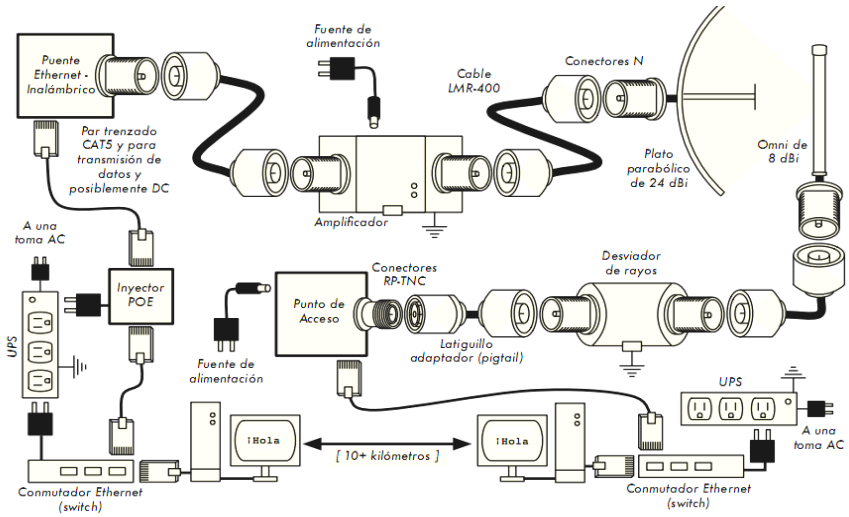
Obviamente, se necesita al menos una computadora conectada a una red *Ethernet*, un enrutador inalámbrico, o un puente en la misma red.

Los componentes de radio deben conectarse a las antenas, pero en el trayecto pueden requerir un amplificador, un protector contra rayos (es un dispositivo de tres terminales, uno conectado a la antena, el otro al radio y el tercero a tierra), u otro dispositivo.

Ahora deben multiplicarse los cables y conectores por el número de nodos que va a instalar, y bien puede surgir la duda por qué se hace referencia a esta tecnología como "inalámbrica".

La siguiente figura da alguna idea del cableado requerido para un enlace típico punto a punto.

Figura 23. **Cableado para el equipo inalámbrico**



Fuente: http://wndw.net/. Consulta 22/08/10.

Aunque los componentes utilizados varían de nodo a nodo, toda instalación va incorporar estas partes:

Una computadora o una red conectada a un conmutador Ethernet (*switch*).

Un dispositivo que conecte esa red a un dispositivo inalámbrico (un enrutador inalámbrico, un puente o un repetidor).

Una antena integrada en el dispositivo inalámbrico, o conectada mediante un cable apropiado.

Componentes eléctricos consistentes en fuentes de alimentación, acondicionadores de energía, y protectores contra rayos.

La selección del equipamiento debe determinarse estableciendo los requerimientos del proyecto, el presupuesto disponible, y verificando que dicho proyecto sea viable, utilizando los recursos disponibles (incluyendo provisiones para repuestos y costos de mantenimiento).

3.4. Equipos para redes inalámbricas

Los diferentes dispositivos inalámbricos necesarios para configurar una red inalámbrica.

Tarjeta o adaptador de red inalámbrica, reciben y envían la información entre las computadoras de la red; puede encontrarse velocidades desde 54 Mbps a 108 Mbps. Traen una antena externa o interna de baja ganancia tipo dipolo de 2 dBi de ganancia, esta se puede desacoplar y reemplazar por otra de

mayor ganancia. Hay que considerar que estas tarjetas las encontrarán integradas en los equipos móviles como laptops. Existen 3 tipos de adaptadores para las computadoras: primero las PCI son útiles para computadoras de escritorio.

Figura 24. **Adaptadores de red PCI Trendnet y D-link**

Fuente: http://5nd.net/. Consulta 24/11/10.

Segundo, PCMCIA/*PCcard* para equipos *laptops*, *notebooks*.

Figura 25. **Adaptadores de red PCMCIA**

Fuente: http://5nd.net/. Consulta 24/11/10.

Tercero, USB para equipos que no tengan puertos disponibles.

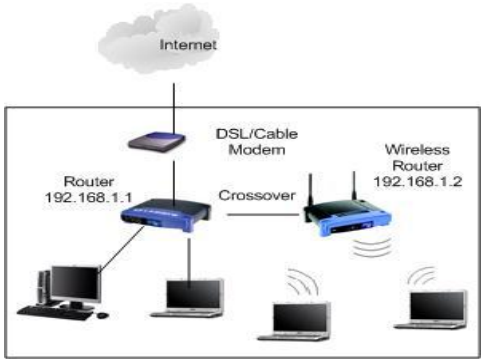
Figura 26. **Adaptadores de res USB**

Fuente: http://5nd.net/. Consulta 24/11/10.

Punto de acceso *(Access Point* AP), dispositivo que se encarga de concentrar la señal de los nodos inalámbricos. Es el punto principal de emisión y recepción, centraliza el reparto de la información de toda la red local inalámbrica. El AP permite configurar redes inalámbricas de buen alcance, seguras y de alta velocidad. En cuanto a seguridad trabaja con filtros de MAC, encriptados con claves WEP, WAP y WAP2 así como el uso de servidores *Radius*.

Tiene varios modos de operación como punto de acceso, Cliente, WDS con AP, repetidor. Trabaja con velocidades de 54 a 108 Mbps. Traen una o dos antenas las cuales pueden reemplazar por otras de mayor ganancia.

Figura 27. ***Access Point TP-Link***



Fuente: http://5nd.net/. Consulta 25/11/10.

Un punto de acceso tiene dos características importantes:

Potencia de su transmisor: qué tan potente es la señal que emite el equipo, esta se mide en dbm o mW (mili*watts*).

Sensibilidad de su transmisor, se refiere a qué tan débiles pueden ser las señales que detecta el equipo, también se determina en dbm.

Router inalámbrico, es el encargado de conectarnos a internet mediante la línea telefónica en el caso del *router* DSL de nuestro ISP (proveedor del servicio de Internet). La función básica del *router* es que puede distribuir la señal de internet mediante cables y en forma inalámbrica mediante el *Access Point* que trae integrado, otra función muy importante del *router* es la capacidad de hacer restricciones de acceso, por usuario, horarios, servicios, páginas web, etc.; asimismo puede hacer control de ancho de banda y prioridades de acceso por dispositivo o servicio, además de poder trabajar con tablas de rutas *(routing*). Hay muchas marcas pero las siguientes son las más conocidas: *Dlink, Tp-link, Linksys*, su costo puede ser entre 50 y 120 dólares.

Figura 28. **Router inalámbrico Linksys**

Fuente: http://5nd.net/. Consulta 25/11/10.

Cámaras de vigilancia inalámbricas, estos dispositivos permiten capturar imágenes en movimiento. Se pueden usar en las empresas, negocios de

tiendas, comerciales, inclusive en las casas, existen muchas variedades con diferentes características como captura, video, sonido, visión nocturna, etc.

Figura 29. **Cámaras de vigilancia inalámbricas**

Fuente: http://5nd.net/. Consulta 25/11/10.

Las antenas, son el elemento más importante de toda estación de transmisión y recepción. Todo lo que hacen los equipos de una estación es amplificar y transformar energía de corriente alterna. Sin embargo, para que una estación pueda comunicarse con otra sin recurrir a cable de interconexión, se necesita transformar la energía de corriente alterna en un campo electromagnético o viceversa. Cuanto más eficaz sea esa transformación mayor alcance tendrá la estación, independientemente del equipo que posea.

Figura 30. **Diferentes tipos de antena Wi-Fi**

Fuente: http://5nd.net/. Consulta 25/11/10.

La antena por sí sola constituye más del 50% de la calidad de una estación, por tanto, solo existen dos posibilidades: la antena es buena o mejor.

Algunos tipos de antenas son sencillas y fáciles de instalar. El hecho de que una antena sea sencilla no quiere decir que no tenga rendimiento óptimo.

- Características de una antena:

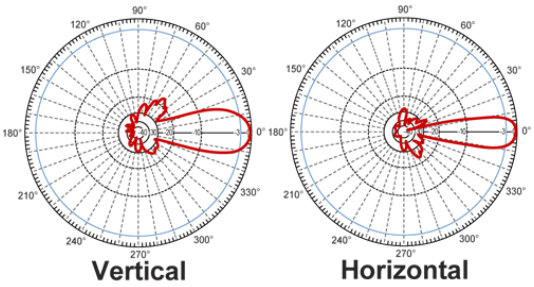
Impedancia característica, resistencia de la antena frente al transmisor de RF, representa la resistencia de carga al transmisor.

Una antena se tendrá que conectar a un transmisor y deberá radiar el máximo de potencia posible con un mínimo de pérdidas. Se deberá adaptar la antena al transmisor para una máxima transferencia de potencia, que se suele hacer a través de una línea de transmisión. Esta línea también influirá en la adaptación, debiéndose considerar su impedancia característica, atenuación y longitud. Esta impedancia característica es de 50 Ohm.

Ganancia, la amplificación de la señal electromagnética al momento de ser irradiada al espacio depende de las características de la antena. Se mide en dbi.

Patrón de radiación, es un diagrama polar que representa las intensidades de los campos o las densidades de potencia en varias posiciones angulares en relación con la antena. Si el patrón de radiación se traza en términos de la intensidad del campo eléctrico (E) o de la densidad de potencia (P), se llama patrón de radiación absoluto. Si se traza la intensidad del campo o la densidad de potencia en relación con el valor en un punto de referencia, se llama radiación relativa.

Figura 31. **Antena grid o parrilla**



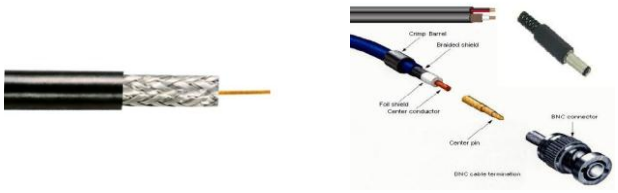
Fuente: www.solucionesinalambricas.pe/cont_antenas.html. Consulta 26/11/10.

Frecuencia de operación, rango de frecuencias soportadas por la antena para poder irradiar adecuadamente. Una antena no puede irradiar en cualquier frecuencia, las antenas son diferentes dependiendo de las frecuencias en la cual operan.

Polarización de la antena, se refiere sólo a la orientación del campo eléctrico radiado desde ésta. Si una antena irradia ondas electromagnéticas polarizadas verticalmente, la antena se define como polarizada verticalmente; si la antena irradia ondas electromagnéticas polarizadas horizontalmente, se dice que la antena está polarizada horizontalmente.

Cables y conectores, las antenas externas se conectan a los equipos *Wireless* mediante un cable. El cable que une el dispositivo *Wireless* con la antena, es un cable de tipo coaxial de impedancia de 50 ohmios. Los cables coaxiales se caracterizan porque disponen de un conector central (normalmente denominado activo) rodeado de una malla metálica concéntrica, que le protege de las interferencias que son muchas en el campo radioeléctrico, en que operan habitualmente las tarjetas y los puntos de acceso inalámbricos.

Figura 32. **Cable coaxial**



Fuente: www.seguridad*wireless*.net/hwagm/conectores-cables.htm. Consulta 01/12/10.

Para conectar el cable a la antena y a los dispositivos inalámbricos, se utilizan los conectores. Tanto la antena como algunos equipos *Wireless* disponen de un conector donde se deben de enchufar sus correspondientes conectores de los extremos de cable. Para llevar esto a cabo existen dos tipos de conectores conocidos como tipo macho y tipo hembra. Tanto el cable como cada conector, añaden perdidas a las señales de radio *Wireless*. Estas pérdidas se pueden evitar utilizando cables y conectores de calidad.

MiniPCI, los podemos encontrar en las tarjeta *Wireless* miniPCI de algunos portátiles, también en muchos puntos de acceso y routers *Wireless*. El más habitual se llama UFL o Conector miniPCI.

Figura 33. **Tarjeta *wireless* MiniPCI de laptop**

Fuente: http://5nd.net/. Consulta 01/12/10.

MC-*Card*, estos también se pueden distinguir entre macho y hembra. Los conectores *MC-Card* se usan en determinados componentes *Wireless*, como pueden ser algunas tarjetas PCMIA *Wireless*.

Figura 34. **Conector MC-Card y conector MC-*Card* macho**

Fuente: http://5nd.net/. Consulta 01/12/10.

El *Pigtail*, es el cable unido con los conectores en ambos extremos, que permite conectar la antena al dispositivo inalámbrico. A diferencia de las antenas, los adaptadores de red *wireless* no suelen disponer de un conector tipo N, sino más bien de un SMA o TNC. No pudiéndose conectar directamente el cable de la antena al equipo *wireless* con conector distinto.

Figura 35. ***Pigtail***

Fuente: http://5nd.net/. Consulta 01/12/10.

- Otros equipos y accesorios:

Amplificadores, estos producen un incremento significativo en el alcance de las redes inalámbricas, al aumentar la potencia efectiva de salida del equipo hacia la antena, consiste en un receptor de bajo ruido preamplificado y un

amplificador lineal de salida de RF (radio frecuencia). Es a prueba de agua y tiene protección contra rayos. La potencia encontrada en el mercado es de 500 mili *watts*, 1, 2, 3 *watts*.

Figura 36. **Diferentes tipos de amplificadores**

Fuente: http://5nd.net/. Consulta 02/12/10.

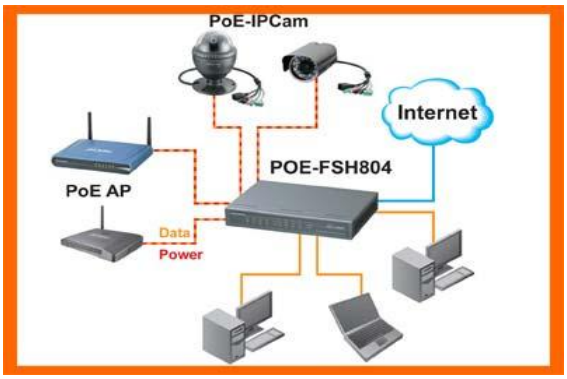
Protector de rayos, llamados también arrestores; están diseñado para proteger dispositivos de electricidad estática y descargas eléctricas producidas por rayos.

Figura 37. **Tipos de arrestores**

Fuente: http://5nd.net/. Consulta 02/12/10.

PoE (*Power Over Ethernet*), mediante este sistema algunos equipos inalámbricos *(access point)* pueden recibir a través del cable UTP, datos y energía eléctrica. No todos los equipos soportan PoE por lo tanto hay que tener cuidado al implementar este sistema en la configuración de una red inalámbrica.

Figura 38. **Diagrama de conexión de un dispositivo PoE**



Fuente: www.forpas.us.es/aula/hardware/PoE. Consulta 02/12/10.

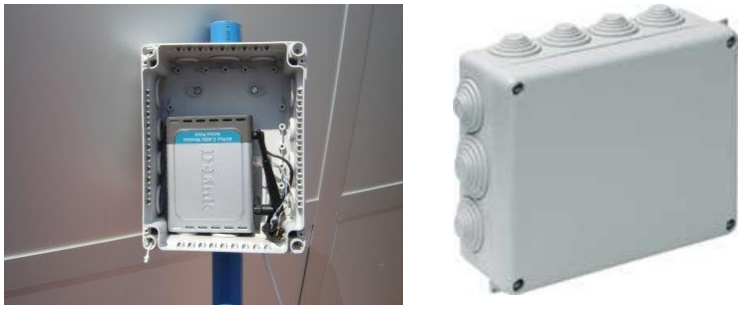
Splitter, este es un divisor de señal mediante este se podrá conectar más de una antena al *Access Point* se pueden encontrar de 2, 3, y 4 salidas.

Figura 39. **Tipos de *Splitters***

Fuente: http://5nd.net/. Consulta 02/12/10.

Caja estanca (*Weather Proof*), es una caja hermética donde se colocan los equipos sobre la torre para protegerlos de las inclemencias del clima como la lluvia, humedad, sol, etc. Permiten que se conserven y funcionen adecuadamente. Se pueden encontrar desde muy sencillas hasta sofisticadas, con sistemas de ventilación.

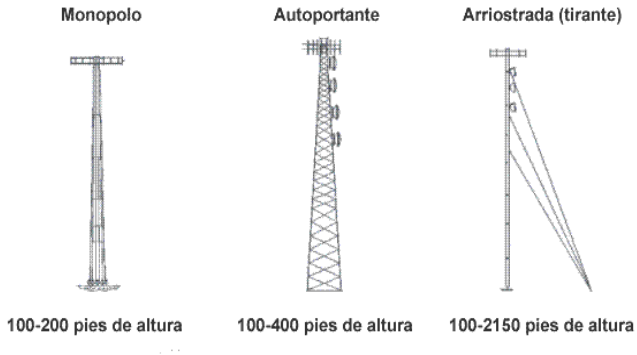
Figura 40. **Diferentes tipos de cajas estanca**



Fuente: *www.rittal*.com. Consulta 03/12/10.

Torre, es la estructura metálica donde se montará el equipo (antenas, *Access Point* y accesorios) para alcanzar línea de vista. Su altura depende de la altura a implementar.

Figura 41. **Tipos de antenas**



Fuente: *es.wikipedia.org/wiki/Antena.* Consulta 03/12/10.

3.4.1. Productos inalámbricos profesionales

Los productos profesionales proporcionan infraestructuras de conectividad con equipamientos líderes en soluciones de infraestructura inalámbrica que le permitirán tener una red completamente inalámbrica a nivel conectividad, tanto para voz como para datos.

Cuando se compare el equipamiento inalámbrico para ser usado en una red, deben considerarse estas variables:

Interoperabilidad, ¿el equipamiento que está considerando funcionará con el de otros fabricantes? Si no es así, ¿es un factor importante para este segmento de su red? Si el equipo en cuestión soporta un protocolo abierto (como el 802.11b/g), entonces probablemente va a funcionar con equipamiento de otras fuentes.

Rango, el rango no es algo inherente a una pieza particular del equipo. El rango de un dispositivo depende de la antena conectada a él, el terreno que lo rodea, las características del dispositivo en el otro extremo del enlace, además de otros factores. En lugar de confiar en el valor del rango semificticio provisto por el fabricante, es más útil conocer la potencia de transmisión del radio así como la ganancia de la antena (si está incluida la antena). Con esta información se podrá calcular el rango teórico.

Sensibilidad del radio, ¿cuán sensible es el dispositivo de radio a una tasa de transferencia dada? El fabricante debe proveer esta información, al menos a las velocidades más rápidas y más lentas. Esto puede utilizarse como una medida de la calidad del equipo, le permite completar el cálculo del

costo del enlace. Mientras más bajo sea este valor mejor será la sensibilidad del radio.

Rendimiento, los fabricantes sistemáticamente ponen la tasa de transferencia más alta posible como la velocidad de su equipo. Se deben tener en mente que el valor de la tasa de transferencia del radio nunca es el verdadero rendimiento del dispositivo. Si la información del rendimiento no está disponible para el dispositivo que se está evaluando, un buen truco es dividir la velocidad del dispositivo por dos, y restar el 20% más o menos. Si se tiene dudas, realizar la prueba de rendimiento en una unidad de evaluación antes de comprometerse a adquirir una gran cantidad de equipamiento que no especifica una tasa de rendimiento oficial.

Accesorios requeridos, para mantener el precio inicial bajo, los vendedores a menudo quitan accesorios que se requieren para un uso normal. ¿El precio incluye todos los adaptadores de potencia? Las fuentes DC generalmente se incluyen; pero los inyectores de potencia para *Ethernet* (POE) en general no. Del mismo modo, debe revisarse dos veces los voltajes de entrada, ya que el equipo normalmente viene con especificaciones de alimentación correspondiente a los estándares utilizados en los Estados Unidos. ¿Viene con los *pigtails*, adaptadores, cables, antenas, y las tarjetas de radio? Si se piensa usar en exteriores, ¿incluye el dispositivo una caja impermeable?

Disponibilidad, ¿va a ser capaz de reemplazar los componentes que se rompan? ¿puede ordenar esa parte en grandes cantidades? ¿el proyecto va a requerir esas partes? ¿cuál es el lapso de vida proyectado de este producto en particular, en términos de tiempo de funcionamiento en el campo y probabilidad de que el vendedor lo siga suministrando?

Otros factores, asegurarse de que se provean otras características importantes para satisfacer sus necesidades particulares. Por ejemplo, ¿incluye el dispositivo un conector para una antena externa? Si lo hace, ¿de qué tipo es? ¿existen limitaciones en número de usuarios o en el rendimiento impuestas por *software*, y si las hay, cuál es el costo de extender esos límites? ¿cuál es la forma física del dispositivo? ¿cuánta potencia consume? ¿soporta PoE como fuente de potencia? ¿provee encriptación, NAT, herramientas de monitoreo de ancho de banda, u otras características críticas para el diseño de la red?

Contestando estas preguntas primero, se va a poder tomar decisiones inteligentes de compra, cuando sea el momento de elegir el equipamiento profesional de la red.

3.4.2. Soluciones comerciales Vs Soluciones DIY (Haciéndolo usted mismo)

La amplia experiencia y capacidad de innovación de las empresas fabricantes, extienden exitosas redes inalámbricas para empresas, proveedores de servicios y gobiernos en todo el mundo. Los productos de redes inalámbricas están específicamente diseñados para rendimiento, confiabilidad e interconectividad en interiores y exteriores.

Las compañías que han optado por implementar la tecnología inalámbrica, como extensión de su infraestructura alámbrica, frecuentemente mencionan las ventajas de la productividad que resultan de trabajar con PC portátiles. En otro informe dirigido específicamente a las pequeñas y medianas empresas, se recomendó instalar una red inalámbrica en lugar de una LAN alámbrica en las pequeñas oficinas y lugares temporales que no tengan una

red, pero que necesiten una. ¿Cuáles son las razones? Las redes inalámbricas son menos costosas de instalar que otras alternativas inalámbricas. Algunos informes han estimado que la eliminación del cableado ahorra a las empresas entre 150 y 350 dólares americanos por usuario.

Según las estadísticas compiladas por la Asociación de redes LAN inalámbricas (*Wireless LAN Association*), el 97% de los clientes dijo que las redes LAN inalámbricas satisfacían o sobrepasaban las expectativas de proporcionar a sus compañías una ventaja competitiva, mientras que los beneficios cuantificados de la productividad constituyeron el 48% del retorno total de la inversión. Son cifras relevantes; también se debe tener en cuenta que los precios para *hardware* inalámbrico continúan descendiendo y no es de extrañar que la tecnología móvil se convierta en una opción viable que vaya creciendo día con día.

La fortaleza principal de las soluciones comerciales es que ellas proveen soporte y garantía de equipamiento (usualmente limitada). También tienen una plataforma consistente que tiende a que las instalaciones de red sean muy estables y a menudo intercambiables.

Si una parte del equipamiento no funciona, es difícil de configurar, o tiene problemas, un buen fabricante puede asistir a quien lo adquiere. Si en uso normal el equipamiento falla (excluyendo daños extremos, como los ocasionados por la caída de un rayo), el fabricante lo va a reemplazar. La mayoría ofrece esos servicios por un tiempo limitado como parte del precio de compra, y otros brindan soporte y garantía por un período de tiempo extendido mediante el pago de una cuota mensual. Teniendo una plataforma consistente, es sencillo tener los repuestos a mano y simplemente cambiar el equipo que falla, sin la necesidad de un técnico que configure el equipo.

Evidentemente, esto viene de la mano de un costo inicial más alto si se compara con los componentes disponibles localmente.

Desde el punto de vista de un arquitecto de red, los tres grandes riesgos ocultos al elegir soluciones comerciales son: quedar atrapado con un proveedor, que las líneas de productos estén descontinuadas, y los costos de licenciamiento futuro.

Deben comprenderse los términos de uso de cualquier equipamiento que se adquiera, incluyendo las futuras cuotas de licenciamiento.

Soluciones DiY, usando equipamiento genérico que soporta estándares abiertos y *software* de fuente abierta, se pueden evitar algunos de estos riesgos. Por ejemplo, es muy difícil verse atrapado por un proveedor que utiliza protocolos abiertos (tales como TCP/IP sobre 802.11a/b/g). Es recomendable utilizar protocolos patentados y espectro con licenciamiento solo en casos donde el equivalente abierto (como el 802.11a/b/g) no es viable técnicamente.

Si bien los productos individuales pueden discontinuarse en cualquier momento, se puede limitar el impacto que esto va a tener en la red utilizando componentes genéricos. La idea es utilizar componentes genéricos para construir un nodo inalámbrico completo.

Está claro que, no va a haber costos de licenciamiento en cuanto al *software* libre. La desventaja de utilizar *software* libre y equipamiento genérico es claramente una cuestión de soporte. Esto a veces se logra consultando recursos gratuitos en línea y motores de búsqueda, y aplicando los parches al código directamente.

Si no se tiene ningún miembro en el equipo que sea competente en el tema y se dedique a diseñar soluciones a los problemas de comunicación, entonces poner en marcha un proyecto de red, puede tomar una cantidad considerable de tiempo. Realizar el trabajo por uno mismo, seguramente va a resultar un gran desafío. Se necesita encontrar un balance entre el enfoque de las soluciones comerciales y las hechas por la empresa, que funcionen de forma adecuada al proyecto.

En resumen, se debe definir primero el objetivo de la red que se va a instalar; luego identificar los recursos que se pueden tener para lidiar con el problema, y permitir que la selección del equipamiento emerja naturalmente de esos resultados.

Deben considerarse las soluciones comerciales, así como los componentes abiertos, manteniendo siempre en mente los costos a largo plazo de ambas.

3.4.3 Construyendo un AP con un PC

Antes de empezar, se necesitará tener un portátil con Wi-Fi integrado o con alguna bahía PCMCIA (también se puede usar una PDA), para poder introducir en ella una tarjeta Wi-Fi. Es recomendable que las tarjetas que se utilicen tengan la posibilidad de conectarles una antena externa, ya que ello facilitará la tarea en el rastreo para descubrir redes a cierta distancia.

Las antenas que se usen es decisión particular; existen ya antenas comercializadas especiales para estas prácticas, aunque lo más divertido y económico es hacerse una.

Las plataformas que se utilizan son GNU/Linux, ya que este sistema ofrece herramientas muy versátiles.

Las tarjetas Wi-Fi, tienen dos formas de funcionamiento: como cliente punto a punto, y como convertidor del computador en un punto de acceso, para que pueda funcionar sobre Linux−*box* en modo monitor. De esta manera permitirá, como el mismo indica, poner la tarjeta en modo de monitorización para detectar conexiones *Wireless.*

Para saber si la tarjeta funciona en el sistema GNU/Linux en modo monitor, se tiene que comprobar con la siguiente línea de mandato:

```
$iwpriv eth0
Eth0    Available private ioctl :
        Force_reset     (8BE0) : set 0          & get 0
        card_reset      (8BE1) : set 0          & get 0
        set_port3       (8BE2) : set 1  int     & get 0
        get_port3       (8BE3) : set 0          & get 1 int
        set_preamble    (8BE4) : set 1  int     & get 0
        get_preamble    (8BE5) : set 0          & get 1 int
        set_ibssport    (8BE6) : set 1  int     & get 0 int
        get_ibssport    (8BE7) : set 0          & get 1 int
        monitor         (8BE8) : set 2          & get 0
        dump_recs       (8BFF) : set 0          & get 0
```

Suponiendo, claro está eth0, como el dispositivo Wi-fi. La información que interesa que aparezca es la que indica el valor monitor. Si la tarjeta no soporta ese modo en Linux (generalmente suele pasar en las que tienen el chip Hermes, tarjetas Orinoco o Avaya), tocará compilar un nuevo kernel y parchear los módulos del paquete pcmcia−cs.

Se utilizarán la plataformas Debian/Ubuntu para hacer un *Access Point* o *Wireless Router* con una tarjeta Wi-Fi.

Cuántas veces se ha querido compartir internet sin tener que hacer un tendido de red y no se dispone tampoco un *wireless router* pero gracias a *hostapd*, un demonio que permite poner muchas tarjetas Wi-Fi en modo máster (le permite actuar a la tarjeta Wi-Fi como un punto de acceso AP). *Hostapd* permite crear un AP con conexión incluso encriptada en seguridad WPA2; el alcance de señal viene dado por el que posea el dispositivo. Para GNU/Linux soporta todos los dispositivos cuyos módulos de kernel sean dependientes del driver mac80211.

Para saber que esta tarjeta depende del driver se debe poner en la consola:

sudo su
lsmod |grep mac80211

Y si se obtiene algo parecido a esto:

mac80211 154480 1 ath9k
cfg80211 119060 3 ath9k,mac80211,ath

Es que se tiene soporte.

Para el siguiente paso se utiliza una tarjeta wireless Atheros a/b/g/n cuyo lspci es:

07:00.0 Network controller: Atheros Communications Inc. Device 002a (rev 01)

Una vez que se sabe que el dispositivo es dependiente del *driver* mac80211 se instalan los paquetes necesarios:

```
sudo su
apt-get install firestarter dhcp3-server hostapd bridge-utils wireless-tools
```

Se reinicia el equipo, debido a que *hostapd* lo requiere para cargar módulos en el kernel (esto es necesario solo la primera vez), luego se procede a editar los archivos de configuración necesarios.

```
nano /etc/network/interfaces
```

Este archivo permite definir un dispositivo que actúa como puente o *switch* virtual con una IP por defecto que será para asignar las IPs dinámicas en la red, sea LAN o WLAN, para ello se edita de la siguiente manera:

```
# The loopback network interface
auto lo
iface lo inet loopback
auto br0
iface br0 inet static
address 192.168.0.1
network 192.168.0.0
netmask 255.255.255.0
broadcast 192.168.0.255
bridge-ports wlan0 eth0
```

Si se desea solo compartir por el dispositivo Wi-Fi, se debe dejar así:

```
# The loopback network interface
auto lo
iface lo inet loopback
```

auto wlan0
iface wlan0 inet static
address 192.168.0.1
network 192.168.0.0
netmask 255.255.255.0
broadcast 192.168.0.255

Se reinicia el demonio para que la configuración tenga efecto:

/etc/init.d/networking restart

Y se verifica con:

ifconfig
brctl show

Si se desea solo compartir por el dispositivo Wi-Fi se debe comprobar así:

ifconfig wlan0

nano /etc/default/dhcp3-server

Este archivo permitirá definir qué interfaz es la que será utilizada para asignar las direcciones IP. Se modifica la siguiente línea:

INTERFACES="br0"

Si se desea solo compartir por el dispositivo Wi-Fi se debe dejar así:

INTERFACES="wlan0"

nano /etc/dhcp3/dhcpd.conf

Este archivo permitirá definir el rango de IPs y los parámetros de red de cada cliente que se conecte a la LAN o WLAN, para ello editamos y dejamos de la siguiente manera:

DHCP configuration
ddns-update-style interim;
ignore client-updates;
subnet 192.168.0.0 netmask 255.255.255.0 {
option routers 192.168.0.1;
option domain-name-servers 10.2.21.13, 201.219.1.19;
option ip-forwarding on;
range dynamic-bootp 192.168.0.10 192.168.0.15;
default-lease-time 21600;
max-lease-time 43200}

Tómese en cuenta que *option domain-name-servers* debe tener las IPs de DNS de su ISP separado por comas, la manera más fácil de ver cuáles son los DNS del ISP es conectarse al internet y revisar el archivo */*etc/resolv.conf; los DNS son aquellas IPs después de la palabra *nameserver*.

Se reinicia el demonio para que la configuración tenga efecto:

/etc/init.d/dhcp3-server restart

nano /etc/sysctl.conf

Con este paso se habilita el kernel para que múltiples equipos salgan a Internet. Se edita y activa lo siguiente:

net.ipv4.conf.forwarding=1

Si todo esto pareció muy difícil, se puede usar *Firestarter*. Se debe estar conectado a Internet. Ya sea que desee compartir Internet tanto para la LAN como para WLAN, o solo por WLAN, es necesario que se tenga ya configurado el caso correspondiente con el paso de nano /etc/*network*/interfaces para proseguir con *firestarter.*

Para ejecutar *firestarter* en consola se debe poner lo siguiente:

sudo firestarter

Si es la primera vez, se ejecuta; se verá un asistente que se explicará a continuación, si no es ese el caso, en *Cortafuegos - Ejecutar Asistente* se halla el mismo.

Se da clic en Adelante. Se selecciona el dispositivo de salida a Internet, en este caso ppp0.

Se marca los *checkbox*, se da clic en Adelante, y se activa el *checkbox.* Se selecciona el dispositivo de área local, br0 o wlan0, según sea el caso. Se da clic en Adelante, y luego en Guardar.

A continuación se debe dirigir a *Editar -> Preferencias*; en la nueva ventana se debe dirigir a *Cortafuegos -> Configuraciones de red* y activar el *checkbox Activar DHCP para la red local*. Se da clic en Detalles del servidor DHCP**,** se marca en *Crear una configuración DHCP nueva* y en IP más baja se coloca una IP mayor a 192.168.0.0 y en IP más alta, una IP menor a 192.168.0.255**.**

Se da clic en *Aceptar*. Se detiene e inicia *Firestarter* y se continúa este

como:

nano /etc/default/hostapd

Este archivo permite establecer si quiere que *hostapd* funcione como demonio y qué archivo de configuración debe tomar para correr.

Se edita y activa lo siguiente:

RUN_DAEMON="yes"
DAEMON_CONF="/etc/hostapd/hostapd.conf"
nano /etc/hostapd/hostapd.conf

El archivo por defecto incluye mucha documentación importante acerca de sí mismo. Aquí se definen los parámetros de la red WLAN que se creará. La configuración ejemplo con WPA2 es:

interface=wlan0
driver=nl80211
bridge=br0
hw_mode=g
channel=1
ssid=mac80211 test
wpa=2
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_passphrase=12345678

Si se desea dejar la conexión abierta puede hacerse así:

interface=wlan0
driver=nl80211

bridge=br0
hw_mode=g
channel=1
ssid=mac80211 test

Si se desea sólo compartir por el dispositivo Wi-F, debe quitarse la línea bridge=br0 por ser un parámetro, únicamente en caso de que el dispositivo Wi-Fi sea parte de un bridge.

Se reinicia el demonio para que la configuración tenga efecto:

/etc/init.d/hostapd restart

Una vez terminado, se ejecuta lo siguiente:

sudo iptables -t nat -A POSTROUTING -o ppp0 -s 192.168.0.0 -j MASQUERADE

Tomando en cuenta que ppp0 es el dispositivo que se conecta a Internet y que 192.168.0.0 es la red tanto del bridge como del DHCP *server*.

Debe agregarse una tarjeta inalámbrica y un dispositivo *Ethernet* a una PC, corriendo Linux, le dará una herramienta muy flexible que puede ayudarlo a repartir el ancho de banda y administrar su red a un costo muy bajo. El equipamiento puede ser desde una computadora portátil reciclada, o una computadora de escritorio, hasta una computadora embebida, tales como un equipo de red *Linksys WRT54G* o *Metrix*.

4. ANÁLISIS DE DISEÑO Y SEGURIDAD DE UNA RED INALÁMBRICA

A pesar de los riesgos existentes, hay soluciones y mecanismos de seguridad para impedir que puedan introducirse en la red; para el diseño de una red inalámbrica, lo importante es la seguridad que se le brinda al cliente.

La seguridad en las redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite. Sin embargo, la gran cantidad de las redes inalámbricas actualmente instaladas, no tienen configurada seguridad alguna o poseen un nivel de seguridad muy débil, con lo cual se está poniendo en peligro la confidencialidad e integridad de dicha información.

Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas. Su implementación depende del uso que se vaya a dar a la red (casera o empresarial), de si es una red ya existente o una nueva, y del presupuesto del que se disponga para implantarla, entre otros factores.

La restricción de acceso mediante direcciones MAC es insuficiente para cualquier red, dado el gran número de herramientas disponibles libremente para cambiar la dirección MAC de una tarjeta cualquiera.

El método mediante WEP con clave estática es el mínimo nivel de protección que existe. En una red casera puede ser suficiente; en una corporativa, el uso de WEP está formalmente desaconsejado, por la facilidad con la que se pueden romper las claves WEP en un entorno de alto tráfico.

El uso de las VPN es una alternativa interesante cuando ya se tiene una red inalámbrica, y no se posee *hardware* inalámbrico que soporte el protocolo 802.1x. Requiere de la instalación de *software* especializado en los clientes inalámbricos y de un servidor o una serie de servidores que manejen las tareas de cifrado de datos, autenticación y autorización de acceso.

La alternativa de 802.1x y EAP es la adecuada, si los equipos de la red inalámbrica se pueden actualizar, o si se va a montar una red nueva. Puede usarse la solución de WEP con clave dinámica, o la de WPA; ambas ofrecen un excelente grado de protección.

Finalmente, todo mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada. El seguimiento de una política consistente evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, y garantiza la calidad y confidencialidad de la información presente en los sistemas de la empresa.

Para considerar una red inalámbrica como segura, debería cumplir con los siguientes requisitos:

Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.

Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella. Los datos deben viajar

cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

4.1. Topología de un diseño

La topología de una red representa la disposición de los enlaces que conectan los nodos de la misma. Las redes pueden tomar muchas formas diferentes dependiendo de cómo están interconectados los nodos. Hay dos formas de describir la topología de una red: física o lógica. La topología física se refiere a la configuración de cables, antenas, computadores y otros dispositivos de red, mientras la topología lógica hace referencia a un nivel más abstracto, considerando por ejemplo el método y flujo de la información transmitida entre nodos.

Topologías de red relevantes en conexión de redes inalámbricas

A continuación se hacen algunas observaciones generales que ayudarán a entender cómo y por qué algunas topologías de red, pueden o no, ser aplicadas a redes inalámbricas. Estas observaciones pueden sonar triviales, pero su comprensión es fundamental para lograr la implementación de una red inalámbrica exitosa.

La comunicación inalámbrica no requiere de cables pero tampoco necesita de algún otro medio, aire, éter u otra sustancia portadora. Una línea dibujada en el diagrama de una red inalámbrica, es equivalente a una (posible) conexión que se está realizando, no a un cable u otra representación física.

La comunicación inalámbrica se da siempre es en dos sentidos (bidireccional).

No hay reglas sin excepción, en el caso de "*sniffing*" (monitoreo) completamente pasivo o *eavesdropping* (escucha subrepticia), la comunicación es no bidireccional. Esta bidireccionalidad existe bien sea que se refiera a transmisores o receptores, maestros o clientes.

4.1.1. Modo *AD – HOC*

Modo ad hoc (IBSS): también conocido como punto a punto, es un método para que los clientes inalámbricos puedan establecer una comunicación directa entre sí. Al permitir que los clientes inalámbricos operen en modo ad hoc, no es necesario involucrar un punto de acceso central. Todos los nodos de una red ad hoc se pueden comunicar directamente con otros clientes.

Cada cliente inalámbrico en una red ad hoc debería configurar su adaptador inalámbrico también en modo *ad hoc* y usar los mismos SSID y "número de canal" de la red. Una red ad hoc normalmente está conformada por un pequeño grupo de dispositivos dispuestos cerca unos de otros. En una red ad hoc el rendimiento es menor a medida que el número de nodos crece.

El término *ad hoc* significa "para esto", pero se usa comúnmente para describir eventos o situaciones improvisadas y a menudo espontáneas.

En redes IEEE 802.11 el modo *ad hoc* se denota como Conjunto de Servicios Básicos Independientes (IBSS -*Independent Basic Service Set*).

Puede usarse el servicio punto a punto, el cual utiliza el modo *ad hoc* cuando desea conectar directamente dos estaciones, de edificio a edificio.

También puede instalarse dentro de una oficina entre un conjunto de estaciones de trabajo.

Si un nodo está conectado a la red (*Intranet* o Internet), puede extender dicha conexión a otros que se conecten a él inalámbricamente en el modo ad hoc, si se le configura para esta tarea.

4.1.2 Modo infraestructura

Infraestructura (BSS), contrario al modo *ad hoc* donde no hay un elemento central, en el modo de infraestructura hay un elemento de "coordinación": un punto de acceso o estación base. Si el punto de acceso se conecta a una red *Ethernet* cableada, los clientes inalámbricos pueden acceder a la red fija a través del punto de acceso. Para interconectar muchos puntos de acceso y clientes inalámbricos, todos deben configurarse con el mismo SSID. Para asegurar que se maximice la capacidad total de la red, no debe configurarse el mismo canal en todos los puntos de acceso que se encuentran en la misma área física.

Los clientes descubrirán (a través del escaneo de la red) cuál canal está usando el punto de acceso de manera que no se requiere que ellos conozcan de antemano el número de canal.

En redes IEEE 802.11 el modo de infraestructura es conocido como Conjunto de Servicios Básicos (BSS – *Basic Service Set*). También se conoce como Maestro y Cliente.

Estrella, la topología de estrella es con mucho, la infraestructura más común en redes inalámbricas. Es la tecnología típicamente usada para un

"*hotspot*" (punto de conexión a Internet), por ejemplo en aeropuertos o telecentros. Esta topología es la disposición típica de un WISP (*Wireless Internet Service Provider*).

A menudo este tipo de redes se combina en árboles o con elementos de otras topologías.

Punto a Punto (PtP), los enlaces punto a punto son un elemento estándar de la infraestructura inalámbrica. A nivel de topología estos pueden ser parte de una topología de estrella, de una simple línea entre dos puntos u otra topología. Un enlace punto a punto puede establecerse en modo ad hoc o infraestructura.

Una configuración típica de un enlace punto a punto. El modo puede ser ad hoc o infraestructura, pero los dos nodos deben utilizar el mismo modo y el mismo número de canal.

4.2. Seguridad física

La seguridad física hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático, para proteger *el hardware* de amenazas físicas. La seguridad física se complementa con la seguridad lógica. Los mecanismos de seguridad física deben resguardar de amenazas producidas tanto por el hombre como por la naturaleza. Básicamente, las amenazas físicas que pueden poner en riesgo un sistema informático son:

- Desastres naturales, incendios accidentales, humedad e inundaciones
- Amenazas ocasionadas involuntariamente por personas

- Acciones hostiles deliberadas como robo, fraude o sabotaje

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio, ha proporcionado nuevos riesgos de seguridad.

La salida de estas ondas de radio fuera del edificio donde está ubicada la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible de la empresa.

4.3. Amenazas a la red

Las amenazas a la seguridad de la información atentan contra su confidencialidad, integridad y disponibilidad. Existen amenazas relacionadas con falla humanas, con ataques malintencionados o con catástrofes naturales. Mediante la materialización de una amenaza podría ocurrir el acceso, modificación o eliminación de información no autorizada; la interrupción de un servicio o el procesamiento de un sistema; daños físicos o robo del equipamiento y medios de almacenamiento de información. Pueden citarse las siguientes:

Ingeniería social, consiste en utilizar artilugios, tretas y otras técnicas para el engaño de las personas, logrando que revelen información de interés para el atacante, como contraseñas de acceso. Se diferencia del resto de las amenazas, básicamente, porque no se aprovecha de debilidades y vulnerabilidades propias de un componente informático para la obtención de información.

Phishing, consiste en el envío masivo de mensajes electrónicos que fingen ser notificaciones oficiales de entidades/empresas legítimas con el fin de obtener datos personales y bancarios de los usuarios.

Escaneo de puertos, consiste en detectar qué servicios posee activos un equipo, con el objeto de ser utilizados para los fines del atacante.

Wardialers: se trata de herramientas de software que utilizan el acceso telefónico de una máquina para encontrar puntos de conexión telefónicos en otros equipos o redes, con el objeto de lograr acceso o recabar información.

Código malicioso / Virus, se define como todo programa o fragmento del mismo que genera algún tipo de problema en el sistema en el cual se ejecuta, interfiriendo de esta forma con el normal funcionamiento del mismo. Existen diferentes tipos de código malicioso; a continuación mencionamos algunos de ellos:

Bombas lógicas, se encuentran diseñados para activarse ante la ocurrencia de un evento definido en su lógica.

Troyanos, suelen propagarse como parte de programas de uso común y se activan cuando los mismos se ejecutan.

Gusanos, tienen el poder de autoduplicarse causando efectos diversos.

Cookies, son archivos de texto con información acerca de la navegación efectuada por el usuario en Internet e información confidencial del mismo, que pueden ser obtenidos por atacantes.

Keyloggers, es una aplicación destinada a registrar todas las teclas que un usuario typea en su computadora; algunos de ellos además registran otro tipo de información útil para un atacante, como imágenes de pantalla.

Spyware, aplicaciones que recogen y envían información sobre las páginas web que más frecuentemente visita un usuario, tiempo de conexión, datos relativos al equipo en el que se encuentran instalados (sistema operativo, tipo de procesador, memoria, etc.) e, incluso, hay algunos diseñados para informar de si el software que utiliza el equipo es original o no.

Exploits, se trata de programas o técnicas que explotan una vulnerabilidad de un sistema para el logro de los objetivos del atacante, como ser, intrusión, robo de información, denegación de servicio, etc.

Ataque de contraseña**,** consiste en la prueba metódica de contraseñas para lograr el acceso a un sistema, siempre y cuando la cuenta no presente un control de intentos fallidos de logueo. Este tipo de ataques puede ser efectuado de las siguientes maneras:

Por diccionario**,** al existir un diccionario de palabras, una herramienta intentará acceder al sistema probando una a una las palabras incluidas en el diccionario.

Por fuerza bruta**,** una herramienta generará combinaciones de letras números y símbolos formando posibles contraseñas y probando una a una en el *login* del sistema.

Control remoto de equipos, un atacante puede tomar el control de un equipo en forma remota y no autorizada, mediante la utilización de programas

desarrollados para tal fin, e instalados por el atacante, mediante, por ejemplo, la utilización de troyanos.

*Eavesdropping***,** es un proceso por el cual un atacante capta información (cifrada o no) que no le iba dirigida. Existen diferentes tipos de técnicas que pueden utilizarse:

Sniffing, consiste en capturar paquetes de información que circulan por la red con la utilización de una herramienta para dicho fin, instalada en un equipo conectado a la red; o bien mediante un dispositivo especial conectado al cable. En redes inalámbricas la captura de paquetes es más simple, pues no requiere de acceso físico al medio. Relacionados con este tipo de ataque, pueden distinguirse también las siguientes técnicas:

*AIRsniffing***,** consiste en capturar paquetes de información que circulan por redes inalámbricas. Para ello es necesario contar con una placa de red *wireless* configurada en modo promiscuo y una antena.

War Driving y Netstumbling, estas técnicas se valen del *AIRsniffing*, ya que consisten en circular (generalmente en un vehículo) por un vecindario o zona urbana, con el objeto de capturar información transmitida a través de redes inalámbricas. Esto es posible debido a que generalmente las ondas de transmisión de información en redes inalámbricas se expanden fuera del área donde se ubican los usuarios legítimos de la red, pudiendo ser alcanzadas por atacantes. Lo que en ocasiones las hace más vulnerables es la falta de seguridad con que se encuentran implementadas.

Desbordamiento de CAM, se trata de inundar la tabla de direcciones de un *switch* con el objeto de bloquear la capacidad que éste posee de direccionar

cada paquete exclusivamente a su destino. De esta forma el atacante podrá efectuar *sniffing* de los paquetes enviados por un *switch*, cuando en condiciones normales un *switch* no es vulnerable a este tipo de ataques.

VLAN *hopping*, las VLANs son redes LAN virtuales las cuales se implementan para generar un control de tráfico entre las mismas, de manera que los equipos conectados a una VLAN no posean acceso a otras. Este tipo de ataque pretende engañar a un *switch* (sobre el cual se implementan VLANs) mediante técnicas de *Switch Spoofing* logrando conocer los paquetes de información que circulan entre VLANs.

*STP manipulation***,** este tipo de ataque es utilizado en topologías que cuentan con un árbol de *switches* que implementan el protocolo *Spanning Tree Protocol,* para coordinar su comunicación. El equipo atacante buscará convertirse en la raíz de dicho árbol, con el objeto de poder tener acceso a los paquetes de información que circulan por todos los *switches.*

Man-in-the-middle, el atacante se interpone entre el origen y el destino en una comunicación, pudiendo conocer y/o modificar el contenido de los paquetes de información, sin ser advertido por las víctimas. Esto puede ocurrir en diversos ambientes, como por ejemplo, en comunicaciones por *e-mail*, navegación en Internet, dentro de una red LAN, etc.

Defacement, consiste en la modificación del contenido de un sitio web por parte de un atacante.

IP Spoofing - MAC Address Spoofing, el atacante modifica la dirección IP o la dirección MAC de origen de los paquetes de información que envía a la red, falsificando su identificación para hacerse pasar por otro usuario. De esta

manera, el atacante puede asumir la identificación de un usuario válido de la red, obteniendo sus privilegios.

Repetición de transacción, consiste en capturar la información correspondiente a una transacción efectuada en la red interna o en Internet, con el objeto de reproducirla posteriormente. Esto cobra real criticidad en transacciones monetarias.

Backdoors, también denominados puertas traseras, consisten en accesos no convencionales a los sistemas, los cuales pueden permitir efectuar acciones que no son permitidas por vías normales. Generalmente son instalados por el atacante para lograr un permanente acceso al sistema.

DHCP Starvation, el atacante busca reemplazar al servidor DHCP que se encuentra funcionando en la red, de forma de asignar a los clientes direcciones IP y otra información (como ser el servidor *Gateway*) de acuerdo con su conveniencia. De esta forma podría luego simular ser el *Gateway* e interceptar la información que los clientes envíen, con el tipo de ataque *Man-in-the-middle.*

Trashing, consiste en la búsqueda de información dentro de la basura. Esto puede representar una amenaza importante para usuarios que no destruyen la información crítica o confidencial al eliminarla.

Denegación de servicio*,* su objetivo es degradar considerablemente o detener el funcionamiento de un servicio ofrecido por un sistema o dispositivo de red. Existen diferentes técnicas para la explotación de este tipo de ataques:

Envío de paquetes de información mal conformados de manera de manera que la aplicación que debe interpretarlo no puede hacerlo y colapsa.

Inundación de la red con paquetes (como ser ICMP - *ping*, TCP – SYN, IP origen igual a IP destino, etc.) que no permiten que circulen los paquetes de información de usuarios.

Bloqueo de cuentas por excesivos intentos de *login* fallidos.

Impedimento de logueo del administrador.

Denegación de servicio distribuida, su objetivo es el mismo que el perseguido por un ataque de denegación de servicio común, pero en este caso, se utilizan múltiples equipos para generar el ataque.

Fraude informático, se trata del perjuicio económico efectuado a una persona mediante la utilización de un sistema informático, ya sea, modificando datos, introduciendo datos falsos o verdaderos, o cualquier elemento extraño que sortee la seguridad del sistema.

Software Ilegal, consiste en la instalación de *software* licenciado sin contar con la licencia correspondiente que habilita su uso, o mediante la falsificación de la misma.

Acceso a información confidencial impresa, ocurre cuando información confidencial impresa es obtenida por personal no autorizado debido a que la misma no es resguardada adecuadamente, mediante por ejemplo, una política de limpieza de escritorios.

Daños físicos al equipamiento, los daños físicos pueden ser ocasionados por: acciones intencionadas, negligencia de los usuarios (ej.: derrame de

líquidos, golpes, etc.), y catástrofes naturales (ej.: fallas eléctricas, incendio, inundación, falta de refrigeración, etc.)

Robo de equipamiento o componentes, el robo puede involucrar todo un equipo o parte del mismo. Puede ocurrir por un deficiente control de acceso establecido al centro de cómputos (o recinto donde residen los equipos: servidores, *routers, switches*, etc.), así como a las propias instalaciones de la institución.

Pérdida de copias de resguardo, si no existen adecuadas medidas de seguridad física para las copias de resguardo, las mismas pueden dañarse; por ejemplo, en caso de ser afectadas por desastres como un incendio, inundación, o incluso por robo. Asimismo, una administración inadecuada de los medios físicos de almacenamiento puede provocar la obsolescencia de los mismos (ej.: reutilización excesiva de cintas).

4.4. Autenticación

Cuando se desea establecer una comunicación entre dos dispositivos, debe primero establecerse una *asociació*n. Para ello el cliente solicita la autenticación, y el Punto de Acceso responde identificando el tipo de autenticación presente en la red. Posteriormente, el cliente procede con la autenticación y, si es satisfactoria, se lleva a cabo la asociación.

El primer paso para poder autenticar un cliente en una red *Wireless* es el conocimiento del SSID *(Service Set Identifier*), que funciona de forma similar al concepto de comunidad en SNMP, es decir, para obtener acceso al sistema es necesario conocer el SSID.

El estándar 802.11b plantea dos posibles formas de autenticación:

*Open System***,** es el mecanismo de autenticación por defecto, y permite que cualquier estación se una al sistema tras la negociación de los parámetros de red necesarios, es decir, se utiliza autenticación NULA, en la que cualquier dispositivo puede obtener acceso a la red.

*Shared Key***,** se lleva a cabo mediante un mecanismo de desafío/respuesta cifrado, siendo necesario durante el proceso que ambas estaciones posean una clave común (autenticación simétrica). Para que una red 802.11b pueda utilizar este tipo de autenticación, debe emplear el protocolo WEP.

La mayoría de los protocolos basados en claves (*Passwords)* en uso hoy en día, dependen de lo complicada que sea la clave (*Password)* que utilice el usuario. El servidor provee de intentos de validación hacia el usuario solicitando una *password* que el cliente envía al servidor, validando éste la respuesta por parte del usuario contra dicha *password* que se encuentra en una base de datos. Esta aproximación de carácter general se describe en CHAP, MS-CHAP, MS-CHAP-V2, EAP/MD5-Challenge y en *EAP/One Time Password*.

El problema de esta aproximación es que si una persona no autorizada observa el proceso de envío y respuesta, puede montar lo que se llama un diccionario de ataque, en el cual los passwords aleatorios se testean contra las validaciones enviadas por los usuarios hacia los servidores, para tratar de averiguar cuáles son las respuestas correctas. Ya que normalmente los *passwords* tienen poca entropía, con estos ataques puede ser sencillo descubrir muchas *passwords.*

Mientras que esta vulnerabilidad ya ha sido bien entendida, no se le da importancia en entornos donde los ataques de personas no autorizadas se pueden producir, aunque sean poco probables. Por ejemplo, en conexiones en redes cableadas a través de software de *dialers* (*dial-up*) usando sus proveedores de servicio; los usuarios no le dan importancia de que estas conexiones puedan ser monitorizadas.

Los usuarios tienen buena voluntad al confiar sus *passwords* a los proveedores de servicios, o al menos permitiéndoles a éstos chequear el proceso de envío y respuesta de *passwords* ya que los proveedores de servicio reenvían estos a sus servidores locales de autenticación usando, por ejemplo, servidores *RADIUS*, sin que el usuario se preocupe de que los proveedores de servicio puedan montar diccionarios de ataque que puedan usar sobre las credenciales de usuario que están observando. Lo que sucede es que un usuario típico tiene relación con un único proveedor de servicio, por lo que este grado de confianza es enteramente aceptable.

Sin embargo, con el advenimiento de las redes inalámbricas, esta situación cambia dramáticamente. El legado al que predisponen los protocolos de *passwords* está sujeto a los usuarios no deseados además de los tipos que aparecen en medio de los ataques (“espías”). Un intruso que ataque una red inalámbrica puede montar un diccionario de ataque contra dichos protocolos de *passwords.* Además, el espía puede saltarse la autenticación íntegra, apropiarse de la conexión y actuar como si fuera un usuario.

Antes de tener acceso a los recursos de la red, los usuarios deben ser autenticados. En un mundo ideal, cada usuario inalámbrico debería tener un identificador personal que fuera único, inmodificable e imposible de suplantar

por otros usuarios. Este es un problema muy difícil de resolver en el mundo real.

Lo más cercano a tener un identificador único es la dirección MAC. Este es un número de 48-bits asignado por el fabricante a cada dispositivo inalámbrico y Ethernet. Empleando un filtro MAC en un punto de acceso, se puede autentificar a los usuarios mediante su dirección MAC.

Con este método el punto de acceso, mantiene una tabla de direcciones MAC aprobadas. Cuando un usuario intenta asociarse a un punto de acceso, la dirección MAC del cliente debe estar en la lista aprobada; de lo contrario, la asociación va a ser rechazada. Como una alternativa, el AP puede tener una tabla de direcciones MAC prohibidas, y habilitar a todos los dispositivos que no están en esa lista.

Desafortunadamente, este no es un mecanismo de seguridad ideal. Mantener las tablas MAC en cada dispositivo puede ser muy engorroso, requiriendo que todos los dispositivos cliente tengan su dirección MAC grabadas y cargadas en los AP. Además, las direcciones MAC a menudo pueden modificarse mediante software. Si un atacante determinado observa las direcciones MAC que están en uso en una red inalámbrica, él puede suplantar una dirección MAC aprobada y asociarse con éxito al AP. A pesar de que el filtro MAC va a evitar que los usuarios involuntarios y los curiosos accedan a la red, el filtro MAC por sí solo no puede proteger su red de los atacantes empecinados.

4.5. Privacidad

Otro asunto es la seguridad de la conexión de datos entre el cliente y el AP después de la autenticación. Aunque los clientes pueden negociar claves después de dicha autenticación, si estas no se encriptan relacionándose a la autenticación efectuada anteriormente, la sesión de transferencia de datos podría estar sujeta a espías. Por lo tanto es incumbencia en el proceso de la autenticación el disponer de claves que se puedan distribuir entre los clientes y los Aps que permitan que la subsiguiente conexión de datos se pueda encriptar.

Gran cantidad de usuarios ignoran que su correo electrónico privado, conversaciones en línea, y aún sus contraseñas, a menudo son enviadas al descubierto por docenas de redes inseguras antes de llegar a su destino en Internet. No obstante lo errados que pueden estar, en general, los usuarios tienen expectativas de un poco de privacidad cuando usan redes de computadoras.

La privacidad se puede lograr, aún en redes inseguras como los puntos de acceso público e Internet. El único método efectivo probado para proteger la privacidad es el uso de una encriptación fuerte de extremo a extremo.

Las técnicas de encriptación como WEP y WPA intentan mantener la privacidad en la capa dos, la cual tiene la función de enlace de datos. Aunque estas protegen de los fisgones en la conexión inalámbrica, la protección termina en el punto de acceso. Si el cliente inalámbrico usa protocolos inseguros (como POP o SMTP para recibir y enviar correos electrónicos), entonces los usuarios que están más allá del AP pueden registrar la sesión y ver los datos importantes. Como se mencionó antes, WEP también tiene la debilidad de utilizar claves privadas compartidas. Esto significa que los usuarios legítimos de

la red pueden escucharse unos a otros, ya que todos conocen la clave privada.

Utilizando encriptación en el extremo remoto de la conexión, los usuarios pueden eludir completamente el problema. Estas técnicas funcionan muy bien aún en redes públicas, donde los fisgones están oyendo y posiblemente manipulando los datos que vienen del punto de acceso.

Para asegurar la privacidad de los datos, una buena encriptación de extremo a extremo debe ofrecer las siguientes características:

Uso de encriptación**,** la manera más efectiva de proteger una red inalámbrica contra los intrusos, es encriptar o codificar las comunicaciones en red. La mayoría de los enrutadores inalámbricos, puntos de acceso y estaciones base, tienen un mecanismo de encriptación incorporado. Si el enrutador inalámbrico no tiene esta función de encriptación, debe conseguirse uno que sí la tenga.

Los fabricantes de enrutadores inalámbricos, frecuentemente despachan sus aparatos con la función de encriptación desactivada y el cliente debe activarla. En el manual de instrucciones del enrutador inalámbrico debería encontrarse la descripción del procedimiento para instalarla. Si no fuera así, puede consultarse el sitio Web del fabricante del enrutador.

Hay dos tipos principales de encriptación: Acceso Protegido para Transferencia Inalámbrica de Datos o WPA (por su acrónimo del inglés *Wi-Fi Protected Access*) y Equivalencia de Privacidad Inalámbrica o WEP (por su acrónimo del inglés *Wired Equivalent Privacy*). Cualquier computadora, enrutador y demás equipo, deben utilizar la misma encriptación. El sistema

WPA provee una encriptación más potente; si se tiene la opción, puede usarse este sistema ya que está diseñado para protegerlo contra la mayoría de los ataques de los *hackers*.

Algunos modelos más antiguos de enrutadores solamente ofrecen encriptación WEP, lo que es mejor que no tener ningún tipo de encriptación. Este sistema de encriptación o codificación debería proteger su red inalámbrica contra las intrusiones accidentales de vecinos o contra los ataques de *hackers* menos sofisticados. Si usa el sistema de encriptación WEP, debe configurarse al nivel de seguridad más alto.

Usar *software* antivirus y antiespía y también activar el *firewall*. Las computadoras conectadas a una red inalámbrica necesitan tener la misma protección que las computadoras conectadas a internet por medio de un cable. Se debe instalar en la computadora un software antivirus y antiespía y mantenerse actualizados. Si la computadora fue entregada con el firewall o cortafuegos desactivados, debe activarse.

Se desactiva el identificador de emisión. Casi todos los enrutadores inalámbricos (*wireless routers*) tienen un mecanismo llamado identificador de emisión (*identifier broadcasting*). Este mecanismo emite una señal a todas las terminales que estén en las cercanías anunciando su presencia.

No es necesario emitir esta información si la persona que está usando la red ya sabe que está disponible. Los *hackers* pueden usar el identificador de emisión para acceder a redes inalámbricas vulnerables. Si el enrutador inalámbrico lo permite, se debe desactivar el mecanismo del identificador de emisión, y cambiar la configuración predeterminada del identificador de su enrutador (*router's pre-set password for administration*). Probablemente, el

identificador del enrutador sea un código o nombre de identificación (ID) estándar predeterminado que fue asignado por el fabricante para todas las unidades de hardware de ese modelo.

Aunque el enrutador no esté emitiendo la señal de su identificador a todo el mundo, los *hackers* conocen los códigos o nombres de identificación predeterminados y pueden usarlos para intentar acceder a su red. Cambiar el identificador del enrutador por un código que solamente el usuario conozca, y recordar que para que el enrutador y su computadora puedan comunicarse entre sí, debe configurar el mismo código de identificación o ID en ambos. Usar una contraseña que tenga por lo menos 10 caracteres: cuanto más extensa sea la contraseña o código de identificación, más difícil resultará que los *hackers* logren acceder a su red.

Cambiar la contraseña predeterminada de instalación del enrutador: probablemente, el fabricante del enrutador inalámbrico asignó una contraseña estándar predeterminada (*pre-set password for administrator*) para permitir la instalación y operación del enrutador. Los *hackers* conocen estas contraseñas predeterminadas, por lo tanto, debe cambiarse por una contraseña nueva y que solamente el usuario conozca. Cuanto más extensa sea la contraseña, más difícil será descifrarla.

Solamente debe permitirse el acceso de la red inalámbrica a computadoras específicas. Cada computadora habilitada para comunicarse con una red tiene asignada una dirección exclusiva de Control de Acceso a Medios o MAC (por su acrónimo del inglés, *Media Access Control*). Generalmente, los enrutadores inalámbricos tienen un mecanismo que permite que solamente los aparatos con una dirección MAC particular puedan acceder a la red. Algunos

hackers han imitado domicilios MAC, por lo tanto no se debe confiar solamente en esta medida de protección.

Debe apagarse la red inalámbrica cuando se sepa que no se va a utilizar. Los *hackers* no pueden acceder a un enrutador inalámbrico cuando está apagado. Si se apaga el enrutador cuando no lo usa, se está limitando la cantidad de tiempo de vulnerabilidad a los ataques de los *hackers*.

No debe darse por supuesto que los *hot spots* públicos son seguros. Muchos bares, hoteles, aeropuertos y otros establecimientos públicos ofrecen redes inalámbricas para sus clientes. Estos *hot spots* o puntos de acceso a internet son convenientes, pero no siempre son seguros. Consulte con el propietario del establecimiento para verificar cuáles son las medidas de seguridad implementadas.

Debe tenerse cuidado con el tipo de información a la que se accede o se envía desde una red inalámbrica pública. Para evitar riesgos, debería tenerse en cuenta que otras personas pueden acceder a cualquier información que se vea o envíe a través de una red inalámbrica pública. A menos que se pueda verificar que un *hot spot* haya implementado medidas de seguridad efectivas, lo mejor es evitar el envío o recepción de información delicada a través de la red.

4.6. Monitoreo

Para poder ver si se tiene intrusos en la red puede hacerse de dos maneras: por casualidad, que la velocidad de internet sea baja, o preocupándose de los sistemas, instalando un programa, ya que es necesario para la detección de problemas y, sobre todo, para detectar tráfico no esperado, presencias de puertas traseras, escaneos y cualquier otra intrusión.

Monitorización activa, (Barrido activo) consiste en que el dispositivo de red inalámbrica envía un paquete sonda o baliza (*beacon frame*) al aire y en caso de existir un AP al que le llegue la señal, contestará con marco de respuesta sonda (*request frame*) que contiene los datos de la red.

Monitorización pasiva, implica la escucha del dispositivo de red inalámbrica en busca de marcos baliza que emiten los puntos de acceso.

Software para detectar redes inalámbricas:

Existen muchas herramientas para detectar redes inalámbricas. A continuación se mostraran algunas de las más destacadas por sus características y facilidades de uso.

NetStumbler, esta es una sencilla herramienta que permite detectar redes de área local sin cables (*Wireless Local Area Network*, WLAN), usando 802.11b, 802.11a y 802.11g. puede usarse para comprobar la integridad y correcto funcionamiento de una red inalámbrica, localizar zonas donde no haya cobertura, detectar otras redes que puedan estar interfiriendo o incluso descubrir puntos de acceso no autorizados.

No es necesario pagar una licencia para usarlo, es completamente gratuito. Además es muy útil para orientar antenas direccionales y es una de las herramientas más utilizadas en la búsqueda de redes inalámbricas (*Wardriving*). Este programa actualmente sólo está disponible para sistemas operativos Windows; aunque el autor también se distribuye una aplicación para WinCE, PDAs y similares llamada *MiniStumbler.*

Wellenreiter, esta es una herramienta muy útil para realizar penetraciones y auditorías a redes inalámbricas. Es capaz de detectarlas, mostrar información sobre el cifrado utilizado en la conexión, datos sobre el fabricante del dispositivo y la asignación de DHCP. También descifra el tráfico ARP para brindar más información sobre la red.

El inconveniente para los que usan *Windows* en sus estaciones de trabajo es que sólo funcionan con los sistemas operativos Linux, Mac OS y *FreeBSD.* Cuando se utiliza de conjunto con *Ethereal* o TCP*Dump*, logran una combinación perfecta para sistemas de auditorías de redes inalámbricas.

Boingo hot spots: este sitio cuenta con un buscador que tiene listados con más de 100,000 puntos de acceso alrededor de todo el mundo. Clasificado por países y por tipo de instalación (aeropuertos, cafeterías, playas, bares, etc.). De cada punto de acceso el directorio muestra la ubicación, su dirección exacta, costo de conexión por minuto, el tipo de instalación y tipo de conexión inalámbrica. Para los puntos de acceso ubicados en Estados Unidos se puede ver la ubicación del punto de acceso utilizando *Yahoo Local Maps*.

Lycos Wi-fi manager, con este *software* se podrán administrar las conexiones inalámbricas en el ordenador. Es una herramienta de uso gratuito y una de las características más importantes es que integra un buscador de puntos de accesos en España.

Visitando el sitio web de esta herramienta se podrá ver que han implementado un buscador de puntos de accesos en todos los países con una búsqueda muy personalizada y que muestra mucha información sobre éstos. También es posible conocer la ubicación exacta del *hotspot* a través de un mapa.

5. VENTAJAS Y DESVENTAJAS DE UNA RED INALÁMBRICA

Las redes Wi-Fi tienen la ventaja de una implantación sin infraestructura aportando la flexibilidad necesaria para adecuarse a las necesidades de una empresa y las de sus clientes. Pero también posen ciertos inconvenientes.

5.1. Comparando todas las tecnologías

IrDA vs. RF (I)

infrarrojos:

- Ventajas:
    - Emisores y receptores muy simples y baratos
    - No interfiere con otros dispositivos de RF
- Desventajas:
    - Poco ancho de banda
    - Necesidad de comunicación visual

Esta es una desventaja importante. Por ejemplo, no se podría comunicar una computadora en una sala con una impresora que esté en otra sala. Esto limita mucho las posibilidades de comunicación entre dispositivos y da un aspecto de comunicación de juguete, habitualmente, comunicaciones sólo entre 2 interlocutores.

IrDA vs. RF (II)

Radiofrecuencia

- Ventajas:
    - Mayor área de cobertura
    - No necesita comunicación visual entre dispositivos
    - Mayor ancho de banda
- Desventajas:
    - Difícil de apantallar -> Interferencias

No solo interferencias entre diferentes dispositivos conectados a una red, sino también entre otro tipo de dispositivos independientes que generen campos electromagnéticos, por ejemplo, microondas.

Rango de frecuencias limitado, el espectro radioeléctrico está ocupado casi al 100 % así que se buscan espacios; pero como la gestión del espacio radioeléctrico es distinta en cada país, surgen dificultades en su estandarización en una determinada tecnología. Datos obtenidos en el año 2010

Tabla XII. **Comparación tecnologías y precios**

Estándar	Tasa de transferencia	Banda de frecuencia	Precio tarjeta	Precio P. Acceso
802.11	2 Mbit/s	2.4 GHz	N/D	N/D
802.11b	11 Mbit/s	2.4 GHz	Q1053	Q2100
802.11a	54 Mbit/s	5 GHz	Q1500	Q3300
802.11g	54 Mbit/s	2.4 GHz	N/D	N/D

Fuente: http://www.monografias.com/trabajos60/wimax-banda-ancha/wimax-banda-ancha2.shtml. Consulta 08/12/10.

5.2. Definiendo ventajas

Flexibilidad**,** dentro de la zona de cobertura de la red inalámbrica, los nodos se podrán comunicar y no estarán atados a un cable para poder estar comunicados por el mundo.

Poca planificación**,** respecto de las redes cableadas. Antes de cablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas, mientras que con una red inalámbrica sólo habrá que preocuparse de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.

Diseño, los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo, etc.

Robustez, ante eventos inesperados que pueden ir desde un usuario que se tropieza con un cable o lo desenchufa, hasta un pequeño terremoto o algo similar. Una red cableada podría llegar a quedar completamente inutilizada, mientras que una inalámbrica puede aguantar bastante mejor este tipo de percances inesperados.

Movilidad, la libertad de movimiento es uno de los beneficios más evidentes de las redes inalámbricas. Un ordenador o cualquier otro dispositivo puede situarse en cualquier otro punto dentro del área de cobertura de la red sin tener que depender de que si es posible o no hacer llegar un cable hasta ese sitio. Ya no es necesario estar atado a un cable para navegar en Internet, imprimir un documento o acceder a los recursos compartidos desde cualquier lugar de la red, hacer presentaciones en la sala de reuniones, acceder a archivos, etc.

Portabilidad, con una computadora portátil o PDA no solo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que puede haber desplazamiento sin perder la comunicación. Esto no solo da cierta comodidad, sino que facilita el trabajo en determinadas tareas.

Escalabilidad, es la facilidad de expandir la red después de su instalación inicial. Conectar una nueva computadora cuando se dispone de una red inalámbrica es algo tan sencillo.

5.3. Definiendo desventajas

Evidentemente, como todo en la vida, no todo son ventajas. Las redes inalámbricas también tienen unos puntos negativos en comparación con las redes cableadas. Los principales inconvenientes de las redes inalámbricas son:

Menor velocidad**,** las redes de cable actuales trabajan a velocidades de 100 Mbps hasta 10 000 Mbps, mientras que las redes inalámbricas Wi-Fi trabajan de 11 a 108 Mbps. Es cierto que existen estándares y soluciones propietarias que llegan a mejores velocidades, pero estos estándares están en los comienzos de su comercialización y tienen un precio superior al de los actuales equipos Wi-Fi.

Más inversión inicial, para la mayoría de las configuraciones de la red local, el costo de los equipos de red inalámbricos es superior al de los equipos de red cableada.

Soluciones propietarias, como la estandarización está siendo bastante lenta, ciertos fabricantes han sacado al mercado algunas soluciones

propietarias que sólo funcionan en un entorno homogéneo y por lo tanto estando atado a ese fabricante. Esto supone un gran problema ante el mantenimiento del sistema, tanto para ampliaciones del mismo, como para la recuperación ante posibles fallos. Cualquier empresa o particular que desee mantener su sistema funcionando se verá obligado a acudir de nuevo al mismo fabricante para comprar otra tarjeta, punto de enlace, etc.

Restricciones, estas redes operan en un trozo del espectro radioeléctrico. Este está muy saturado hoy día y las redes deben amoldarse a las reglas que existan dentro de cada país. Concretamente en España, así como en Francia y en Japón, existen unas limitaciones en el ancho de banda a utilizar por parte de ciertos estándares.

Seguridad en dos vertientes, por una parte seguridad e integridad de la información que se transmite. Este campo está bastante criticado en casi todos los estándares actuales, que, según dicen no se debe utilizar en entornos críticos en los cuales un robo de datos pueda ser peligroso. Por otra parte, este tipo de comunicación podría interferir con otras redes de comunicación (policía, bomberos, hospitales, etc.) y esto hay que tenerlo en cuenta en el diseño.

5.4. Ventajas y desventajas de una red inalámbrica frente a una red cableada convencional

Es clara la alta dependencia en los negocios de la redes de comunicación. Por ello la posibilidad de compartir información sin que sea necesario buscar una conexión física permite mayor movilidad y comodidad.

Asimismo, la red puede ser más extensa sin tener que mover o instalar cables. Respecto de la red tradicional, la red sin cable ofrece las siguientes ventajas:

Movilidad, información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. El que se obtenga en tiempo real supone mayor productividad y posibilidades de servicio.

- Facilidad de instalación, evita obras para tirar cable por muros y techos.
- Flexibilidad, permite llegar donde el cable no puede.
- Escalabilidad, el cambio de topología de red es sencillo y trata igual tanto a pequeñas como a un gran conjunto de redes.

Las redes WLAN también, presentan alguna desventaja, o más bien inconveniente, "baja" velocidad que alcanzan, por lo que su éxito comercial es más bien escaso y, hasta que los nuevos estándares no permitan un incremento significativo, no es de prever su uso masivo, ya que por ahora no pueden competir con las LAN basadas en cable.

Las redes alámbricas proporcionan a los usuarios una buena seguridad y la capacidad de mover muchos datos de manera rápida y efectiva. Son más rápidas que las redes inalámbricas y más económicas de implementar.

Sin embargo el costo de las redes alámbricas puede crecer entre más computadoras sean y más retiradas se encuentren entre ellas. Además, a menos que se esté construyendo una casa o edificio nuevo y se planee con anticipación la instalación del cableado, se tendrá que perforar paredes y conformarse con una instalación visible.

CONCLUSIONES

1. Cuando la estructura del edificio y la ubicación de las áreas de trabajo dificultan la instalación de la red cableada, se implementa la instalación de la red inalámbrica, para poder cubrir las necesidades de la empresa.

2. La seguridad ha sido uno de los criterios decisivos para la toma de decisiones ya que mediante esta se suministrarán elementos de seguridad, tales como algoritmos de cifrado, que autenticarán el tráfico de la red.

3. Los beneficios y comodidades que presenta una WLAN incrementarán el uso de las tecnologías de la información, lo que provocará en un futuro una expansión de la red. Mediante la flexibilidad, escalabilidad y compatibilidad que presenta una red inalámbrica, podrá extenderse tanto en número de usuarios como en su infraestructura, cuando sea necesario.

4. Las prestaciones de poseer una red interna que facilite el flujo de información entre las sedes justifica la inversión para implementación de la red.

5. Una red WIFI brinda conectividad a internet a lugares complicados, ya sea por lejanía con el proveedor de Internet, costos de instalación o debido a que la distancia compromete la cobertura por el nivel de atenuación.

6. Ningún sistema (telecomunicaciones) se diseña para atender al 100% de los usuarios a la vez, ya que sería altamente costoso y poco eficiente.

7. La capacidad de tráfico (velocidad de transmisión de datos) de una radio base, dependerá tanto del esquema de modulación utilizado, como de la multiplexación usada.

8. El diseño de una red WIFI permite agrupar varias subredes espaciadas geográficamente a través de un radioenlace con antenas de alta ganancia.

RECOMENDACIONES

1. El análisis de tráfico para cualquier sistema, debe de realizarse para la hora pico, ya que si los requerimientos se cumplen en ésta, se puede asegurar que se cumplirán el resto del tiempo.

2. El dimensionamiento de los recursos de una red de telecomunicaciones debe de basarse en dos estudios independientes: el tráfico y la cobertura. Tomando para la implementación, el resultado que exija más recursos.

3. Al dimensionar los recursos de una red, siempre se debe de incluir la capacidad necesaria para las funciones propias del sistema (control, *paging*, *handoff*, etc.).

4. Debe tomarse en cuenta un sistema Wimax; entre más alto sea el esquema de modulación mayor será su sensibilidad al ruido.

5. En un sistema Wimax, para poder enviar una gran cantidad de datos, es necesario utilizar un esquema de modulación alto, como de 64 QAM.

6. Debido a la naturaleza variable de los parámetros de tráfico, en ocasiones, para llevar a cabo el análisis, se les debe dar valores promedio, obtenidos tanto de estudios como de experiencia de los diseñadores (por ejemplo el tráfico promedio por usuario).

7. El diseño, basado en tráfico, de las redes de comunicación inalámbrica, tendrá que realizarse para una zona en específico y dependerá de las características propias de la misma.

BIBLIOGRAFÍA

1. ARBAUGH, W.A.; WAN, SHANKAR, N, Justin, *Your 802.11 Wireless Network has No Clothes.* 2ª. ed. USA: University of Maryland, College Park, 2001. 180 p.

2. ESPINOSA DE LOS MONTEROS, Julián; LÓPEZ GÓMEZ, Oscar; GARCÍA, Santiago. *Técnico en Telecomunicaciones.* 3ª ed. Madrid: Cultural, 2002. 225 p. Tomo 2.

3. MOLINA, Juan Manuel. *Seguridad en redes inalámbricas.* Madrid: Universidad Icesi, 2000. 395 p.

4. RAMOS PASCUAL, Francisco. *Radiocomunicaciones.* 2ª ed. España: Marcombo, 2007. 344 p.

5. RIGNEY, C. S., *Remote authentication dial in user service.* USA: RADIUS RFC 2865, 2000. 168 p.

6. TABACMAN, Eduardo. *seguridad en redes wireless.* 2ª ed. Colombia: ACIS, 2003. 395 p.

7. TRICAS GARCÍA, Fernando. *Ética y seguridad en red*. España: Universidad de Zaragoza, 2002. 326 p.