CAPÍTULO 1

INTRODUCCIÓN

1.1 ANTECEDENTES

Desde el principio de las telecomunicaciones dos han sido las opciones principales para llevar a cabo una comunicación: con ó sin hilos, por cable o por el aire. La portabilidad de los extremos de la comunicación excluye casi por completo la utilización de cables para alcanzar dichos extremos. Por tanto utiliza básicamente la comunicación vía radio. Esta se convierte en una de las mayores ventajas de la comunicación inalámbrica que aparte de obviarse toda la infraestructura física que conllevaría mayor tiempo e inversión ofrece una disponibilidad a los extremos de desplazarse sin necesidad de desconectarse perdiendo vínculos importantes. Las opciones de redes inalámbricas permiten a los proveedores de servicios más opciones y mayor flexibilidad para satisfacer al máximo las necesidades de aplicaciones y cobertura inalámbrica de sus usuarios finales. La empresa COMPUATEL tiene sus inicios en el año 2002 en la ciudad de Quito, su misión es la de brindar servicios de internet a sectores desatendidos por la competencia. Uno de sus proyectos para los años 2009-2010 es la posibilidad de expandir su mercado a ciudades con gran crecimiento comercial enfocándose en esta ocasión en la ciudad de Manta la cual ha venido incorporándose con un gran potencial al desarrollo económico del Ecuador. El tipo de servicio que se propone no existe actualmente en la ciudad siendo una gran oportunidad de mercado. Por el momento la empresa no cuenta con infraestructura en la ciudad para ofrecer servicios de internet, por lo cual se hace indispensable el estudio y diseño de una red WIFI en las zonas comerciales y económicas de la ciudad de Manta.

1.2 Justificación e Importancia del Proyecto

El presente proyecto tiene como finalidad realizar el análisis, diseño y la determinación de los equipos y sistemas que presten mejores ventajas para que COMPUATEL pueda brindar servicio de internet inalámbrico en la ciudad de Manta.

La ciudad de Manta ubicada en la provincia de Manabí alberga algunas de las más importantes empresas a nivel nacional las cuales producen jabones, aceites, atún, etc. Su gran crecimiento económico se ve reflejado en sus centros de dispersión, distracción y conjuntos habitacionales de lujo construidos y proyectos habitacionales por construirse, esto atrae la inversión de los servicios de datos escasos en la ciudad que ahora es el centro de operación de importantes ejecutivos que no cuentan con servicios de Internet portátil que la tecnología actual permite ofrecer.

Un ISP que proporcione un servicio de internet portátil entraría como competidor único de las empresas que no han explotado este tipo de servicio en la ciudad de Manta.

La gran capacidad de escalamiento en redes inalámbricas de tráfico, permite construir grandes redes *wireless* que podría a futuro permitir expander la cobertura de esta, inclusive planificar y crear futuras ampliaciones y servicios requeridos por la empresa COMPUATEL.

La cobertura que se considera en el presente proyecto corresponde a toda el área urbana de la ciudad de Manta que permitirá una conexión de los terminales en cualquier parte que estos se encuentren ubicados.

1.3 ALCANCE DEL PROYECTO

El presente proyecto tiene la finalidad de realizar el estudio para diseñar una red de internet portátil a lo largo de la ciudad de Manta determinando dimensionamientos, equipos y software de administración que permita cumplir con las expectativas de la empresa COMPUATEL de contar y ofrecer este

servicio en la ciudad de Manta.

Se efectuará el análisis de equipamiento e infraestructura que permita ofrecer una cobertura garantizada en los sectores económicos y comercialmente más importantes de la ciudad de Manta.

Se incluirá un estudio de mercado en diferentes lugares determinando el requerimiento, capacidades y sectores potenciales para la implementación de internet portátil en la ciudad de Manta.

A través del estudio se identificarán los puntos estratégicos para la ubicación de los equipos y el número necesario de ellos para permitir el cambio de locación de los usuarios conectados y garantizar los niveles mínimos de servicio.

Las pruebas de campo a realizarse en coordinación con COMPUATEL permitirán establecer la efectividad y eficiencia del diseño que será entregado al finalizar el presente proyecto y que se constituirán en la base para la futura implementación de toda la red de internet portátil en la ciudad de Manta.

1.4 OBJETIVOS

1.4.1 General

- Realizar el estudio, análisis y diseño de una red de internet portátil basado en sistemas WIFI para su posterior implementación en la ciudad de Manta.

1.4.2 Específicos

- Analizar las redes MESH inalámbricas sus ventajas y facilidad de implementación.
- Realizar un estudio de mercado y análisis de demanda.
- Realizar un análisis técnico económico de equipos que permita cumplir con los requerimientos de cobertura, ancho de banda y calidad de servicio para la red de internet portátil.
- En coordinación con COMPUATEL efectuar pruebas de cobertura de los equipos en diferentes partes de la ciudad, considerando áreas estratégicamente comerciales y económicas.
- Localizar los puntos estratégicos para la ubicación de los dispositivos, antenas y AP.
- Elaborar un mapa de estaciones, cobertura, infraestructura y localización de los equipos como parte del diseño de la red planteada.

CAPITULO 2

REDES MESH INALÁMBRICAS

INTRODUCCIÓN

El importante desarrollo y avance de las telecomunicaciones ha tenido varios factores que han coadyudado a su progreso y uno de estos factores es la modulación.

Antes de desarrollar el tema de la investigación es necesario recordar algunos conceptos claves y básicos como es el concepto de FM la cual fue utilizada en un principio por la radiodifusión para crear canales radiofónicos, pero que con el avanzar de los tiempos se han dado a conocer diferentes métodos de modulación de frecuencia que han aportado un gran desarrollo a las telecomunicaciones.

2.1 CONCEPTOS BÁSICOS

2.1.1 Características de FM

La frecuencia modulada posee varias ventajas sobre el sistema de modulación de amplitud (AM) utilizado alternativamente en radiodifusión. La más importante es que al sistema FM apenas le afectan las interferencias y descargas estáticas. Las características principales de la frecuencia modulada son: su modulación y su propagación por ondas directas como consecuencia de su ubicación en la banda de frecuencia de VHF.

La modulación en frecuencia consiste en variar la frecuencia de la portadora proporcionalmente a la frecuencia de la onda moduladora (información), permaneciendo constante su amplitud. A diferencia de la AM, la modulación en frecuencia crea un conjunto de complejas bandas laterales cuya profundidad (extensión) dependerá de la amplitud de la onda moduladora. Como consecuencia del incremento de las bandas laterales, la anchura del canal de la FM será más grande que el tradicional de la onda media, siendo también mayor la anchura de banda de sintonización de los aparatos receptores. La principal consecuencia de la modulación en frecuencia es una mayor calidad de reproducción como resultado de su casi inmunidad hacia las interferencias eléctricas. En consecuencia, es un sistema adecuado para la emisión de programas (música) de alta fidelidad.

2.1.2 Espectro disperso

El espectro disperso es una técnica de comunicación que por los altos costos que acarreaba, se aplicó casi exclusivamente para objetivos militares, hasta comienzos de los años noventa donde comienza a surgir lentamente un mercado comercial.

Para poder captar un programa radial hay que sintonizar con un emisor que está en una determinada frecuencia. Emisores diferentes están en diferentes frecuencias. Cada emisor ocupa un pequeño rango de la banda emisora dentro de la cual se concentra la potencia de emisión irradiada. Esta pequeña banda, también llamada amplitud de banda, tiene que ser lo suficientemente grande como para que los emisores cercanos no sean interferidos. A medida que la amplitud de banda es más angosta, pueden funcionar más emisores en una banda de frecuencia.

La radio-receptora se puede sintonizar siempre en una frecuencia. Esa frecuencia es retransmitida por el emisor con una amplitud de banda lo más pequeña posible, pero lo suficientemente grande como para transmitir la

información deseada. Este tipo de receptores se llaman receptores de banda angosta (estrecha).

Por el contrario, en *Spread Spectrum* o espectro disperso no se elige por una amplitud de banda lo más pequeña posible, sino justamente por una lo más grande posible. La amplitud de banda es mayor de lo que se necesita estrictamente para la transmisión de la información. Esta mayor amplitud de banda puede obtenerse de dos maneras. La primera es codificar la información con una señal seudo-fortuita (aleatoria). La información codificada se transmite en la frecuencia en que funciona el emisor para lo cual se utiliza una amplitud de banda mucho mayor que la que se usa sin codificación (secuencia directa). La segunda posibilidad es codificar la frecuencia de trabajo con una señal seudo-fortuita (aleatoria), por lo que la frecuencia de trabajo cambia permanentemente. En cada frecuencia se envía una pequeña porcion de información *(Frecuencia Hopping)*.

2.1.3 Salto en frecuencia (FHSS: FREQUENCY HOPPING SPREAD SPECTRUM)

FHSS de banda estrecha consiste en que una trama de bits se envía ocupando ranuras específicas de tiempo en diversos canales de radio-frecuencia. *FHSS* de banda ancha consiste en que durante el intervalo de 1 bit se conmutan diversos canales de radio-frecuencia.

Al igual que en Ethernet los datos son divididos en paquetes de información, solo que estos paquetes son enviados a través de varias frecuencias, esto es conocido como *"Hopping Pattern"*, la intención de enviar la información por varias frecuencias es cuestión de seguridad, ya que si la información fuera enviada por una sola frecuencia sería muy fácil interceptarla.

Además, para llevar cabo la transmisión de datos es necesario que tanto el aparato que envía como el que recibe información coordinen este denominado

"Hopping Pattern". El estándar IEEE 802.11 utiliza *FHSS*, aunque hoy en día la tecnología que sobresale utilizando *FHSS* es *Bluetooth*

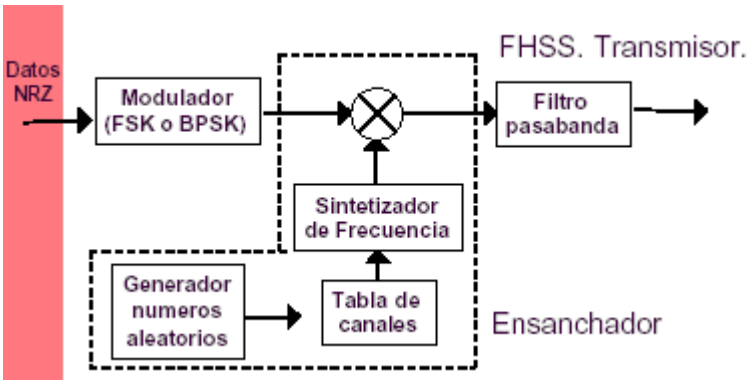


Figura 2. 1 Transmisión de FHSS

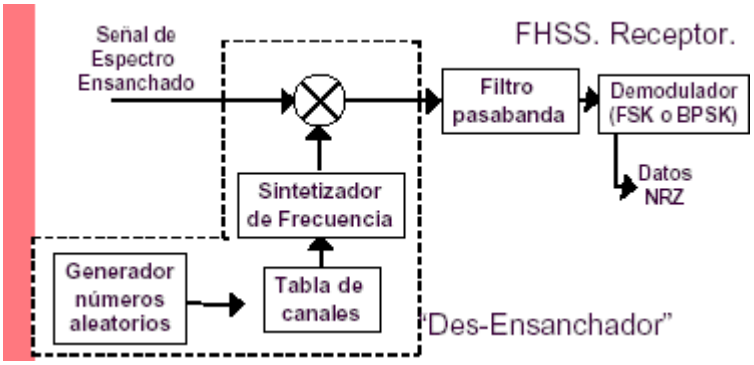


Figura 2. 2 Recepción de FHSS[1]

2.1.4 Acceso inalámbrico

[1] http://images.google.com.ec/imgres?imgurl=http://www.monografias.com/trabajos14/modulac-frecuencia/Image445.gif&imgrefurl=http://www.monografias.com/trabajos14/modulac-frecuencia/modulac-frecuencia.shtml&usg=__hyy6BNbuQr_saZnGFFcSf4Q9bg8=&h=188&w=378&sz=8&hl=es&start=12&itbs=1&tbnid=WgA10xrMK2tfdM:&tbnh=61&tbnw=122&prev=/images%3Fq%3Drecepcion%2Bfhss%26gbv%3D2%26hl%3Des%26sa%3DG

El acceso inalámbrico es aquél en que los usuarios obtienen su servicio mediante un enlace óptico o de radio-frecuencias.

Para tener acceso, se han creado protocolos que garantizan que el acceso obedezca a algún criterio acordado: acceso justo, dar prioridad a la información sensible a retardos, ofrecer garantías de transporte confiable, etc.

El acceso puede ser mantenido indefinidamente o ser asignado temporalmente por demanda de cada usuario:

FAMA (Fixed Assigned Multiple Access)
DAMA (Demand Assigned Multiple Access)

Por lo general, estas modalidades se utilizan en enlaces satelitales, aunque también es factible encontrarlo en enlaces terrestres.

El acceso inalámbrico en modo de asignación dinámica puede presentar diversas variantes, cada una de las cuales se adapta mejor a la aplicación específica.

2.1.5 FDMA

FDMA es una tecnología de acceso múltiple por división de frecuencias, que corresponde a una tecnología de comunicaciones usado en los teléfonos móviles de redes GSM.

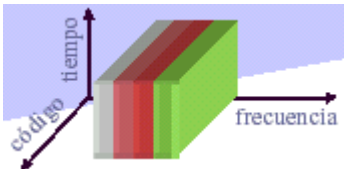


Figura 2. 3 Representación gráfica de la tecnología FDMA

FDMA es la manera más común de acceso truncado. Con FDMA, se asigna a los usuarios un canal de un conjunto limitado de canales ordenados en el dominio de la frecuencia. Los canales de frecuencia son muy preciados, y son asignados a los sistemas por los cuerpos reguladores de los gobiernos de acuerdo con las necesidades comunes de la sociedad. Cuando hay más usuarios que el suministro de canales de frecuencia puede soportar, se bloquea el acceso de los usuarios al sistema. Cuantas más frecuencias se disponen, hay más usuarios, y esto significa que tiene que pasar más señalización a través del canal de control. Los sistemas muy grandes FDMA frecuentemente tienen más de un canal de control para manejar todas las tareas de control de acceso. Una característica importante de los sistemas FDMA es que una vez que se asigna una frecuencia a un usuario, ésta es usada exclusivamente por ese usuario hasta que éste no necesite el recurso. FDMA utiliza un filtro RF para evitar las interferencias con canales adyacentes.

2.1.6 (FDM) MULTIPLEXACIÓN POR DIVISIÓN EN FRECUENCIA

El empleo de técnicas de multiplexación por división en frecuencia requiere el uso de circuitos que tengan un ancho de banda relativamente grande. Este ancho de banda se divide luego en subcanales de frecuencia.

Cuando una portadora usa FDM para la multiplexación de conversaciones de voz en un circuito ordinario, el paso-banda de 3 Khz de cada conversación se traslada hacia arriba en la frecuencia según un incremento fijo de frecuencia.

Este cambio de frecuencia coloca la conversación de voz en un canal predefinido del circuito multiplexado de FDM.

En el destino, otro FDM demultiplexa la voz, cambiando el *spectro* de frecuencia de cada conversación hacia abajo con el mismo incremento de frecuencia que se hizo al principio hacia arriba.

El principal uso de FDM es para permitir a las portadoras llevar un gran número de conversaciones de voz simultáneamente en un único circuito común enrutado.

Las técnicas de multicanalización son formas intrínsecas de modulación, permitiendo la transición de señales múltiples sobre un canal, de tal manera que cada señal puede ser captada en el extremo receptor. Las aplicaciones de la multicanalización comprenden telemetría de datos, emisión de FM estereofónica y telefonía de larga distancia.

FDM es un ambiente en el cual toda la banda de frecuencias disponible en el enlace de comunicaciones es dividida en subbandas o canales individuales. Cada usuario tiene asignada una frecuencia diferente. Las señales viajan en paralelo sobre el mismo canal de comunicaciones, pero están divididos en frecuencia, es decir, cada señal se envía en una diferente porción del espectro. Como la frecuencia es un parámetro analógico, por lo regular el uso de esta técnica de multicanalización es para aplicaciones de televisión. Las compañías de televisión por cable utilizan esta técnica para acomodar su programación de canales.

2.1.7 (OFDM) ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING

OFDM[2] es una tecnología de modulación digital, una forma especial de modulación *multi-carrier* considerada la piedra angular de la próxima generación de productos y servicios de radio frecuencia de alta velocidad para uso tanto personal como corporativo. La técnica de espectro disperso de OFDM distribuye los datos en un gran número de *carriers* que están

[2] http://en,wikipedia.org/wiki/OFDM

espaciados entre sí en distintas frecuencias precisas. Ese espaciado evita que los demoduladores vean frecuencias distintas a las suyas propias.

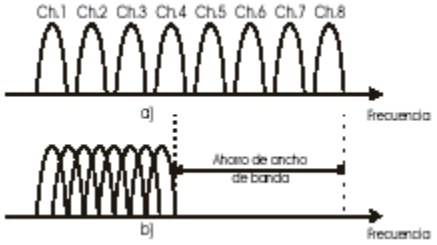


Figura 2. 4 a) Técnica Multiportadora convencional b) Modulación con portadoras ortogonales[3]

OFDM tiene una alta eficiencia de espectro, resistencia a la interface RF y menor distorsión multi-ruta. Actualmente OFDM no sólo se usa en las redes inalámbricas LAN 802.11a, sino en las 802.11g, en comunicaciones de alta velocidad por vía telefónica como las ADSL y en difusión de señales de televisión digital terrestre en Europa, Japón y Australia.

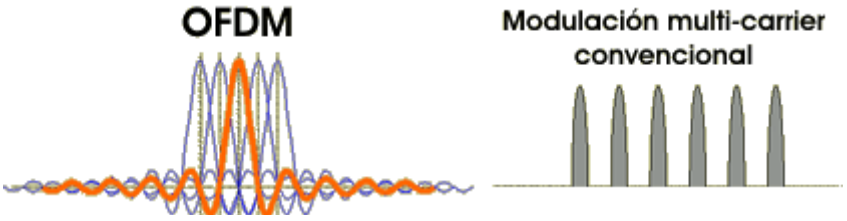


Figura 2. 5 Espectro de OFDM traslapado

2.1.8 WDM

Esta técnica conceptualmente es idéntica a FDM, excepto que la multicanalización y involucra haces de luz a través de fibras ópticas. La idea es la misma, combinar diferentes señales de diferentes frecuencias, sin embargo aquí las frecuencias son muy altas (1x1014 Hz) y por lo tanto se manejan

[3] http://images.google.com.ec/imgres?imgurl=http://www.monografias.com/trabajos14/modulac-frecuencia/Image449.gif&imgrefurl=http://www.monografias.com/trabajos14/modulac-frecuencia/modulac-frecuencia.shtml&usg=__A0OZs2p_aOTe1EkGbcwcrB6NaY4=&h=123&w=228&sz=4&hl=es&start=1&itbs=1&tbnid=dekua5jZQmuAMM:&tbnh=58&tbnw=108&prev=/images%3Fq%3DT%25C3%25A9cnica%2BMultiportadora%2Bconvencional%26gbv%3D2%26hl%3Des%26sa%3DG

comúnmente en longitudes de onda (wavelenght). WDM[4], así como DWDM son técnicas de multicanalización muy importantes en las redes de transporte basadas en fibras ópticas.

En resumen, los multicanalizadores que optimizan el canal de comunicaciones, son pieza importante en las redes de transporte y ofrecen las siguientes características:

- Permiten que varios dispositivos compartan un mismo canal de comunicaciones
- Útil para rutas de comunicaciones paralelas entre dos localidades
- Minimizan los costos de las comunicaciones, al rentar una sola línea privada para comunicación entre dos puntos.
- Normalmente los multicanalizadores se utilizan en pares, un mux en cada extremo del circuito.
- Los datos de varios dispositivos pueden ser enviados en un mismo circuito por un mux. El mux receptor separa y envía los datos a los apropiados destinos
- Capacidad para compresión de datos que permite la eliminación de bits redundantes para optimizar el ancho de banda.
- Capacidad para detectar y corregir errores entre dos puntos que están siendo conectados para asegurar que la integridad y precisión de los datos sea mantenida.
- La capacidad para administrar los recursos dinámicamente con niveles de prioridad de tráfico.

2.2 Sistemas WIFI 802.11

WI-FI es un estándar de protocolo de comunicaciones del IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI. A este estándar se le han hecho modificaciones a través de hardware y software que permiten que

[4] http://alegsa.com.ar/DIC/wdm.php

los productos Wi-Fi se conviertan en una opción de instalación de acceso para áreas metropolitanas.
Las dos modificaciones más importantes tratan dos modelos de uso diferentes:

- Uso de acceso fijo o *last mile* (801.11 con Antenas de Alta Ganancia)
- Uso de acceso portátil o *hot zone* (redes de malla 802.11)

Los productos Wi-Fi asociados con la opción de instalación de acceso para áreas metropolitanas usan frecuencias de radio diferentes:

- El estándar 802.11 usa 5 GHz en un inter-enlace AP a AP.
- Los estándares 802.11b y 802.11g usan 2.4 GHz[5].

Los dispositivos basados en estos estándares no se interfieren mutuamente. Por otro lado, los dispositivos en bandas diferentes no se comunican; por ejemplo, un radio 802.11a no puede conversar con un radio 802.11b. A la fecha, las instalaciones más comunes de WISPs *(wireless Internet services provider*) para acceso para áreas metropolitanas son los estándares 802.11b y 802.11g debido a la interoperabilidad y al mayor alcance en la banda de 2.4 GHz.

Cada estándar también difiere en el tipo de tecnología de modulación de radio usada, como se muestra a continuación:

- El estándar 802.11b usa espectro ensanchado por secuencia directa (DSSS) y soporta velocidades de ancho de banda de hasta 11 Mpbs.
- Los estándares 802.11a y 802.11g usan multiplexación por división de frecuencia ortogonal (OFDM) y soportan velocidades de hasta 54 Mpbs. Como OFDM es más adaptable a ambientes externos y a la interferencia, se lo usa más frecuentemente en soluciones de acceso para áreas metropolitanas.

[5] IEEE standar

La tecnología OFDM usa optimización de sub-portadoras (*sub-carriers*) para usuarios basados en condiciones de frecuencia de radio.

Ortogonal significa que las frecuencias en las que la portadora (*carrier*) se divide son elegidas para que el pico de una frecuencia coincida con los nulos de la frecuencia adyacente. El flujo de datos es convertido de seriado a paralelo, y cada flujo de datos paralelo es mapeado por un bloque de modulación. Los datos modulados pasan a un bloque de transformación rápida de Fourier (IFFT) para procesamiento. El bloque IFFT convierte las frecuencias moduladas discretas en una señal de dominio de tiempo que se usa para impulsar el amplificador de la frecuencia de radio (RF).

Esta eficiencia espectral mejorada es un gran beneficio para las redes OFDM, lo que las hace ideales para conexiones de datos de alta velocidad en soluciones fijas y móviles.

El estándar 802.11 ofrece 64 sub-portadoras. Estas portadoras son enviadas desde la estación base (BS) o AP a la estación del abonado (*subscriber station-SS*) o cliente y reconstituidos en el lado del cliente. En situaciones "*non-lineof-sight*" - NLOS (sin línea de vista), estas portadoras chocarán contra paredes, edificios, árboles y otros objetos, que reflejarán la señal y crearán una interferencia multi-path.

Cuando las señales de la portadora llegan al cliente para su reconstitución, las señales de la portadora individual ya están demoradas. Por ejemplo, una portadora puede haberse reflejado una vez y llegado 1 µs más tarde que otro, y el segundo puede haberse reflejado dos veces y llegar 2 µs más tarde. Cuanto más sub-portadoras sobre la misma banda resulta en sub-portadoras menores, que equivale a mayores períodos de símbolo de OFMD. En consecuencia, el mismo porcentaje de tiempo de guarda o prefijo cíclico (CP) dará valores cíclicos mayores en tiempo para mayores demoras y aumentarán la resistencia

a interferencia *multi-path*. Como los estándares 802.11a y 802.11g usan OFDM, son más elásticos que el estándar 802.11b en ambientes propensos a *multi-paths*.

La topología de red de malla amplía el alcance de LANs y WLANs tradicionales. En una topología de red de malla, se conecta cada nodo y se comparten los protocolos de comunicación en todos los nodos. Una infraestructura Wi-Fi se forma cuando enlaces 802.11 interconectan un grupo de nodos basados en 802.11a, b o g. El estándar 802.11 es el más usado en enlaces AP a AP debido a su desempeño y la superposición con transmisiones 802.11b o 802.11g (Ver tabla 2.1). Las redes de malla aprenden automáticamente y mantienen configuraciones dinámicas de *path*. Los dispositivos inalámbricos en una topología de red de malla crean un *path* para datos entre sí sobre un espectro de exención de licencia a 2.4 o 5 GHz con velocidades de hasta 54 Mbps. Implementaciones dorsales de infraestructuras de malla Wi-Fi se basan en soluciones propias. Estas soluciones propias pueden soportar VoIP y QoS. También pueden aumentar el alcance de cobertura del límite de 100 metros de Wi-Fi a más de 10 km. Además, el desempeño puede aumentarse del límite de 54 Mbps de Wi-Fi a más de 100 Mbps. Sin embargo, estas implementaciones no son interoperables, tienen escalabilidad limitada y en ciertas instalaciones se encuentran limitadas por *backhaul* por cable (*wired backhaul*). La ratificación de 802.11s estandarizará la topología de red de malla Wi-Fi. Las topologías de red de malla Wi-Fi pueden ser utilizadas como solución *last mile* pero son mejores para áreas extensas con acceso 802.11.

Tabla 2. 1 Estándares Wi-Fi (IEEE 802.11)

Estándares de la especificación de redes WLAN IEEE 802.11	
Estándar	**Alcance del estándar**
802.11a	Red WLAN de 54 Mbps,5Ghz
802.11b	11Mbps, 2.4Ghz
802.11e	Calidad de servicio (QoS)
802.11g	Red WLAN de 54Mbps, 2.4Ghz
802.11h	Administración del espectro(802.11a)
802.11i	Seguridad
802.11k	Medición de recursos
802.11s	Redes en malla

A veces a la red de malla también se la denomina red *multi-hop* (de saltos múltiples). Las topologías de malla ofrecen una arquitectura que puede mover datos entre nodos de forma eficiente.

Dentro de una red de malla, los pequeños nodos actúan como enrutadores.

Los nodos se instalan en una extensa área (como, por ejemplo, un barrio o una escuela). Cada nodo transmite una señal baja capaz de alcanzar los nodos vecinos, cada uno de los cuales transmite la señal al próximo nodo, con el proceso que se repite hasta que los datos llegan a su destino. Una ventaja de esta topología es la capacidad que tiene la instalación para circundar un gran obstáculo, como ser una montaña que impediría que el abonado llegase a una estación base. En una red de malla, los abonados bloqueados pueden llegar a la estación base indirectamente por medio de otros nodos. Aun una pequeña cantidad de malla puede mejorar mucho la cobertura de la estación base si se colocan pequeños nodos.

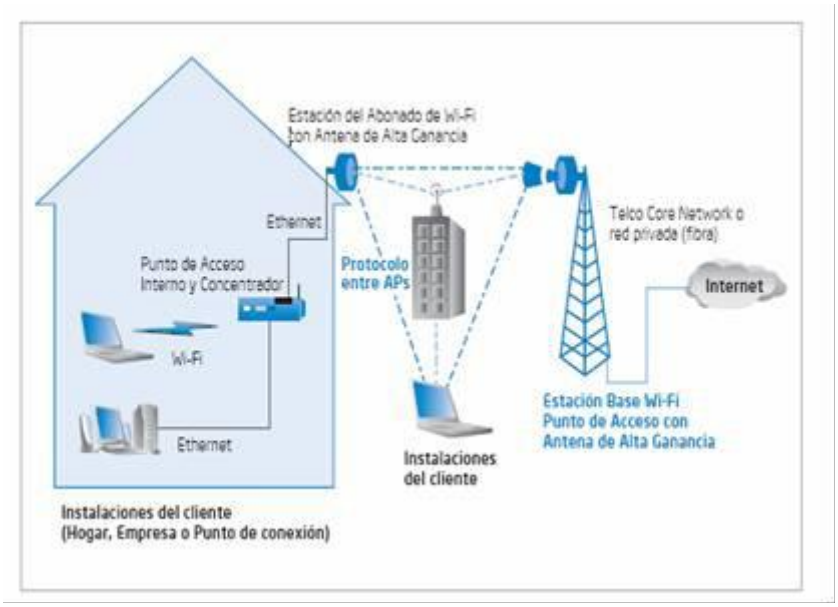


Figura 2. 6 Red de malla 802.11[6]

2.3 Introducción a las redes MESH

Algunas aplicaciones comerciales que son interesantes para redes de alta velocidad basadas en redes *Mesh* de área local se han desarrollado recientemente. Esta tecnología viable económicamente hablando ya que ha sido construida para redes de banda ancha, municipales, de seguridad pública y a gran escala en las llamadas zonas calientes. La arquitectura de las redes *Mesh* surgió de las redes móviles MANETs usadas para redes militares. El grupo de trabajo IEFT MANET ha estado desarrollando varios protocolos por casi una década. Debido a la popularidad de las redes *Mesh* y a la cantidad de vendedores que comenzaron a construir dispositivos para redes *Mesh* se vio la necesidad de crear un estándar que se evidencio en el 2003. El trabajo del grupo de la IEEE que creó el estándar 802.15.5, fue seguido por otro grupo que creó el estándar 802.11s en el 2004. El estándar IEEE 802.11 especifica las

[6]http://images.google.com.ec/imgres?imgurl=http://uvirtual.ufpso.edu.co/file.php/187/imagen6.jpg&imgrefurl=http://uvirtual.ufpso.edu.co/mod/resource/view.php%3Fid%3D4190&usg=__BD3_vCx-SVC1qHgEwp8m23IHOCU=&h=288&w=451&sz=19&hl=es&start=50&itbs=1&tbnid=6AS_yYzYIKr6vM:&tbnh=81&tbnw=127&prev=/images%3Fq%3Dred%2Bmalla%2B802.11%26gbv%3D2%26ndsp%3D21%26hl%3Des%26sa%3DN%26start%3D42

operaciones de acceso a las redes entre clientes y *Access points* (APs). El estándar 802.11 fue creado para *Mesh, Backhaul* (infraestructura WLAN) y *gateway* (infraestructura WLAN a redes LAN cableadas).

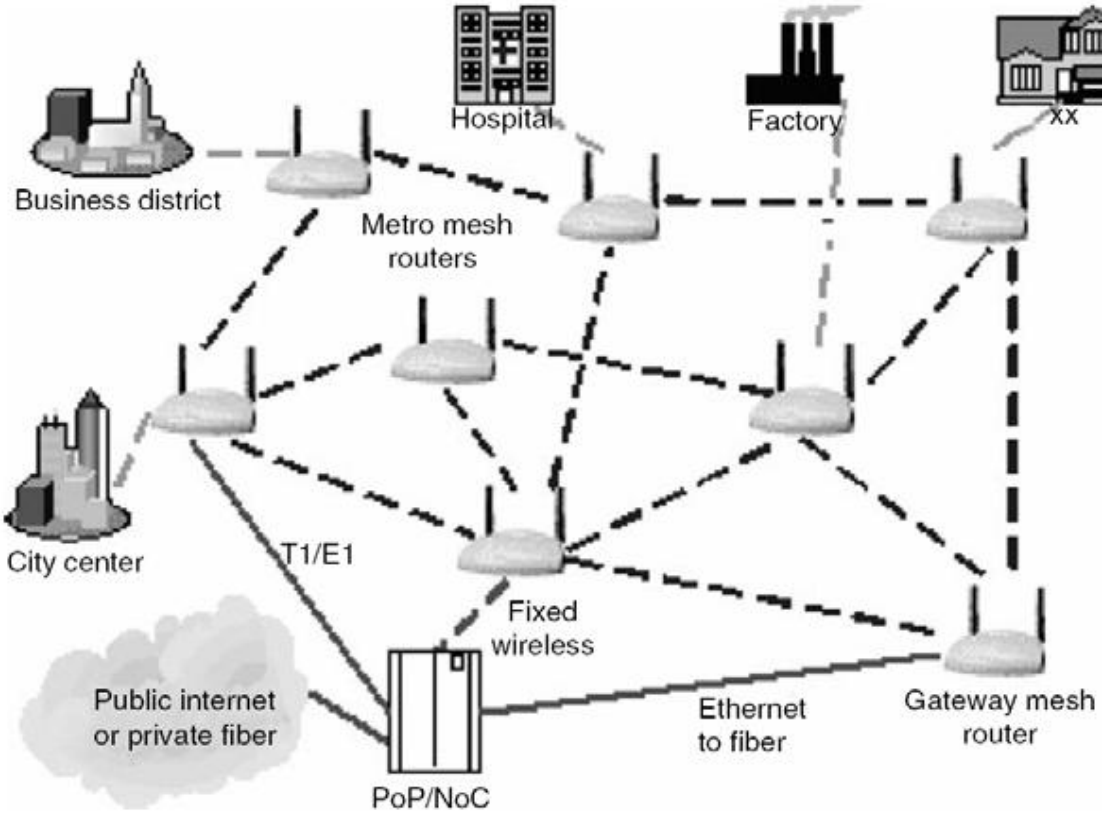


Figura 2. 7 ***Wireless*** **LAN Mesh Networks.**[7]

El estándar ofrece flexibilidad, requerida para satisfacer los requerimientos de ambientes residenciales, de oficina, seguridad pública y aplicaciones militares. La propuesta se enfoca sobre múltiples dimensiones: La subcapa MAC, enrutamiento, seguridad y la de interconexión. Además, define sólo sistemas para ambientes en interiores, pero los principales fabricantes de equipos inalámbricos le están apostando también a sistemas en ambientes exteriores.

[7]http://images.google.com.ec/imgres?imgurl=http://img143.imageshack.us/img143/5527/cwna14hjo7.jpg&imgrefurl=http://setup-wireless.blogspot.com/2008/11/specialty-wlan-infrastructure-devices.html&usg=__MiAJgJne3u4bkay6eKQukm8ViuQ=&h=377&w=373&sz=19&hl=es&start=8&itbs=1&tbnid=HHIPyj6Kcexd3M:&tbnh=122&tbnw=121&prev=/images%3Fq%3Dwireless%2Blan%2Bmesh%2Bnetwork%26gbv%3D2%26ndsp%3D21%26hl%3Des%26sa%3DN

El estándar IEEE 802.11 esta soportada por dos modos adicionales de operación, el Ad Hoc que puede comunicarse directamente sin necesidad de usar AP y por el modo de distribución inalámbrica que utiliza AP punto a punto, donde cada AP actúa no solo como estación base sino que son nodos despachadores. Sin embargo el estándar 802.11 puede ser usado para formar redes *Mesh* Efectivas, algunos funcionamientos, seguridad y manejo de problemas que necesitan ser ubicados.

2.3.1 Primeras redes *mesh*

Los estándares 802.11a y 802.11g han incrementado sustancialmente la tasa de datos de las WLAN usando esquemas de modulación eficientes (a 54Mbps).

EL estándar 802.11 AP (Conocido como punto *Mesh* [MP] cuando es usado en redes *Mesh* WLAN). Los puntos MP-a-MP forman una troncal inalámbrica conocida como *Mesh Backhaul*, la cual proporciona a los usuarios bajo costo, alto ancho de banda y servicios de interconexión *multihop* con un número de puntos de Internet y con otros usuarios sin la red.

Estos dispositivos son llamados *Mesh Access Point* (MAPs). La figura anterior muestra una red *mesh* WLAN típica con sus componentes. Una WLAN *Mesh* está definida como: Una red *Mesh* WLAN está basada en el sistema de distribución inalámbrico del estándar 802.11 (WDS),en la cual una parte DS que consiste en una distribución de dos o más MPs interconectadas por los puntos 802.11 y la comunicación a través de los servicios *Mesh* WLAN.

2.3.2 Selección del canal *Backhaul*

La topología de una red *Mesh* WLAN puede incluir MPs con uno o más interfaces de radios y puede utilizar uno o más canales para la comunicación entre MPs. Cuando cada canal está siendo usado cada interface de radio opera en una MPs sobre un canal al tiempo. Pero el canal debe cambiar durante el tiempo de vida de la red *Mesh* de acuerdo a los requerimientos de selección de frecuencias dinámicas (DFS). La selección de un canal específico usado en una red *Mesh* debe variar de acuerdo a los requerimientos de la aplicación y a las diferentes topologías. Una variedad de interfaces de radio MP que están interconectadas a otras por medio de un canal común, son llamados canales gráficos unificados (UCP). El mismo dispositivo puede tener diversos UCGs. La interface de radio establece puntos de conexión con los vecinos que activa la identificación de la red y el perfil, y selecciona su canal basado en un valor procedente del canal más alto.

2.3.3 Protocolo de unificación de canal simple

Una interfaz lógica de radio que es configurado en modo unificado de canal simple que funciona con técnicas de escaneo pasivo y activo para descubrir los vecinos MPs. Si una MP no puede detectar un vecino MPs, adopta una identificación de acoplamiento a partir de uno de sus perfiles, y selecciona un canal para la operación, así como un valor inicial de la procedencia del canal.

El valor inicial procedente del canal se puede ser iniciado al número de microsegundos más un valor al azar.

2.4 Características de una red Mesh

Una red enmallada está compuesta por una colección de nodos que se comunican entre sí, de manera directa, transmitiendo la información de otros nodos hasta su destino final por medio de múltiples saltos no hay necesidad de una unidad centralizada que los controle, el modo de operación se conoce como distribuido. En caso de existir una unidad que administre las condiciones de operación de la red se conoce como centralizado.

Si no hay necesidad de una entidad centralizada que los controle el modo de operación se conoce como distribuido, pero puede existir una entidad central que administre las condiciones de operación de la red, en cuyo caso se conoce como centralizado. En cualquier caso, la comunicación se realiza entre los nodos directamente y cada nodo puede ser al mismo tiempo fuente o destino de los datos o un enrutador de la información de otro nodo. En la Figura 2.8 se muestra un diagrama de una red de múltiples saltos, donde la información es llevada desde un extremo a otro por diferentes nodos.

Figura 2. 8 Diagrama de red multisaltos

Si los nodos de la red se conectan de manera autónoma, sin configuración previa, se dice que la red opera en modo *ad hoc.* Si los nodos tienen movilidad, entonces se conocen como redes móviles *ad hoc* o MANET (*Mobile* ad-hoc *Network*). Su característica principal es que existe un continuo cambio en la topología de la red, con enlaces que aparecen y desaparecen de modo permanente.

Las características más relevantes de las redes enmalladas inalámbricas son las siguientes:

- **Robustez:** La presencia de enlaces redundantes entre los usuarios permite que la red se reconfigure automáticamente ante fallas.
- **Topología dinámica:** Se supone que las redes enmalladas tienen la capacidad de reaccionar ante cambios de la topología de la red. Por lo tanto la topología cambiante es una condición de diseño necesaria.
- **Ancho de banda limitado:** Como el proceso de comunicación exige transportar datos de otros usuarios y la cercanía de unos con otros precisa una coordinación en los tiempos de transmisión, las redes

enmalladas cuentan con enlaces que usualmente permanecen en condiciones de congestión.

- **Seguridad:** La información transmitida se encuentra expuesta a la amenaza de viajar a través de un medio compartido. El estándar define una subcapa de seguridad para proteger la información de los usuarios y evitar el acceso de usuarios no autorizados.
- **Canales de comunicación aleatorios:** A diferencia de las redes fijas, las redes inalámbricas cuentan con la incertidumbre propia de los canales de comunicación de radio. La característica cambiante de los mismos hace bastante inciertas las condiciones de comunicación. El estándar define aspectos como la modulación y codificación adaptativas para hacer frente a este problema.
- **Carencia de modelos de dimensionamiento apropiados:** El modelo de capacidad de redes de datos está orientado a determinar la capacidad del enlace ante procesos de multiplexación de la información de los usuarios. El modelo de capacidad de las redes enmalladas de múltiples saltos es un problema abierto, Las redes enmalladas proveen, sin embargo, condiciones que permiten el acceso a usuarios en regiones apartadas.

Tabla 2. 2 Características de las redes inalámbricas enmalladas según la movilidad de los nodos

	Estática	Baja Movilidad	Alta Movilidad
Descubrimiento de la red	Pasivo/Activo	Pasivo/Activo	Activo
Enrutamiento	Actualizaciones poco frecuentes. Rendimiento altamente estable	Actualizaciones poco frecuentes. Rendimiento altamente estable	Actualizaciones frecuentes. Bajo overhead.
Seguridad	Infrecuentes re-autenticaciones	Infrecuentes re-autenticaciones	frecuentes autenticaciones
QoS	Mecanismos estáticos/lentos.	Mecanismos lentos.	Mecanismos dinámicos/Rápidos
Consumo de energía	Principalmente dispositivos conectados a la red eléctrica.	Una mezcla pero dominan los dispositivos conectados a la red eléctrica.	Principalmente dispositivos basados en el uso de baterías.

2.4.1 Operación de una red Mesh

La operatividad del sistema no solo depende del buen diseño, sino también de la elección correcta del equipamiento y la robustez de los mismos. Por ello, es necesario diseñar un conjunto de estaciones tanto *Gateway* como *Relay* a fin de crear alternativas de diseño según sean los requerimientos. Aparte de estos prediseños, se tienen que tener en cuenta las ganancias de las antenas, direccionalidad de antenas, potencia de amplificadores, etc.

Para crear una red *mesh* se debe conectar un punto de acceso *mesh* a algún Tipo de acceso a Internet. Este acceso a Internet puede ser una línea dedicada, una ADSL (Línea de Suscriptor Digital Asimétrica), una SDSL (Línea de Suscriptor Digital Simétrica) o en áreas remotas, por medio del satélite.

Todo es compatible siempre que use IP (Protocolo de Internet) El tamaño y el tipo de acceso a Internet se decidirá según una variedad de factores:

- Lo que se tenga disponible
- La cantidad de usuarios que se deba atender
- Los requerimientos de ancho de banda de los usuarios
- El costo

Se configura el primer *Mesh*-AP con un canal inalámbrico, usualmente un canal 802.11b, un SSID. Al Punto de Acceso a la red *Mesh* se lo refiere como *gateway*.

También se utilizan nodos que tienen exactamente la misma programación del nodo *gateway*. La única cosa que decide si los *Mesh*-AP se muestran como *gateway* es si han obtenido una dirección IP de un DHCP o son configurados con una dirección IP fija.

El primer nodo repetidor se desplegará dentro del alcance del primer nodo *Mesh-AP*, simplemente dándole energía, el mismo canal y el mismo SSID del *gateway*. Cuando se inicie el *Mesh-AP* se sabrá que no es un nodo repetidor por el hecho de no haber obtenido una dirección IP. Este tratará de descubrir el nodo *gateway*. Una vez que haya sido establecido un enlace con un nodo *gateway*, el tráfico de Internet es encaminado desde el cliente, por medio del nodo repetidor y a Internet por medio del *gateway*.

De esta manera pueden agregarse más nodos al *mesh*, y, siempre que el nodo *mesh* agregado esté dentro del radio de alcance de un nodo que sea o bien un *gateway* o bien otro nodo que pueda alcanzarlo, entonces el tráfico de Internet será encaminado a través del *mesh*, por medio de la ruta a Internet más eficiente.

2.4.2 Alcance de una red *Mesh*

Para definir el alcance de una red *Mesh* hay que tener en cuenta una Variedad de factores que afectan su radio de acción. Algunos de estos factores son:

- La potencia de la tarjeta inalámbrica
- El tipo y ganancia de la antena
- La ubicación de la antena

- El terreno en que se encuentra, la existencia de intrusiones u obstrucciones en la ruta de la señal inalámbrica.
- La existencia de interferencia inalámbrica de otros dispositivos que provoquen un incremento en el nivel ruido general.
- La sensibilidad inalámbrica de los dispositivos de recepción
- El tipo de antena, ganancia y ubicación de los dispositivos de recepción.

La apropiada revisión de los sitios, la correcta instalación, la experiencia y una selección cuidadosa del equipamiento de recepción, todo esto optimizará la capacidad de cobertura del *mesh*.

El sistema *Mesh* tiene la capacidad de llevar a cabo un gran número de funciones. A continuación aparece una muestra de algunas de las características de *Mesh*:

- Servicios DHCP
- Servidor VPN2
- Calidad de servicio o prioridad para protocolos de voz SIP, IAX – y H323
- Soporte a *Bluetooth*
- Cámaras Web USB de circuito cerrado de televisión accesibles desde Internet público
- Administración remota basada en web.
- Informes estadísticos remotos
- Encriptación de 2048 bits
- Mapeo de servidor y puertos hacia dispositivos
- Autenticación
- Servicios DNS en cada AP
- *Firewall* - Cortafuegos
- Agrupación para permitir otras interfaces inalámbricas

2.5 Ventajas y desventajas de las redes MESH inalámbricas

Una red WLAN tradicional consta de uno o más puntos de acceso (PA) inalámbrico (Access Point) que se conectan mediante un cable UTP categoría 5e directamente a un switch/hub Ethernet hacia la red cableada. De esta misma manera se podrían conectar más puntos de acceso para incrementar el área de cobertura de la red.

Con las redes Wi-Fi en malla es posible que estos puntos de acceso se puedan conectar y comunicar entre ellos de forma inalámbrica, utilizando las mismas frecuencias del espectro disperso, ya sea en 2.4 GHz o en la banda de 5.8 GHz. Las redes Wi-Fi en malla son menos ambiciosas pero más reales. Para operar sólo necesitan de clientes ordinarios IEEE 802.11.

Las redes Wi-Fi en malla son simples, todos los puntos de acceso comparten los mismos canales de frecuencia. Esto hace a los AP relativamente baratos. El único problema es que el canal es compartido, es decir el ancho de banda de la red. Los APs actúan como hubs, así la malla funciona de manera similar a una red plana construida completamente de hubs; es decir todos los clientes contienden para acceder al mismo ancho de banda.

Los sistemas multiradio utilizan un canal para enlaces hacia los clientes Wi-Fi y el resto para enlaces en malla hacia otros APs. En la mayoría de las arquitecturas los enlaces a los clientes están basados en 802.11b/g, debido a que la banda de frecuencia de 2.4 GHz es la más utilizada por el hardware de los equipos Wi-Fi. En cambio la red de malla está basada en el estándar 802.11a debido a que la banda de 5 GHz está menos congestionada, habiendo menos riesgo de interferencia entre los enlaces de la malla y los clientes. Sin embargo, el estándar 802.11 no soporta nativamente las mallas, así que cada fabricante necesita implementar su propia tecnología propietaria por encima del 802.11a. El estándar 802.11s, tiene la finalidad de reemplazar estas tecnologías propietarias, tanto para sistemas de un solo canal o de varios canales de radio.

Las redes Wi-Fi en malla son útiles en lugares donde no existe cableado UTP, por ejemplo, oficinas temporales o edificios tales como bodegas o fábricas.

Pero muchos de los fabricantes se están concentrando más bien en ambientes exteriores. En muchos lugares se ha incrementado el Internet público sobre redes Wi-Fi, tales como aeropuertos o comercios. Quizá Wi-Fi en malla sea un modesto competidor de otra tecnología más madura conocida como WiMax.

Un aspecto fundamental del funcionamiento de las redes en malla es que la comunicación entre un nodo y cualquier otro puede ir más allá del rango de cobertura de cualquier nodo individual. Esto se logra haciendo un enrutamiento multisaltos, donde cualquier par de nodos que desean comunicarse podrán utilizar para ello otros nodos inalámbricos intermedios que se encuentren en el camino. Esto es importante si se compara con las redes tradicionales WiFi, donde los nodos deben de estar dentro del rango de cobertura de un AP y solamente se pueden comunicar con otros nodos mediante los AP; estos AP a su vez necesitan de una red cableada para comunicarse entre sí. Con las redes en malla, no es necesario tener AP, pues todos los nodos pueden comunicarse directamente con los vecinos dentro de su rango de cobertura inalámbrica y con otros nodos distantes mediante el enrutamiento multisalto ya mencionado.

2.6 ARQUITECTURA DE LAS REDES *MESH*

2.6.1 Clasificación de arquitecturas en redes *Mesh*

Una red inalámbrica *Mesh* puede ser diseñada basada en tres diferentes arquitecturas de red:

- Arquitectura plana
- Arquitectura jerárquica
- Arquitectura híbrida

2.6.2 Arquitectura plana

En una red plana WMNs, la red está formada por los equipos cliente que actúan como host[8] y routers. En este caso, todos los nodos están al mismo nivel. Los nodos de los clientes inalámbricos coordinan entre sí para proporcionar enrutamiento, configuración de la red, provisión de servicios, y algún otro tipo de solicitud. Esta arquitectura es la más parecida a una red Ad Hoc y es el caso más simple entre los tres tipos de arquitecturas WMNs. La principal ventaja de esta arquitectura es su sencillez, y sus desventajas incluyen la falta de escalabilidad y limitaciones de recursos. Los principales problemas a resolver en el diseño de esta arquitectura WMNs son: esquema de direccionamiento, enrutamiento y servicios. En una red plana, el direccionamiento es uno de los problemas que llega a impedir la estabilidad.

2.6.3 Arquitectura jerárquica

En una arquitectura jerárquica, la red tiene múltiples niveles jerárquicos en la que los nodos del cliente forma el nivel más bajo dentro de la arquitectura.

Estos nodos del cliente pueden comunicarse con la red que está formada por routers. En la mayoría de los casos, los nodos WMNs se dedican a forman un *backbone* de una red troncal WMNs. Esto significa que los nodos que forman el *backbone* no pueden originar o terminar el tráfico de datos como los nodos del cliente. La responsabilidad de auto-organizar y mantener la red troncal está a cargo de los routers WMNs, algunos de los cuales pueden tener interfaz externa a Internet y a esos nodos se los llama nodos pasarela.

2.6.4 Arquitectura Hibrida

Éste es un caso especial de la arquitectura jerárquica donde la red enmallada utiliza otras redes inalámbricas para la comunicación. Por ejemplo, el uso de

[8] Aquel dispositivo de la red que ofrece servicios a otros ordenadores conectados a la red

otras redes basadas en infraestructura tal como redes celulares, redes de WiMAX, o redes basadas en los satélites. Ejemplos de tales sistemas híbridos incluyen las redes celulares *multihop*, rendimiento de procesamiento radio realzada en las redes locales del lazo y redes ad hoc de celulares unificadas.

Una solución práctica para tal híbrido WMN para los usos de la respuesta de la emergencia es la plataforma de *CallMesh*. Este es el híbrido WMN que puede utilizar las tecnologías múltiples para WMN y el establecimiento de una red inalámbrica con acoplamiento de transporte del *backbone* y de la parte posterior. Puesto que el crecimiento de WMNs depende generalmente de la manera como trabaja con otras soluciones inalámbricas existentes de una red, esta arquitectura llega a ser muy importante en el desarrollo de las redes inalámbricas enmalladas.

2.6.5 Criterios de diseño en redes inalámbricas Mesh multiradio MR-WMNs

Las principales ventajas de utilizar redes MR-WMNs son el aumento de la capacidad, escalabilidad, fiabilidad, robustez, y flexibilidad de implementación. A pesar de las ventajas de utilizar un sistema de multiradio para WMNs, existen muchos desafíos para el diseño de un sistema eficiente MR-WMNs.

Los principales elementos a tener en cuenta para el diseño de una MRWMNs se pueden clasificarse en: diseño de la arquitectura, diseño MAC, diseño de protocolos de enrutamiento y diseño de métricas, que se explican a continuación.

2.6.6 Criterios de diseño arquitectónico

La arquitectura de red desempeña un papel importante para obtener un buen rendimiento de una red MR-WMNs, cuando se diseña una red MR-WMN la arquitectura seleccionada debe tomar en cuenta el tipo de aplicación y el escenario. Las principales opciones de arquitectura para ser consideradas son

las siguientes: (a) basada en la topología, (b) basada en la tecnología, y (c) basada en el nodo.

Una MR-WMNs basada sobre la topología, se puede diseñar ya sea como topología plana o topología jerárquica**.** Basada en tecnología se puede diseñar en homogéneas o heterogéneas. Aunque la forma más general para sistemas MRWMNs son tecnologías homogéneas es decir utiliza un solo tipo de tecnología de radio como la popular tecnología de conexión inalámbrica IEEE 802.11, es posible desarrollar una red MR-WMNs con tecnologías heterogéneas que utilizan una variedad de tecnologías de comunicación. Por último, la arquitectura basada en el nodo puede clasificarse dentro de las siguientes: basado en el host, basado en la infraestructura, o redes híbridos MR-WMNs. En el caso de las basadas en host MR-WMNs, la red está formada por los nodos host y tiene una similar operación a la de una red Ad Hoc pero con limitada movilidad. Por otra parte la arquitectura de red MR-WMNs basada en infraestructura está formada por nodos situados en infraestructuras fijas o edificios. Por último una arquitectura de red híbrida MR-WMN que opera tanto basado en infraestructura troncal y host inalámbricos en malla. Estos hosts se comunican a través de *backbone* inalámbricos en malla. Esta topología de red troncal se puede organizar bien como una topología plana o como una topología jerárquica, en algunos entornos de aplicación, los hosts son móviles y ellos también retransmiten tráfico en beneficio de otros hosts en la red. Un ejemplo de este tipo de red híbrida MRWMNs es una red WMNs vehicular que se comunica a través de una infraestructura inalámbrica de malla. Por lo tanto, el diseño de un sistema MRWMNs debe considerar el tipo de aplicación y el entorno de despliegue para la elección adecuada de una arquitectura.

2.6.7 Diseño para la capa MAC

La capa MAC para MR-WMNs se enfrenta a varios problemas, entre ellos tenemos la interferencia inter-canal[9], interferencia inter-radio, distribución del canal, y el diseño de protocolos MAC.

[9] Es la interferencia experimentada en un determinado canal producido por la actividad de canales vecinos

Para la interferencia intercanal hay que tomar en cuenta la presencia de múltiples sistemas de radio en la misma zona. Esta interferencia con un canal vecino dará lugar a una degradación significativa del rendimiento.

La interferencia inter-radio[10] se debe principalmente al diseño de los componentes de hardware y de la propia interfaz. La separación física de las interfaces pueden ayudar a evitar este problema en cierta medida, en algunos casos la separación puede ser difícil, especialmente en nodos móviles.

Otra cuestión de importancia para MAC es el canal de distribución. Se trata de un proceso en que la asignación de canales sin interferencia daría lugar a un rendimiento alto y un buen acceso al medio. El canal de distribución debe considerar el número de canales disponibles y el número de interfaces disponibles. Por último, la cuestión más importante es el diseño de protocolos MAC. Esta disponibilidad de múltiples interfaces y múltiples canales que conducen a nuevos diseños para protocolos de acceso que deben beneficiar la presencia de múltiples radios.

Algunos ejemplos de estos protocolos son: MCSMA, ICSMA, 2P-TDMA. Estos protocolos utilizan simultáneamente múltiples canales y también tratan de resolver la cuestión de acceso a los medios en MR-WMNs.

2.6.8 Diseño de protocolos de enrutamiento

El diseño de protocolos de enrutamiento depende del diseño de la arquitectura de la red WMNs y que en algunos casos, también depende de la aplicación de la red y del entorno de despliegue. El Diseño de protocolos de enrutamiento se

[10] Interferencia que experimenta un radio debido a la actividad de canales en otra interfaz

puede clasificar en varias categorías: (a) la topología de enrutamiento, (b) enrutamiento en el *backbone* y (c) la información de mantenimiento de enrutamiento.

Sobre la base de la topología de enrutamiento, los protocolos de enrutamiento se pueden diseñar ya sea para un solo nivel o protocolos de enrutamiento jerárquico. En el enrutamiento jerárquico, una jerarquía de enrutamiento se construye entre los nodos de tal manera que la responsabilidad de encaminamiento se delega a los nodos de mayor nivel jerárquico cuando el nivel de nodos de inferior jerarquía no puede establecer la ruta. Por otra parte en un sistema de enrutamiento de un solo nivel no tiene incorporadas las jerarquías y cada nodo tiene la misma responsabilidad para encontrar un camino para el destino y participar en el proceso de encaminamiento. El camino elegido puede incluir cualquier nodo en la red sin seguir ningún orden jerárquico. La segunda categoría de diseño se basa en el encaminamiento de rutas troncales y la topología de enrutamiento híbrido.

2.6.9 Diseño de métricas de enrutamiento

Una métrica de enrutamiento es una técnica utilizada por los ruteadores para aprender rutas y mantenerlas actualizadas conforme cambia la red, y su función principal es el intercambio de información de ruteo con otros ruteadores, la información de ruteo se encuentra en las tablas de ruteo.

Las métricas incluyen ancho de banda, costo de la comunicación, retraso, número de saltos, costo de la ruta y confiabilidad. Contar los saltos es la más simple métrica de enrutamiento y es una métrica de enrutamiento aditivo. Debido a las características especiales de una red WMNs.

La métrica de enrutamiento desempeña un papel crucial en el desempeño de un protocolo de enrutamiento y el diseño de métricas de enrutamiento debe tomar en cuenta varios factores, como (a) la arquitectura de red, (b) el entorno

de red, (c) la dimensión de la red, (d) las características básicas del protocolo de enrutamiento, con el fin de diseñar un eficiente protocolo de enrutamiento para WMNs.

2.6.10 Topología de control de la red

Topología de control se define como la capacidad de manipular tanto los parámetros de la red como la ubicación de los nodos, la movilidad de los nodos, la energía, las propiedades de la antena, y las interfaces de red. La topología de control tiene la capacidad de modificar ya sea una sola vez los parámetros durante la actividad de la red, en la fase de inicialización o como una actividad periódica durante el tiempo de funcionamiento de la red. El uso eficaz de la topología de control de la red puede ayudar a mejorar la capacidad. Los objetivos de los mecanismos de topología de control son la conectividad, la capacidad, fiabilidad, tolerancia a fallos y la cobertura de la red.

2.6.11 Protocolo de unificación multiradio [MUP]

El MUP es una solución de capa de enlace para proporcionar una capa virtual que controla múltiples interfaces de radio a fin de optimizar el uso del espectro en una red MR-WMNs. Los principales objetivos de diseño del protocolo MUP son los siguientes: (a) reducir al mínimo las modificaciones de hardware, (b) evitar hacer cambios en los protocolos de capa superior.

El MUP proporciona una única interfaz virtual a las capas superiores ocultando las múltiples interfaces físicas y canalizar mecanismos de selección para escoger un canal adecuado para la comunicación entre nodos. MUP es implementado en la capa enlace y por tanto las capas superiores no necesitan experimentar ningún cambio para utilizar de forma eficiente múltiples interfaces de radio. El diagrama de arquitectura MUP se muestra en la figura 2.9

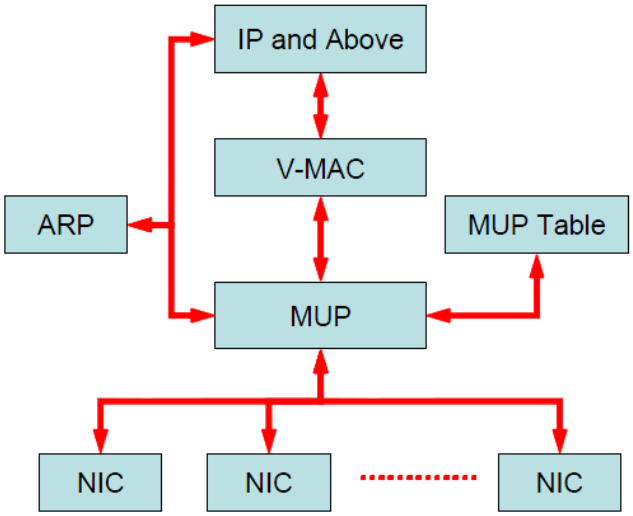


Figura 2. 9 MUP diagrama de arquitectura[11]

Una de las principales tareas que hace la capa MUP es vigilar la calidad del canal entre un nodo y sus vecinos de tal manera que el nodo puede elegir la mejor interfaz para comunicarse con un nodo vecino. Con el fin de virtualizar múltiples interfaces de radio con una dirección MAC diferente, MUP utiliza una dirección MAC virtual que oculta eficazmente las múltiples direcciones físicas que tiene cada tarjeta de red inalámbrica. Esto hace que la capa física aparezca para las capas más alta como una única interfaz.

MUP emplea dos diferentes esquemas para la selección de interfaces de radio, estos esquemas son llamados *MUP-Random* y *MUP-Channel-quality*. De acuerdo con el esquema *MUP-Random* que es el esquema básico, un nodo al azar elige una interfaz para la transmisión de un paquete hacia un nodo destino. El esquema *MUP-channel-quality* está diseñado para mantener la información del estado del canal (conocida también como calidad métrica del canal) este esquema escoge entre algunos nodos y elige el mejor canal basado en mensajes de sondeo de información del estado del canal. El uso de mensajes de sondeo permite a la capa MUP obtener información sobre el estado del canal.

MUP consta de dos módulos: a) módulo vecino y b) módulo de selección de canal. El módulo vecino proporciona tablas y el estado de los canales de nodos

[11] A Multi-Radio Unification Protocol for IEEE 802.11 Wireless Networks, Atul Adya

vecinos. El módulo MUP de selección de canal elige el canal más adecuado. Cada nodo elige y mantiene la información de calidad del canal para todas las interfaces mediante el intercambio de mensajes de sondeo. El retardo del viaje de ida y vuelta experimentado por el mensaje de sondeo es utilizado como canal de observación de la calidad de la métrica. Este retardo de viaje de ida y vuelta incluye el retardo debido al protocolo MAC de contención, la carga de tráfico, las interferencias en el canal, las colisiones de paquetes, y el retardo de procesamiento entre los nodos finales. Con el fin de reducir el retardo, que en general podría ser muy alto en un nodo que tiene gran carga, MUP proporciona una alta prioridad para los paquetes de sondeo ya sea colocando el paquete a la cabeza de los demás paquetes mediante el uso de mecanismos de prioridad definidos en los protocolos MAC tales como IEEE 802.11e.

Las ventajas de MUP son las siguientes: (a) puede trabajar con nodos que tengan una interfaz única o múltiple interfaces, (b) aísla a las capas superiores de conocer los protocolos que manejan múltiples interfaces de radio, y (c) mejora la eficiencia del espectro y el rendimiento del sistema. Algunas de las desventajas son las siguientes: (a) la asignación de canales es ordinaria y, por lo tanto MUP no podrá hacer uso de los mejores canales disponibles, (b) MUP decide cual canal utilizar en un nodo local y este canal a veces puede que no sea el más óptimo sobre los otros canales disponibles, esto afecta en la utilización adecuada de los recursos globales de la red. Otra cuestión con MUP es la asignación de canales para nuevos nodos que entran en funcionamiento en la red, para una red que tiene múltiples canales, se hace necesario el reinicio de todo el sistema, para determinar cuáles son los canales que se asignarán a las interfaces de los nuevos nodos con el fin que estos puedan comunicarse con el resto de la red.

2.6.12 Protocolos de control de acceso al medio para MR-WMNs

El diseño de protocolos MAC es importante en una red MR-WMNs en comparación con redes WMNs de un solo radio a causa de problemas adicionales que esta enfrenta. Aquí se presenta algunas de las recientes propuestas para protocolos MAC en redes MR-WMNs. Estos protocolos son los MCSMA, ICSMA.

2.6.13 Acceso múltiple por detección de portadora multicanal (MCSMA)

El protocolo MAC MCSMA es similar al sistema FDMA (Acceso múltiple por división de frecuencia). En este protocolo el ancho de banda disponible se divide en anchos de banda más pequeños para tener n+1 canales, es decir, n canales de datos y un canal de control. Esta división es independiente del número de nodos en el sistema.

Un nodo que tiene paquetes para ser transmitidos selecciona un canal óptimo de datos para su transmisión. Cuando un nodo está inactivo, es decir, no transmite paquetes de información, monitorea todos los n canales de datos y todos los canales por los cuales a recibido el TRSS (*total received signal strength* = total de intensidad de la señal recibida), el TRSS se estima por la suma de componentes individuales de señal de múltiples rutas, los canales que tienen un TRSS por debajo de ST (*sensing threshold* = sensibilidad del umbral) son marcados como canales inactivos. Cuando un canal está inactivo durante un determinado tiempo, se añadirá a la lista de canales libres. El mecanismo de transmisión de paquetes con el protocolo MCSMA es el siguiente.

Cuando un nodo potencial está en la capacidad de enviar y recibir paquetes de datos, comprueba en su lista de canales, si existe algún canal libre, el transmisor comprueba si el canal por el cual transmitió con éxito el último paquete está incluido en la lista de canales libres, se iniciará la transmisión por este canal. Si la lista de canales libres está vacía, espera a que un canal esté inactivo. Tras detectar un canal inactivo, el transmisor espera por un LIFS (*long interframe space* = gran espacio interframe), seguido por un acceso aleatorio *back-off*. Después del período de back-off el transmisor comprueba nuevamente el canal, y si el canal está aún inactivo, se inicia la transmisión por ese canal. En el caso que el último canal utilizado para la transmisión no esté presente en la lista de canales libres, el transmisor elige al azar un canal entre los canales inactivos, incluso en estos casos, el transmisor espera a que el canal siga inactivo durante el tiempo LIFS más el período de *back-off*, si después de este tiempo el TRSS del canal supera al ST, entonces el proceso

de back-off se cancela, cuando el TRSS del canal va por debajo de ST se inicia la transmisión. Si un canal está siendo ocupado para una transmisión exitosa, se da prioridad a otro canal para poder entablar la transmisión, siempre y cuando n> N, donde n es el número de canales de datos y N es el número de nodos de la red.

2.6.14 Acceso múltiple por detección de portadora intercalado (ICSMA)

El ICSMA es un nuevo protocolo multicanal de acceso al medio. Está diseñado para superar el problema del terminal expuesto, que está presente en los sistemas de un solo canal, basados en censar portadoras de los protocolo MAC, en una topología similar a la que se muestra en la Figura 2.10

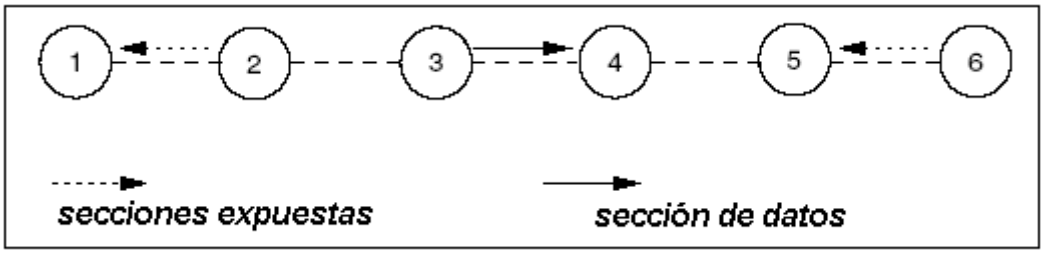


Figura 2. 10 ICSMA

Cuando existe una transmisión en curso entre los nodos 3 y 4, los otros nodos en la red es decir los nodos 2 y 6 no están autorizados a transmitir a los nodos 1 y 5 respectivamente. Esto se debe a dos razones: (a) ninguna transmisión simultánea del nodo 2 es posible por su propio mecanismo de censar portadora y (b) el reconocimiento de los paquetes recibidos por el nodo 3 también puede colisionar por la transmisión del nodo 2. Del mismo modo el nodo 6 es impedido para la transmisión porque el reconocimiento de los paquetes originados por el nodo 5 que podrían colisionar con la recepción de los paquetes de datos del nodo 4. Por lo tanto, los nodos 2 y 6 son designados como transmisor-receptor respectivamente.

ICSMA es un sistema de dos canales de intercambio de paquetes. En comparación con el esquema CSMA/CA, el protocolo de proceso es intercalado entre los dos canales. Por ejemplo en la figura 2.10 (a), si un remitente RTS transmite en el canal 1 y si el receptor está dispuesto a aceptar la petición, envía la correspondiente CTS en el canal 2. Si el emisor recibe el paquete CTS, comienza la transmisión de paquetes de datos sobre el canal 1. En el receptor, si el dato es recibido con éxito, responde con paquetes ACK en el canal 2. La figura 2.10 b ilustra el funcionamiento intercalado de ICSMA cuando un nodo (S) envía un paquete RTS a un nodo receptor (R). En la figura muestra la capacidad de transmisión simultánea entre los nodos A y B.

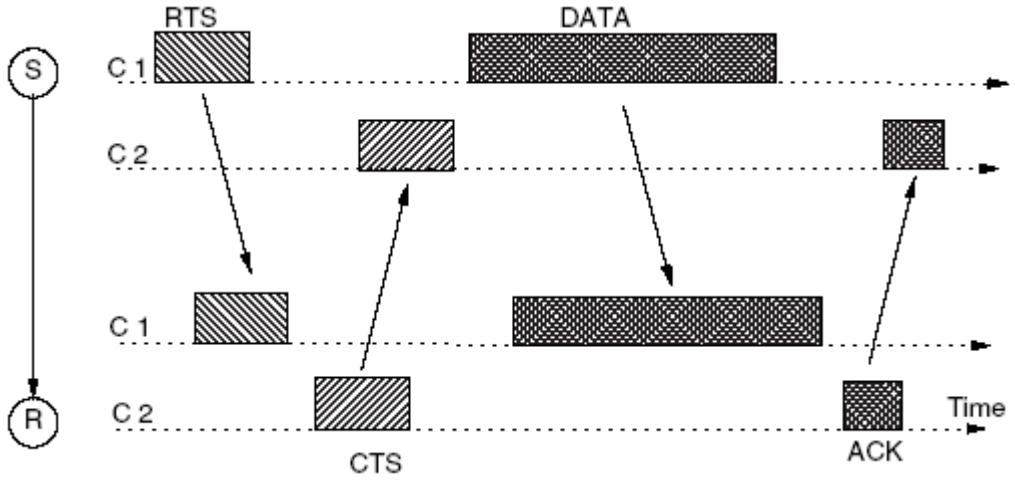


Figura 2. 11 **Paquetes intercalados para transmitir en ICSMA**

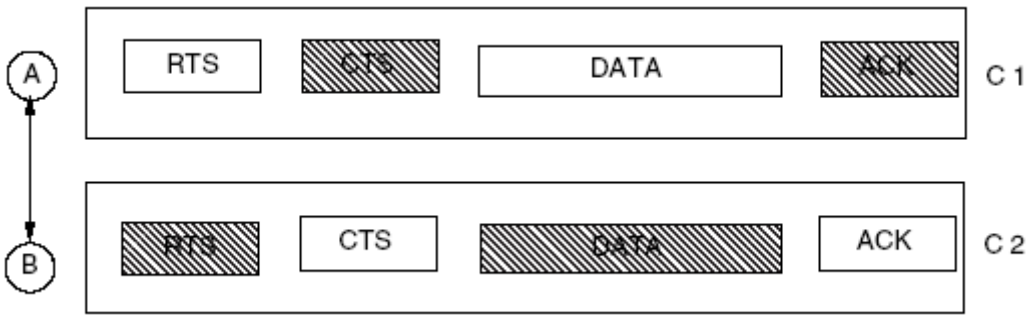


Figura 2. 12 **Transmisión simultánea entre dos nodos**

Este mecanismo, intercalado de la portadora aumenta el rendimiento alcanzado por los dos canales WMNs. El protocolo ICSMA utiliza una amplia red de distribución de vectores ENAV para determinar si un canal en particular está

libre para su transmisión. ENAV es una forma extendida de NAV utilizados para CSMA/CA.

2.7 PROTOCOLOS DE ENRUTAMIENTO DE UNA RED MESH

La tarea principal de los protocolos de ruteo es la selección de el camino entre el nodo fuente y el nodo destino. Esto tiene que ser hecha de una manera confiable, rápida, y con gastos indirectos mínimos. En general, los protocolos de ruteo pueden ser clasificados en los basados en topología y en los basados en posición. Los protocolos de ruteo basados en topología seleccionan trayectorias basadas en información topológica, como por ejemplo los enlaces de nodos. Los protocolos de ruteo basados en posición seleccionan trayectorias basadas en la información geográficas con algoritmos geométricos.

También hay protocolos que combinan esos dos conceptos. Los protocolos de ruteo híbridos tratan de combinar las ventajas de las 2 filosofías anteriores proactivo es usado para nodos cercanos o para caminos cercanos mientras que el ruteo reactivo es usado para nodos lejanos y por lo general caminos o rutas menos usadas.
En principio las redes *mesh* pueden manejar cualquier clase de protocolo de ruteo descrita anteriormente. Sin embargo no cada protocolo trabajará bien. La selección de un protocolo de enrutamiento conveniente depende del panorama, uso, y requisitos de funcionamiento.

2.7.1 REQUISITOS DE ENRUTAMIENTO EN LAS REDES WMNs

Un protocolo de asignación de ruta óptimo para redes WMNs debe cumplir con lo siguiente:

- **Tolerancia a fallos:** un problema importante en las redes es la supervivencia, que es la capacidad de la red para funcionar en caso de que un nodo falle. De la misma manera los protocolos de enrutamiento

también deberían permitir una nueva selección de ruta en caso de fallas.

- **Balanceo de carga:** los routers inalámbricos *mesh* son recomendados en el balanceo de carga porque ellos pueden escoger la ruta más eficaz para los datos.

- **La reducción del Enrutamiento *overhead*:** la conservación del ancho de banda es indispensable en el éxito de cualquier red inalámbrica. Es importante reducir la asignación de ruta *overhead*, sobre todo el causado por la retransmisión.

- **Escalabilidad:** una red mallada es escalable y puede ocuparse miles de nodos, ya que el funcionamiento de la red no depende de un punto mando central

.

- **QoS:** debido a la limitada capacidad del canal, la interferencia es un factor muy importante, el gran número de usuarios y las aplicaciones multimedia en tiempo real, apoyada por la calidad de servicio (QoS) se ha vuelto un requisito indispensable en redes de computadoras.

2.7.2 Protocolos basados topología (*Topology based*)

Los protocolos de ruteo basados en topología son separados en 2 categorías que son llamados reactivos, proactivos y los protocolos de ruteo híbrido. Los protocolos reactivos tales como AODV y DSR inician la determinación de las rutas solo si existe una petición Esto quiere decir que la información de la ruta solo está disponible cuando se recibe una petición, utilizando este tipo de implementaciones pueden existir retardos significativos antes de que la ruta al destino pueda ser determinada. También será necesario hacer cierto control de tráfico mientras se busca la ruta. En los protocolos proactivos como OLSR y

OSPF, intentan establecer todas las rutas con la red. Esto significa que cuando se necesita una ruta, esta ya es conocida y puede usarse de forma inmediata.

2.7.3 AODV (Ad Hoc On-Demand Vector Routing)

AODV es un protocolo de ruteo muy popular para MANETs el cual es un protocolo de ruteo reactivo. Este protocolo permite el enrutamiento dinámico, autoarranque y *multihop* entre todos los nodos móviles que participan en la red.

AODV permite a todos los nodos obtener las rutas rápidamente para las nuevas destinos y no requiere que los nodos mantengan las rutas hacia los destinos que no están activos en la comunicación.

El protocolo de enrutamiento está diseñado para redes móviles ad hoc con gran cantidad de nodos y con distintos grados de movilidad. Este protocolo se basa en que todos los nodos tienen que confiar en los otros para transportar sus datos, aunque sea por el uso de una clave preconfigurada, o activando mecanismos para evitar la participación de nodos intrusos.

Una característica distintiva de este protocolo es el uso del número de secuencia para cada ruta. Este número de secuencia es creado por el destino para ser incluido con la información necesaria para los nodos que requieren la información. El uso de estos números implica que no se crean *bucles* y la facilidad de programación.

Este protocolo define tres tipos de mensajes: *Route Requests* (RREQs), *Route Replies* (RREPs) y *Route Errors* (RERRs). Estos mensajes se reciben vía UDP. Mientras todos los nodos tengan las rutas correctas de cada nodo el protocolo no intercambia mensajes ni tiene ninguna función. Cuando una ruta hacia un nuevo destino es necesaria, el nodo que la necesita envía una mensaje *broadcast* RREQ que llega al destino, o a un nodo intermedio que tiene una ruta suficientemente “fresca” hacia el destino. Una ruta es “fresca” cuando el número de secuencia hacia el destino es como mínimo tan grande como el

número que contiene el RREQ. La ruta se considera disponible por el envió de un mensaje RREP hacia el nodo que originó el RREQ. Los nodos monitorizan el estado de las conexiones de los nodos, a un salto, participantes en las rutas activas. Cuando una conexión se rompe en una ruta activa, se envía un mensaje RERR para notificar a los otros nodos la pérdida de la conexión.

Este protocolo tiene una tabla de rutas. La información de la tabla de rutas debe guardarse incluso para las rutas de corta vida. Los campos que tiene cada entrada de la ruta son los siguientes:

- IP de destino.
- Número de secuencia de destino.
- *Flag* número de secuencia de destino válido.
- Otros estados y *flags* de enrutamiento (válido, invalido, reparable...).
- Interfaz de red.
- Contador de saltos.
- Salto siguiente.
- Listado de precursores.
- Tiempo de vida.

2.7.3.1 Mantenimiento de números de secuencia

Cada entrada de la tabla de cada nodo debe incluir la última información sobre el número de secuencia para la dirección IP del nodo destino. Este número de secuencia se llama “número de secuencia de destino”. Se actualiza cada vez que un nodo recibe nueva información del número de secuencia por los mensajes RREQ, RREP o RERR. Este protocolo depende de que cada nodo de la red mantenga su propio número de secuencia de destino para garantizar que no haya bucles. Un nodo destinatario incrementa su propio número de secuencia en dos circunstancias:

- Inmediatamente antes que un nodo origine el descubrimiento de una ruta, debe incrementar su propio número de secuencia.

- Inmediatamente antes que el nodo destino origine un mensaje RREP como respuesta a un RREQ, este nodo debe actualizar su número de secuencia, eligiendo el valor máximo entre su actual número de secuencia o el número del paquete RREQ que le ha llegado.

2.7.3.2 Entradas de la tabla de enrutamiento

Cuando un nodo recibe un paquete de control desde un vecino, crea o actualiza una ruta hacia un destino particular o una subred, el nodo comprueba su tabla de enrutamiento por una entrada para el destino. La ruta se actualiza en los siguientes casos:

- El número de secuencia es mayor que el que hay en la tabla de enrutamiento.
- El número de secuencia es igual, pero el nuevo valor del contador de saltos más uno, es menor que el valor que tenia la ruta de la tabla de enrutamiento.
- El número de secuencia es desconocido.

Las entradas de la tabla tiene un campo de tiempo de vida, este tiempo se determina por el paquete de control que llega, o se toma un valor determinado.

2.7.3.2 Generación de peticiones de rutas

Un nodo envía un mensaje RREQ cuando determina que necesita saber la ruta hacia un destino y no lo tiene en su tabla de enrutamiento o es una entrada no válida. En ese momento se envía un mensaje RREQ con el valor del número de secuencia de destino igual al último número conocido para este destino. El valor del número de secuencia de origen en el mensaje RREQ es el número de secuencia del nodo que es incrementado antes del envío del mensaje.

Al tener en cuenta que las comunicaciones son bidireccionales, además de la ruta para llegar al destino también es necesario saber una ruta de vuelta. Para este cometido cualquier nodo intermedio que genere un mensaje de respuesta (RREP) debe también realizar una acción que notifique al nodo destino una ruta de vuelta hacia el nodo origen.

Para no crear congestión en la red ni hacer que los mensajes circulen indefinidamente por ella, el nodo que origina peticiones debe indicar un TTL máximo a los mensajes y además seleccionar un *timeout* para esperar una respuesta. Tanto el *timeout* como el TTL son calculados de manera periódica y tiene en cuenta el tamaño de la red y el tiempo que tarda un paquete en cruzarla.

2.7.3.4 Procesamiento y retransmisión de peticiones de ruta

Cuando un nodo recibe un RREQ, crea o actualiza una ruta hacia el salto anterior. Posteriormente comprueba que no haya recibido una mensaje con el mismo ID y origen y si lo ha recibido descarta este nuevo mensaje. En este apartado se explicará las acciones que se realizan cuando este mensaje no se descarta.

Lo primero que se hace es aumentar el valor del contador de saltos en uno. Después, el nodo busca una ruta hacia la IP origen del mensaje. Si no existe se debe crear esta nueva ruta de vuelta. Una vez se ha creado esta ruta de vuelta se siguen las siguientes acciones:

- El número de secuencia origen se compara con el número de secuencia hacia el destino que se tiene en la tabla, y si es mayor se copia en ella.
- Se valida el campo de número de secuencia.
- El siguiente salto en la tabla de enrutamiento se convierte el nodo desde donde nos ha llegado el mensaje.

- Se copia el número de saltos en la tabla de enrutamiento.

2.7.3.5 Generación de respuesta de ruta

Un nodo genera un mensaje RREP si él mismo es el destino, o tiene una ruta activa hacia el destino y el número de secuencia de la entrada de la tabla es mayor que el del mensaje RREQ. Una vez se genera el RREP el nodo descarta el mensaje RREQ.
Si un nodo no genera un RREP y el valor del TTL es mayor de uno entonces actualiza y envía el mensaje RREQ a una dirección *broadcast*.

Si el nodo que genera el mensaje RREP no es el nodo destino sino que es un nodo intermedio, copia su propio número de secuencia para el destino en el campo de número de secuencia destino del mensaje RREP. Entonces este nodo intermedio actualiza la ruta de retransmisión poniéndose a él como último nodo en la lista de precursores.

2.7.3.6 Recepción y retransmisión de respuesta de ruta

Cuando un nodo recibe un mensaje RREP busca una ruta hacia el salto anterior, si es necesario se crea esta ruta. Posteriormente el nodo incrementa el contador de saltos en el mensaje. Entonces se crea una ruta para llegar al destino si no existe. De otra manera, el nodo compara el número de secuencia de destino del mensaje con el que tiene guardado. Después de la comparación la ruta existente se actualiza en los siguientes casos:

- El número de secuencia en la tabla de enrutamiento está marcado como inválido.
- El número de secuencia de destino en el mensaje es mayor que el que el nodo tiene guardado y el valor es válido.

- Los números de secuencia son iguales pero la ruta está marcado como inactiva.
- Los números de secuencia son los mismos, y el nuevo valor del contador de saltos es menor.

Cuando se actualiza una entrada en la tabla la ruta se marca como activa, el número de secuencia de destino también se marca como válido y en el siguiente salto en la entrada de la tabla se asigna el nodo del que ha llegado el mensaje RREP. También se debe actualizar el nuevo valor del contador de saltos, el tiempo de expiración de la ruta y el número de secuencia de destino, se debe actualizar por el número de secuencia del mensaje RREP[12].

2.7.3.7 Mensajes de error (RERR)

Normalmente una ruta errónea o el corte de un enlace necesitan un procedimiento similar. Primero invalidar las rutas existentes, listar los destinos afectados, determinar los vecinos afectados y enviar un mensaje apropiado RERR a estos vecinos.

Un nodo inicia el procesamiento de un mensaje RERR en tres situaciones:

- Si detecta la caída de un enlace para el siguiente salto de una ruta activa en su tabla de enrutamiento mientras envía datos.
- Si recibe un paquete de datos hacia un nodo del que no tiene ninguna ruta activa.
- Si recibe un mensaje RERR desde un vecino por una o más rutas activas.

2.7.4 DSR (*Dynamic Source Routing*)

[12] *Wireless* mesh network "Introduction to *wireless* mesh networking" mayo 2005 Gilbert Held, cap 4 pág 60- 75

El protocolo DSR se fundamenta en el encaminamiento desde el origen, es decir, los paquetes de datos incluyen una cabecera de información acerca de los nodos exactos que deben atravesar. No requiere ningún tipo de mensajes periódicos (reactivo), disminuyendo así la sobrecarga con mensajes de control. Además ofrece la posibilidad de obtener, con la solicitud de una ruta, múltiples caminos posibles hacia el destino. Tampoco son un problema, a diferencia de la mayoría de protocolos de encaminamiento en este tipo de redes, los enlaces unidireccionales. Para poder realizar el encaminamiento en el origen, a cada paquete de datos se le inserta una cabecera DSR de opciones que se colocará entre la cabecera de transporte y la IP. Entre dichas opciones se incluirá la ruta que debe seguir el paquete nodo a nodo. Cada nodo mantiene una memoria caché de rutas en la que se van almacenando las rutas obtenidas a través de procesos de descubrimiento de rutas ya sean propios o obtenidos a través de escuchas en la red. En los procesos de descubrimiento de rutas se generan mensajes de solicitud, respuesta y error siendo estos mensajes *ROUTE REQUEST, REPLY y ERROR* respectivamente.

2.7.5 OSPF (*OPEN SHORTEST PATH FIRST*)

El protocolo OSPF (Iniciar con la primera ruta más corta), propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red y el mantenimiento de bases de datos con información sobre sistemas locales y vecinos. De esta manera es capaz de calcular la métrica para cada ruta, entonces se eligen las rutas de encaminamiento más cortas.

Todos los routers de OSPF tienen una base de datos detallada con la información necesaria para construir un árbol de encaminamiento del área, con la descripción de las interfaces, conexiones y métricas de los routers. Además de todas las redes de multiacceso[13] y una lista de todos los routers de la red.

Los routers envían periódicamente mensajes de saludo (*Hello*), para que el resto de los routers sepan que siguen activos. También envían mensajes de

[13] Sistema que permite a varios usuarios hacer uso de un mismo ordenador simultaneamente

saludo al otro extremo de un enlace punto a punto o un circuito virtual para que estos vecinos sepan que siguen atentos.

Una de las razones por las que funcionan los mensajes de saludo es que un mensaje contiene la lista de todos los identificadores de los saludos cuyos vecinos escucharán el emisor, así los routers conocen si se les está escuchando en la red.

2.7.5.1 Tipos de mensajes OSPF

Los cinco tipos de mensajes del protocolo OSPF que se utilizan son:

- **Saludo:** se usa para identificar a los nodos vecinos.
- **Descripción de la base de datos:** durante la inicialización, se usa para intercambiar información de manera que un router puede descubrir los datos que le faltan en la base de datos.
- **Petición del estado del enlace:** se usa para pedir datos cuando un router se ha dado cuenta que le faltan datos en su base de datos o que están obsoletos.
- **Actualización del estado del enlace:** se usa como respuesta a los mensajes de petición del estado del enlace y también para informar dinámicamente de los cambios en la topología de la red.
- **ACK[14] de estado del enlace:** se usa para confirmar la recepción de una actualización del estado del enlace. El emisor retransmitirá hasta que se confirme.

2.7.5.2 Router designado

En una red multiacceso, los mensajes de saludo también se usan para identificar a un Router designado. El router designado cumple dos funciones:

[14] Mensaje que se envía para confirmar que un mensaje o un conjunto de los mismos han llegado

1. Es responsable de la actualización fiable de sus vecinos adyacentes con la información más reciente de la topología de la red.
2. Crea avisos de enlaces de red con la lista de todos los routers conectados a la red multiacceso.

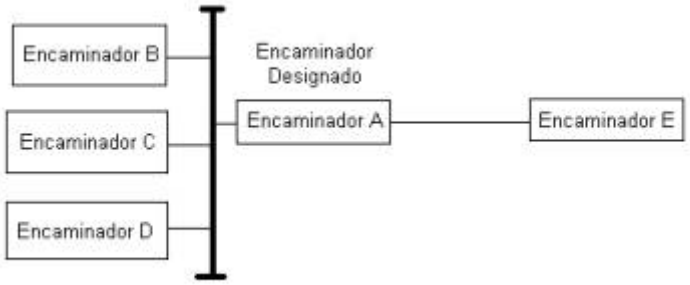


Figura 2. 13 Dibujo de router designado

El router designado A intercambia información con los routers B, C y D de su LAN así con el router E conectado con su enlace punto a punto. El router designado A actúa como experto local y mantiene actualizada la topología local completa.

Después comunica a los routers adyacentes la información. B, C y D mantienen sus propias bases de datos sincronizadas hablando con A. No tienen que hablar con los otros, así se reduce drásticamente el tráfico de información. Dos routers que sincronizan sus bases de datos uno con otro se llaman adyacentes. B y C son vecinos, pero no son adyacentes el uno del otro debido a que consultan con A.

2.7.5.3 Sistemas autónomos de área

Un área es un conjunto de redes y host contiguos, junto con routers con interfaces a estas redes. Un sistema autónomo que use OSPF está construido por una o más áreas. Cada área tiene asignado un número. El área 0 está

conectada al *Backbone* que enlaza con el resto de áreas y agrupa al resto de sistemas autónomos.

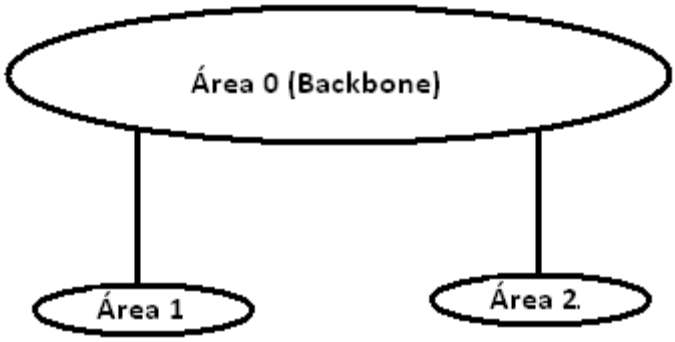


Figura 2. 14 Backbone y áreas en OSPF[15]

La red agrupa las áreas. El *backbone* contiene todos los *routers* que pertenecen a múltiples áreas, así como las redes y *routers* no asignados a ninguna área. Se debe recordar que las áreas están numeradas y que el *backbone* es el área 0. Un router frontera pertenece a una o más áreas y al *backbone*[16].

2.7.5.4 Encaminamiento de área en OSPF

El encaminamiento dentro de un área se basa en un mapa completo de estado de enlace del área. Todos los routers con OSPF implementado en un área mantienen una base de datos de encaminamiento idéntica que describe la topología y estado de todos los nodos de esa área. La base de datos se usa para construir el mapa de esa área. Siempre que ocurre un cambio, la información se propaga por toda el área. De esta forma siempre los routers estarán en un estado óptimo para cualquier petición. Un router que esté arrancando obtendrá una copia de la base de datos actual de encaminamiento de su vecino más cercano (vecino se denomina a cualquier router que esté en su área).

---

[15] http://images.google.com.ec/imgres?imgurl=http://www.cisco.com/en/US/i/100001-200000/140001-150000/141001-142000/141451.jpg&imgrefurl=http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/L3VPNCon.html&usg=__iLMgC2W6OQ52e6NWID5wPYnE3EI=&h=369&w=678&sz=32&hl=es&start=2&itbs=1&tbnid=hyHwHDi9IFdu1M:&tbnh=76&tbnw=139&prev=/images%3Fq%3Dbackbone%2By%2Barea%2B0%26gbv%3D2%26ndsp%3D21%26hl%3Des%26sa%3DN

[16] Se refiere a las principales troncales de la red

El router de frontera conoce la topología completa de las áreas a las que está conectado. Estos routers resumen la información de área e indican a otros routers del *backbone* lo lejos que están de las redes dentro de su propia área.

De esta forma todos los routers frontera pueden calcular las distancias a destinos fuera de sus propias áreas y transmitir esta información dentro de sus propias áreas.

2.7.5.5 Destino fuera de los Sistemas Autónomos de OSPF

Muchos sistemas autónomos están conectados a Internet, o a otros sistemas autónomos. Los enrutadores límite de OSPF ofrecen información sobre distancias a las redes externas al sistema autónomo.

Existen dos tipos de métricas de distancia externa de OSPF. La de tipo 1 es equivalente a la métrica local de estado del enlace. Las métricas de tipo 2 de larga distancia, se miden con un mayor orden de magnitud.

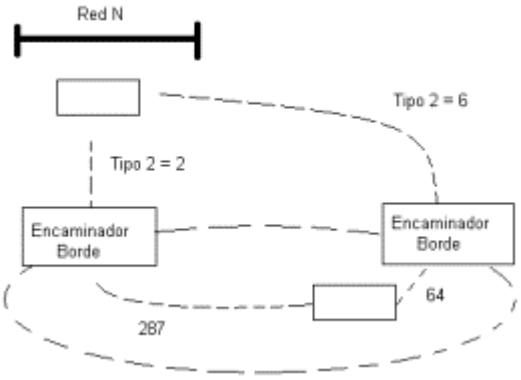


Figura 2. 15 Grafica de elección de métrica

En la grafica vemos que existen dos rutas, hemos elegido la métrica de tipo 2, para llegar a la red externa vemos que eligiendo la de tipo 2 la más corta es la de valor 2. Otra característica de OSPF conveniente para los Proveedores de Servicios Internet es que un router límite de un sistema autónomo puede

comportarse como un servidor de encaminamiento y puede informar de las entradas que identifican las rutas a otros routers límite.

2.7.5.6 Wireless

El protocolo OSPF tiene un gran funcionamiento para redes cableadas pero tiene distintos problemas en las redes sin cables como la aleatoriedad y los cambios continuos de la infraestructura. Para solucionar estos problemas se desarrollan versiones posteriores que incluyan funcionalidades de enrutamiento MANET (*Mobile Ad-hoc NETwork*).

En este sentido se han desarrollado distintos proyectos intentando dar una solución a los distintos problemas que tienen las redes sin cables. Aún no existe ningún estándar en este sentido y se está trabajando en ellos desde distintas perspectivas:

- Establecimiento del problema para extensiones OSPF para enrutamiento móvil Ad-hoc. En las redes ad hoc muchas de las características y capacidades de OSPF son necesarias. En este documento trata de explicar los cambios necesarios que se deberían hacer para que este protocolo funcionara correctamente en redes de este tipo.
- Consideraciones de diseño para una interface OSPF inalámbrica. En este proyecto se presentan análisis y resultados de simulaciones de un diseño del protocolo OSPF con interfaces inalámbricas.
- Tipo de interfaz inalámbrica OSPFv2. Describe mejoras al protocolo OSPFv2 para el soporte de interfaces inalámbricas, con capacidad *broadcast* y para redes *multi-hop*.
- Extensiones a OSPF para soportar redes móviles Ad-hoc. Este documento especifica un mecanismo para la señalización local de enlaces, una interfaz SPF-MANET, un método para reducir el tamaño de los paquetes *Hello* y un método para optimizar la inundación de actualizaciones de enrutamiento.

- Extensión MANET de OSPF usando inundación CDS. Describe y evalúa una familia de métodos de inundación para las redes ad hoc.

Los principales problemas que suponen este tipo de redes al protocolo OSPF son las siguientes:

- Movilidad y cambios de la geografía en la que se encuentran los nodos (routers) puede llevar a muchas situaciones complejas con vecinos que tienen cobertura por dos routers distintos, o dificultan la elección del mejor camino hacia el destino.
- Adaptación de la red al entorno gráfico. Posibilidad de usar antenas direccionales o no.
- Minimización del tráfico retransmitido. En OSPF hay optimizaciones de inundación de mensajes como el uso de DR, pero estas optimizaciones son basándose en redes con multiacceso. Sin embargo, las redes inalámbricas muchas veces no cumplen esta característica, y no se puede asumir que la conectividad es en ambos sentidos. Por este motivo estas optimizaciones no son óptimas si no se combinan con otras como la inundación del estado de los enlaces (LSF). Se debe utilizar un mecanismo que permita sincronizar la información de todos los nodos del segmento.
- Limitar transmisión. Se debe minimizar también el tráfico originado. Una solución estudiada es la de que los nodos envíen un mensaje LSA y asuman que se encuentran en la base de datos LSA hasta que no sea explícitamente retirado.
- Control de potencia. Al ser dispositivos móviles que pueden actuar con baterías es muy importante el uso que se le da. Los dispositivos que utilicen este tipo de energía sólo actuarán y retransmitirán mensajes siempre que sea necesario porque ningún otro vecino pueda encargarse.
- Gran número de vecinos inmediatos. En una interfaz inalámbricas puede haber un gran número de vecinos adyacentes, además en este tipo de redes puede haber un gran número de nodos con características de

routers. Por estos dos motivos los protocolos que trabajen en este tipo de redes deben poder dar soporte a un gran número de adyacencias y permitir fácilmente la llegada de nuevos vecinos.

- Movilidad rápida. La topología de este tipo puede cambiar bruscamente y un gran número de veces en poco tiempo cuando la red es muy densa, estos cambios tan variados no pueden llevar a un gran número de mensajes que colapsen la red para la creación de adyacencias o la caída de enlaces. Por este motivo deben haber cambios en el establecimiento de vecinos, resumen de topologías e inundación de mensajes LSA.

Inundación fiable o no. Para la inundación de mensajes LSA se puede utilizar transmisión *multicast*[17] pero el reconocimiento llegará desde cada vecino. Esto hace que aumente considerablemente el tráfico, se ha trabajado con distintas soluciones para minimizar este tráfico como TBRPF (*Topology Dissemination Based on Reverse-Path Forwarding*) que tiene routers que transmiten los LSAs hacia sus vecinos necesarios para que estos puedan calcular las rutas hacia ellos mismos, asumiendo que otros mensajes LSA llegarán hacia ellos por otras rutas si realmente son necesarios.

2.7.6 OLSR (Optimized Link State Routing Protocol)

OLSR es un protocolo de ruteo proactivo para *wireless* ad hoc *netwoks*. Este protocolo desarrollado para redes móviles ad hoc, opera en modo proactivo.

Cada nodo selecciona un grupo de nodos vecinos como *"multipoint relay*[18]*"* (MPR), en este caso sólo los nodos seleccionados como tales son responsables de la retransmisión de tráfico de control. Estos nodos también tienen la responsabilidad de declarar el estado del enlace a los nodos que los tienen seleccionados como MPR.

[17] Servicio de red en el cual el único flujo de datos puede ser enviada simultáneamente para diversos destinatarios

[18] Un nodo que es seleccionado por un nodo vecino para retransmitir todos los mensajes *broadcast* que recibe el nodo

Es muy útil para redes móviles densas y grandes, porque la optimización que se consigue con la selección de los MPR trabaja bien en estos casos. Cuanto más grande y densa sea una red mejor es la optimización que se consigue con este protocolo. OLSR utiliza un enrutamiento salto-a-salto, es decir, cada nodo utiliza su información local para enlutar los paquetes. La selección de los nodos MPR reduce el número de retransmisiones necesarias para enviar un mensaje a todos los nodos de la red. OLSR optimiza la reacción a cambios en la topología reduciendo el intervalo de transmisión de los mensajes periódicos de control. Como este protocolo mantiene rutas hacia todos los destinos de la red trabaja muy bien en redes donde el tráfico es aleatorio y esporádico entre un gran número de nodos.

OLSR trabaja de manera distribuida sin ninguna entidad central. Este protocolo no requiere transmisiones seguras de mensajes de control porque los mensajes son periódicos, y se pueden permitir algunas pérdidas. Tampoco necesita una recepción de mensajes secuencial, se utiliza números de secuencia incrementales para que el receptor sepa que información es más reciente.

2.7.6.1 Funcionamiento núcleo

El núcleo especifica el comportamiento de un nodo que tiene interfaces OLSR. Se basa en las siguientes funcionalidades:

- Formato de paquete y retransmisión: OLSR se comunica mediante un formato de paquete unificado para todos los datos del protocolo. El propósito de esto es facilitar la extensión del protocolo. Estos paquetes se envían como datagramas UDP. Cuando recibimos un paquete básico, un nodo examina el mensaje, y basándose en un campo donde se indica el tipo de mensaje determinará el procesamiento del mensaje que seguirá los siguientes pasos:

  - Si el paquete no contiene mensaje (el tamaño es demasiado pequeño) se descarta.
  - Si el valor del TTL[19] es menor o igual que 0 también se descarta.
- Condiciones de proceso: Si es un mensaje es duplicado (la dirección de origen y la número de secuencia ya se han tratado) no se procesa. En caso contrario el paquete es tratado de acuerdo al tipo de mensaje que haya llegado.
- Condiciones de retransmisión: Si es un mensaje duplicado no se retransmite, si no es duplicado se retransmite el mensaje siguiendo el algoritmo del tipo de mensaje.
- Percepción de enlace: Se consigue saber el estado del enlace mediante el envío de mensajes "*HELLO*". El propósito de esta funcionalidad es que cada nodo tenga asociado un estado en el enlace a cada uno de sus vecinos. El estado puede ser simétrico (enlace verificado es bidireccional) y asimétrico indica que los mensajes "*HELLO*" se han escuchado pero no podemos asegurar que este nodo escuche las respuestas.
- Detección de vecino: Dada una red de nodos con sólo una interfaz, un nodo debe deducir los vecinos que tiene mediante la información intercambiada durante la percepción de enlace. Cada nodo debe tener guardados su grupo de vecinos. Cada vecino debe tener asociado el estado del enlace. Cuando se detecta la aparición de un nuevo enlace, se debe crear una entrada con un vecino que tiene un enlace asociado, en esta entrada también se debe guardar el estado de este enlace. Se debe tener en cuenta que cada vez que varía el estado del enlace se debe comprobar en la tabla que el cambio se lleva a cabo. Si no se recibe información de un enlace durante un tiempo establecido se debe borrar el enlace en cuestión y el vecino asociado.
- Selección de MPR y señalización MPR: La selección de los MPR sirve para seleccionar los nodos vecinos que se quiere que hagan *broadcast* de los mensajes de control. La señalización viene dada mediante mensajes "*HELLO*". Cada nodo elige uno o más MPRs de manera que

[19] Contador de tiempo de vida que decrece con cada salto o por esperar en la cola

se asegura que a través de los MPRs seleccionados, cada nodo llega a todos los vecinos a dos saltos.

- Difusión de mensajes de control de topología. Estos mensajes se difunden con el objetivo de dar a cada nodo de la red la información necesaria para permitir el cálculo de rutas, son llamados mensajes TC (*Topology Control*). Estos mensajes que retransmite un nodo hacia sus vecinos seleccionados como MPR, tienen la información de todos sus enlaces para que los otros nodos conozcan los vecinos a los que puede llegar.
- Cálculo de rutas: Dada la información del estado del enlace que se adquiere mediante el intercambio de mensajes periódicos. Cada nodo mantiene una tabla de enrutamiento que permite encaminar los paquetes de datos destinados a otros nodos. Esta tabla esta basada en la información contenida en las bases de información de enlace y de la topología. Esta tabla se actualiza cuando se detecta algún cambio en estos campos:

    - El enlace
    - El vecino
    - El vecino de dos saltos
    - La topología

Funciones auxiliares: Hay situaciones donde funcionalidades auxiliares son necesarias, como por ejemplo un nodo con múltiples interfaces, donde algunas de ellas participan en el otro dominio de enrutamiento.

Interfaces no OLSR: Hay nodos que pueden tener interfaces que no son OLSR, estas interfaces pueden ser conexiones punto a punto o conectar con otras redes. Para poder tener conectividad entre las interfaces OLSR y estas otras el router debe ser capaz de introducir información externa de encaminamiento a la red. Para esto las interfaces no OLSR crean un mensaje *Host and Network Association* (HNA) que contiene información suficiente para poder crear nuevas rutas con esta información.

Notificación capa enlace: OLSR no trabaja con información de capa enlace. Sin embargo, si la información de esta capa está disponible, esta información se utiliza además de la información de los mensajes "*HELLO*", para mantener información de los vecinos y los MPR. Por ejemplo: la pérdida de conectividad de la capa de enlace se puede deber a la ausencia de reconocimientos de capa de enlace.

Información redundante de topología: Para poder proveer redundancia a la información de topología, la información de anuncio que emite el nodo ha de tener información de enlaces hacia nodos vecinos que no necesariamente tengan a este nodo como MPR. El mensaje de anuncio publica información de todos los enlaces de los nodos vecinos. Hay tres posibles niveles de redundancia:

- Sin redundancia: sólo se emite información del grupo que ha elegido a este nodo como MPR.
- Redundancia media: se emite información del grupo que ha elegido el nodo como MPR y también información de los nodos que este ha elegido como MPR.
- Redundancia alta: se emite información de todos los enlaces hacia los vecinos.

MPR redundante: Esta funcionalidad especifica la habilidad del nodo de seleccionar MPR redundantes. Aunque la redundancia crea mucho más tráfico y pierde eficiencia el mecanismo de MPR, se tiene una gran ganancia al asegurar la llegada de los paquetes a sus destinos. Esta funcionalidad es útil para situaciones en que la red tiene mucha movilidad y mantener una buena cobertura con los MPR.

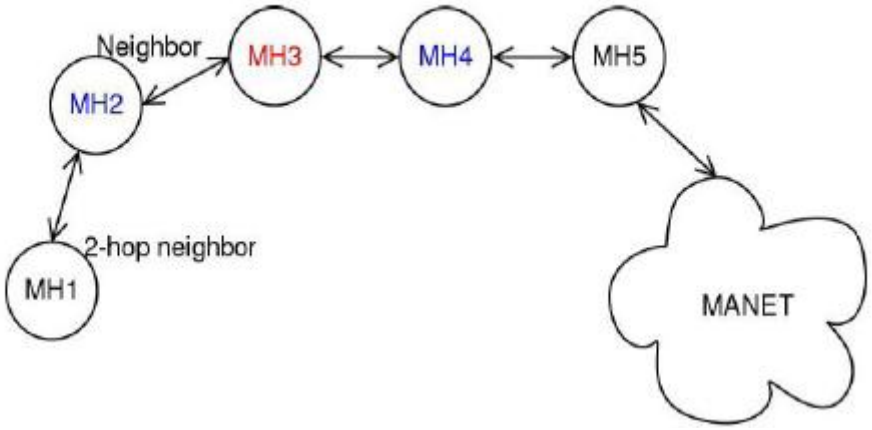


Figura 2. 16 Topología de la red

2.8 SEGURIDAD EN *WIRELESS* MESH NETWORKS

2.8.1 Descripción de la tecnología en seguridad

Esta sección da una descripción de la tecnología utilizada para la seguridad básica que es necesaria para WMNs. Aquí se hará un resumen general sobre la seguridad en las *wireless mesh networks.* Las WMN se exponen a las mismas amenazas básicas comunes de las redes alambradas e inalámbricas: los mensajes pueden ser interceptados, modificados, retrasados, reenviado, o los nuevos mensajes pueden ser insertados. Una red que posee recursos importantes, se podría acceder sin autorización. Los servicios de seguridad que por lo general tratan de combatir estas amenazas son:

- Confidencialidad: Los datos se revelan solamente en las entidades o personas interesadas.

- Autentificación: Una entidad tiene de hecho la identidad que demanda tener, es decir, reconocimiento de los usuarios dueños del servicio.

- Control de acceso: Se asegura de que solamente las acciones autorizadas puedan ser realizadas.

- No negación: Protege las entidades que participan en un intercambio de la comunicación puede negar más adelante algo falso que ocurrió el intercambio.

- Disponibilidad: Se asegura de que las acciones autorizadas puedan tomar lugar.

Los Servicios de seguridad en el futuro serán mucho más restringidos buscando para el usuario privacidad (anonimato, seudonimidad, usuario perfilado, y *tracking*) y la confidencialidad del tráfico.

La protección del tráfico de comunicación implica: la confidencialidad (cifrado), la autentificación de los socios de la comunicación, así como la protección de la integridad y de la autenticidad de mensajes intercambiados.

La protección de la integridad se refiere no sólo a la integridad del mensaje, sino también al orden correcto de los mensajes relacionados (reenvío, el reordenamiento, o cancelación de mensajes). Esta sección describe la tecnología de protección para el tráfico de la comunicación. Estas tecnologías pueden también ser utilizadas dentro de una red *mesh* para autenticar los nodos *Mesh* (MNs) y para establecer las llaves de la sesión que protegen la confidencialidad y la integridad del tráfico intercambiado entre MNs.

El tráfico de la comunicación puede ser protegidas por diversas capas (capa de enlace, capa de red, capa de transporte y capa de aplicación): especialmente en sistemas inalámbricos, (GSM, UMTS, DECT, IEEE 802.11 WLAN, *Bluetooth*, 802.16 WiMax), que incluye medios de proteger el enlace inalámbrico. Éstos utilizan diversos esquemas de encapsulación de tramas, diversos protocolos de autentificación, y diversos algoritmos criptográficos[20].

Redes de área local inalámbricas (WLAN) basada en IEEE 802.11i (acceso de Wi-Fi *Protected*: WPA, WPA2) apoya dos modos de seguridad: también una

[20] *Wireless* mesh networking "Architectures, Protocols and Standards" 2006
Yan Zhang, Jijun Lou, Hoglin Hu pág 183-225

shared key (llaveo compartida) es configurada en los dispositivos de WLAN (*preshared* llaveo [PSK]), que es de uso frecuente en las redes caseras, los usuarios pueden ser autenticados con un servidor autentificador (servidor AAA). Para este propósito, se utiliza el protocolo extensible de autentificación (extensible *authentication protocol*) (EAP).

La autentificación real ocurre entre la estación móvil (MS) y el servidor AAA Usando EAP (véase Fig.2.17). El EAP es transportado entre el MS y el punto de acceso (AP) que usan EAPOL, y entre el AP y el servidor AAA por el protocolo RADIUS. Si es habilitado el nodo, una sesión maestra de llaveo (MSK) es utilizada, el cual se envía desde el servidor de la autentificación (AS) al WLAN AP. Se utiliza como entrada al WLAN

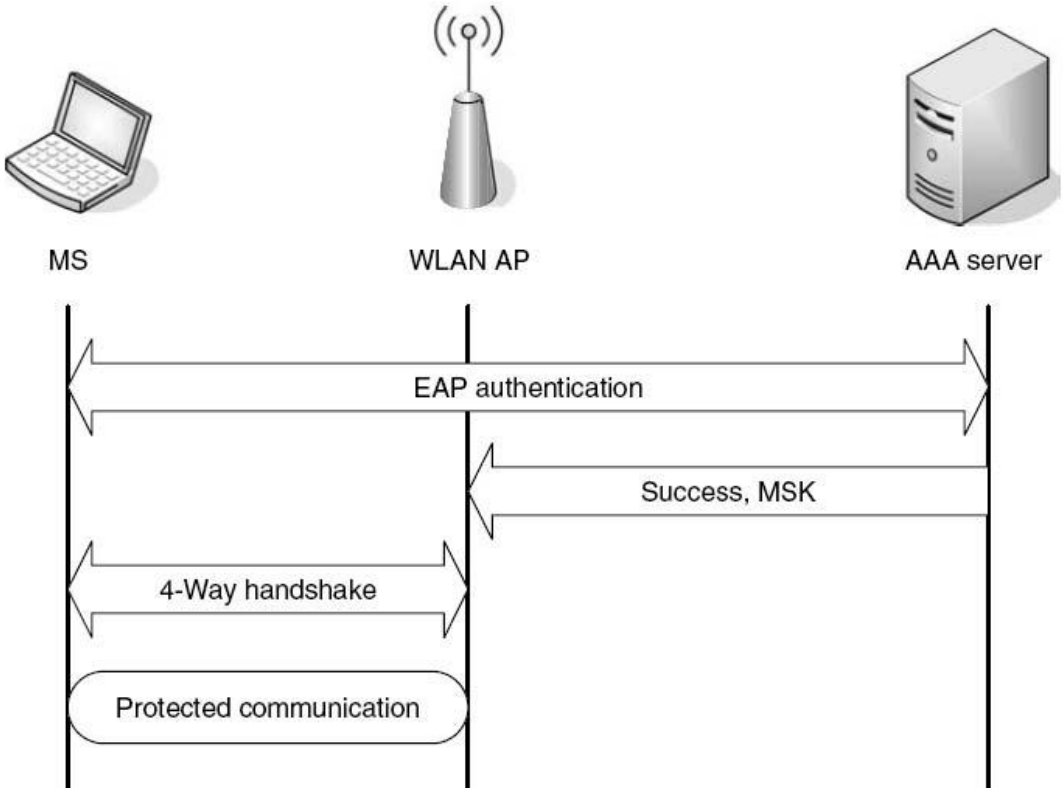


Figura 2. 17 Acceso a WLAN basada en EAP[21]

Hay 4 maneras que establece una sesión de llaveo temporal para proteger el enlace inalámbrico. Esta llave se utiliza realmente para proteger el tráfico del usuario, usando cualquier protocolo dominante temporal de la integridad

[21] *Wireless* mesh networking "Architectures, Protocols and Standards" 2006
Yan Zhang, Jijun Lou, Hoglin Hu

([TKIP], la parte de WPA) o AES-basado en CCMP (CTR con el protocolo de CBC-MAC, parte de WPA2). Los varios métodos de EAP existen para una autentificación basada en los certificados digitales, las contraseñas, o los protocolos móviles *reusing* de la autentificación de la red (EAP-SIM, EAP-AKA).

El acceso EAP-basado en WLAN se utiliza particularmente para las redes de la empresa y los *hot-spots* públicos donde está disponible una base de datos del usuario. El tráfico de la comunicación se puede también proteger en la capa enlace. IPsec protege tráfico IP en la capa de la red (IP). La arquitectura de IPsec especifica dos protocolos de seguridad: *ENCAPSULATION SECURITY PAYLOAD* (ESP) y *AUTHENTICATION HEADER* (AH). En el caso de ESP, ella encapsula solamente la carga útil (*payload*) del paquete del IP (modo del transporte) o del paquete entero del IP (modo del túnel). Una IPsec *security association* (SA) define las llaves (*keys*) y los algoritmos criptográficos para utilizar. Un SA es identificado por 3 cosas consistentes en: un IP *address* de la destinación, un identificador del protocolo (AH o ESP), y un índice del parámetro de la seguridad.

Este SA unidireccional se puede configurar explícitamente, o puede ser establecido dinámicamente, por ejemplo, por el protocolo del *Internet key Exchange* (IKEv2). Un uso común de IPsec son las redes privadas virtuales (VPN) para tener acceso con seguridad a un Intranet de la compañía. El tráfico de la comunicación se puede proteger en la capa de transporte usando el protocolo de la seguridad de la capa de transporte (TLS), que se basa en el encendido y es muy similar al *secure socket layer* (SSL). Su uso principal está para proteger El HTTP sobre TLS/SSL (https), pro esta puede también ser utilizada como protocolo independiente. Los protocolos TLS/SSL incluyen la autentificación y el establecimiento de *key´s* basado en certificados digitales.

Recientemente, la ayuda para *preshared* o compartir las llaves (PSK-TLS) también fue introducida. Es también posible a proteger el tráfico en capas más altas. Esto permite para realizar operaciones y aplicaciones específicas de la seguridad. Por ejemplo, los mails pueden ser encriptados (protección a la

confidencialidad) y/o ser señalados como (autentificación, la integridad, y no compartido del origen) que usa S/MIME o el PGP.

2.8.2 Ediciones de seguridad *Mesh*

Uno de los objetivos de las WMNs son diversificar las capacidades de redes ad hoc. Las redes ad hoc se pueden considerar realmente como subconjunto De WMNs. Ambas Comparten características comunes, tales como el *multihop, wireless,* topología dinámica, y membresía dinámica. Por otra parte, las *mesh* pueden tener infraestructura/*backbone wireless* y tener menos movilidad.

Los esquemas existentes de la seguridad propuestos para las redes ad hoc pueden ser adoptadas para WMNs. Sin embargo, la mayor parte de las soluciones de la seguridad para las redes ad hoc todavía no son bastante maduras para ser puestas en ejecución. Por otra parte, las diversas arquitecturas de red entre WMNs y las redes ad hoc pueden dar una solución para las redes ad hoc ineficaces en WMNs.

2.8.3 Desafíos para la seguridad

Los desafíos para la seguridad de las WMNs se basan en sus características topológicas. Analizando las características de WMNs y comparándolas con otras tecnologías de red, los autores demuestran que los nuevos desafíos de la seguridad son debido a las comunicaciones inalámbricas *multihop* y por el hecho de que los nodos no están protegidos físicamente.

El *Multihopping* es imprescindible para que WMNs amplíe la cobertura de redes inalámbricas actuales y proporcionar una *non-line-of-sight* (NLOS) en la conectividad entre los usuarios. El *Multihopping* retrasa la detección y el tratamiento de los ataques, hace encaminar un servicio de red crítico, los nodos confían en otros nodos para comunicarse, y la cooperación del nodo es así imprescindible. Mientras que el uso de enlaces inalámbricos hace una red

mesh susceptible a los ataques, la exposición física de los nodos permite que un adversario tome, clone, o trate de forzar a estos dispositivos.

Otros desafíos específicos para WMNs son:

- Las WMN puede ser dinámicas debido a cambios en su topología y su membresía (es decir, los nodos entran y salen con frecuencia de la red). Ninguna seguridad con configuración estática sería suficiente.

- En WMNs, los routers *mesh* y clientes *mesh* llevan a cabo características muy diversas tales como la movilidad y la energía. Consecuentemente, la misma solución de la seguridad puede no trabajar para ambas al mismo tiempo para *mesh router y mesh client*.

CAPITULO 3

ESTUDIO TECNICO DE LA RED DE INTERNET PORTATIL

3.1 Descripción de la ciudad Manta perteneciente a la Provincia de Manabí.

Manta[22] cantonizada en 1922, es el principal cantón de la provincia de Manabí ubicada en la costa ecuatoriana, tiene como limites:

- Norte y Oeste con el Océano Pacifico
- Al sur con el cantón Montecristi
- Al Este con el cantón Jaramijo.

Tiene una extensión 292,89 Km^2, con un Área Urbana de 6.049,23 Hectáreas, y un Área Rural de 23.239,77 Hectáreas. Los datos del último censo de Población y vivienda del 2001 establecen una población total para el Cantón Manta de 192.322 habitantes con una tasa de crecimiento de 3.4 que está sobre la media nacional. La población urbana llega a 183.105 habitantes y la rural 9.217 habitantes, existiendo en ello un porcentaje importante de los llamados habitantes periféricos que por la cercanía y dependencia con el área urbana pueden considerarse como insertos en el. En porcentaje, la población urbana del Cantón constituye el 95,21% lo que determina un cantón prominentemente urbano.

El cantón Manta se encuentra divido en 5 parroquias urbanas (Tarqui, Eloy Alfaro, San Mateo, Manta, Los Esteros) y 2 rurales (San Lorenzo y Santa Marianita).
Entre las principales encontramos a:

Eloy Alfaro

Es una nueva parroquia urbana, de Manta su parroquialización se debió a su crecimiento acelerado de sus diversas asociaciones de agrupaciones parroquiales. Un grupo de dirigentes activos, lograron la misma, bajo la presión del municipio de Manta, se logró su objetivo. Su antiguo nombre se debía a la isla Caribeña de Cuba y de su líder Fidel Castro por eso llevaba el nombre de Cuba Libre.

Los Esteros

[22] http:manta.gov.ec/historia

La parroquia Los Esteros, bajo ordenanza municipal, se dispuso su parroquialización el 12 de octubre de 1979 siendo presidente municipal el Abogado Onofre de Genna A., es el mayor asentamiento de fábricas de procesamiento de atún, por donde pasa la vía puerto – aeropuerto, esta parroquia cuenta con Iglesias, Colegios, escuelas, etc.

San Mateo

Para la creación de la parroquia urbana de San Mateo, la corporación municipal de Manta, expidió la correspondiente ordenanza, que fue discutida y aprobada, en sesiones 12 y 28 de mayo de 1982.

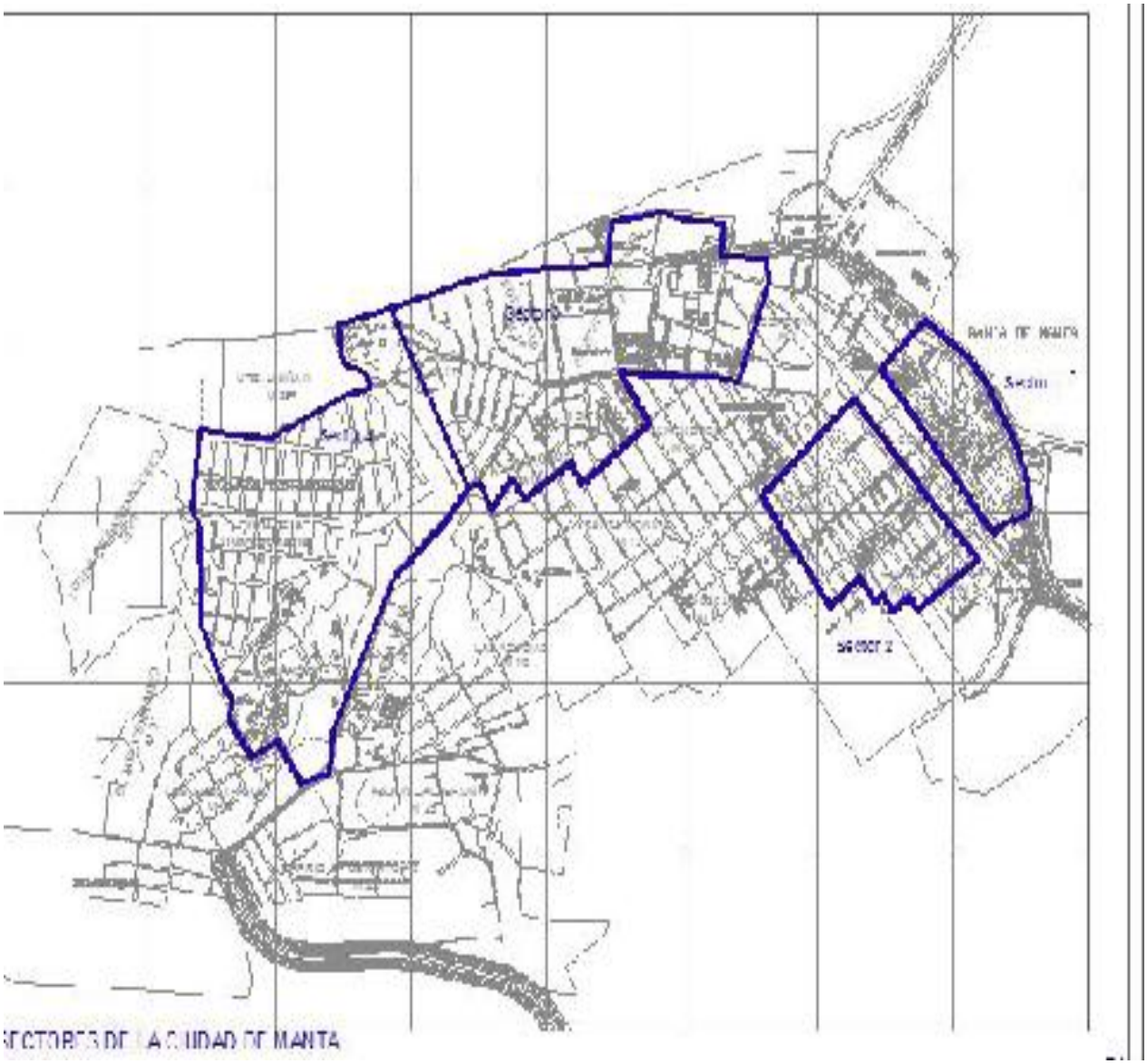
Tarqui

En 1929 el Consejo de Manta crea su primera parroquia urbana, mediante un proyecto de ordenanza municipal que fue discutido por tres ocasiones, en las sesiones del 15 y 23 de enero y 11 de febrero del referido año. Se aprueba la creación de la parroquia mediante decreto N° 328 del 20 de agosto de 1929, según comunicación del Sr. Gobernador de la provincia, en oficio N° 506 enviado al presidente del consejo, quien al recibir la comunicación con fecha 6 de septiembre.

De acuerdo a los resultados de la encuesta las zonas de cobertura que desean la población se encuentra ubicada en las parroquias de Eloy Alfaro y Manta, ya que estas abarcan la ciudadela universitaria, el malecón escénico hotel Oro verde entre otros lugares en donde los encuestados manifestaron su deseo de contar con internet portátil.

3.1.1 Sectores de interés en la ciudad de Manta

En la ciudad de Manta se encuentran cuatro sectores importantes de interés, los mismos que comprenden la parte comercial, turística y residencial de la ciudad. Los sectores se encuentran en el centro de la ciudad donde se localiza el mayor movimiento comercial como se muestra en el Figura 3.1.



3.1.1.1 Sector 1

Como se muestra en la Figura 3.1, este sector se encuentra ubicado en el centro de manta entre las calles 8-16 y avenidas malecón-8. En esta zona se encuentra el sector bancario y administrativo de la cuidad la cual incluye El Muy Ilustre Municipio de la cuidad, La Empresa Eléctrica, Empresa de Agua Potable, La cámara de comercio, Plaza cívica, Matriz Banco del Pichincha, Matriz Banco del Pacífico, Banco de la Producción, Colegio de señoritas Stela Marys.

3.1.1.2 Sector 2

Como se muestra en la Figura 3.1, este sector se encuentra ubicado entre las calles 8-16 y avenidas 10-21. En esta zona se encuentra el mercado Municipal, el Cuerpo de Bomberos y pequeños negocios y una pequeña zona residencial.

3.1.1.3 Sector 3

Como se muestra en la Figura 3.1, este sector se encuentra ubicado entre la playa de Murciélago y la calle 18. En esta zona se encuentra el Hotel Oro Verde, Las Cabañas Balandra, Malecón Escénico, Centro Comercial Manicentro, Complejo Deportivo Thoalí, Colegio Ascario Paz así como complejos residenciales y centro de distracción.

3.1.1.4 Sector 4

Como se muestra en la Figura 3.1, este sector se encuentra ubicado entre la Escuela de pesca y la Universidad Laica. En esta zona se encuentra el Hotel Howard Johnson, Torres del Mar, Torres del Sol, la ciudadela universitaria, Restaurantes, casinos y la universidad.

3.2 Encuesta

Los sectores de interés seleccionados dentro de la ciudad de Manta fueron el sector del malecón escénico (sector tres) y de la ULEAM (sector 4) por encontrarse en estas áreas lugares como centros comerciales (Manicentro), residenciales (Ciudadela Universitaria, Urbanización Umiña,) Universidad Laica Eloy Alfaro de Manabí, y centros de diversión así como la Plaza del Sol y el Malecón Escénico, es decir lugares donde los encuestados pusieron mayor disposición a contar con servicio de internet portátil.

Mientras que en los sectores 1 (Centro de Manta) y sector 2 (Cuerpo de Bomberos) no se vio factible realizar la encuesta en virtud que las entidades bancarias cuentas con servidores de datos propios de cada banco.

La encuesta es el instrumento que permite la recolección ordenada de la información que servirá para conocer el comportamiento de la necesidad de un servicio en una zona poblada.

Antes de su elaboración se debe precisar, con claridad, los objetivos de la investigación y la información necesaria para obtener datos que permitan brindar un servicio orientado a las necesidades de la población.

3.2.1 Objetivo: La encuesta, tiene por objeto determinar los siguientes parámetros:

- Saber la cantidad de personas que tiene acceso a internet en una zona comercial.
- Conocer los sitios comunes donde las personas están cómodas al usar el servicio de internet.
- Conocer las necesidades de la población en cuanto a los requerimientos de calidad de servicio en una conexión de internet.
- Investigar en la muestra la tendencia de la población a contar con un servicio de internet portátil.

3.2.2 Grupo Meta: La encuesta está dirigida a la población que se encuentra ubicada en las zonas comerciales y urbanas de la ciudad de Manta.

3.2.3 Tamaño de muestra: 1000

A continuación se muestra el formato de la encuesta utilizada

ESCUELA POLITËCNICA DEL EJËRICTO

DEPARTAMENTO DE ELËCTRICA Y ELECTRÖNICA

ENCUESTA PARA REALIZAR EL ANÁLISIS Y DISEÑO PARA LA IMPLEMENTACIÓN DE UN SISTEMA PARA BRINDAR SERVICIO DE INTERNET INALÁMBRICO EN LA CIUDAD DE MANTA

Permite conectarse sin cables al Internet de banda ancha, por medio de sistemas inalámbricos ubicados estratégicamente en áreas determinadas en la ciudad de Manta.

1) Usted tiene servicio de internet?

   SI_____ No_____

   (Si la respuesta es no pasar a la pregunta 5)

2) Usted en que lugares cuenta con internet?

CASA	TRABAJO	UNIVERSIDAD	CENTRO COMERCIAL	NINGUNO

3) Con qué frecuencia usa internet?

NUNCA	OCASIONALMENTE			SIEMPRE
	Una vez a la semana	Una vez al mes	Una vez al año	

4) Sabe usted acerca de empresas que brinden servicio de internet portátil en su ciudad?

   SI_____ No_____

5) Le gustaría poseer servicio de internet portátil en cualquier sitio de la ciudad utilizando su mismo ordenador?

   SI_____ No_____

6) Como desearía su servicio de internet portátil en su ciudad?

VELOZ	QUE NO HAYA RESTRICCIONES A LA HORA DE CONECTARSE	SIN LÍMITE DE DESCARGA	TODOS LOS ANTERIORES

7) Donde le gustaría usar internet portátil en su ciudad?

CENTROS COMERCIALES	MALECÓN	LUGAR DE TRABAJO	PLAYA	RESIDENCIA	TODOS

3.2.4 Resultados de la encuesta:

Pregunta 1: *Usted tiene servicio de internet*,

Si (72%)

No (28%)

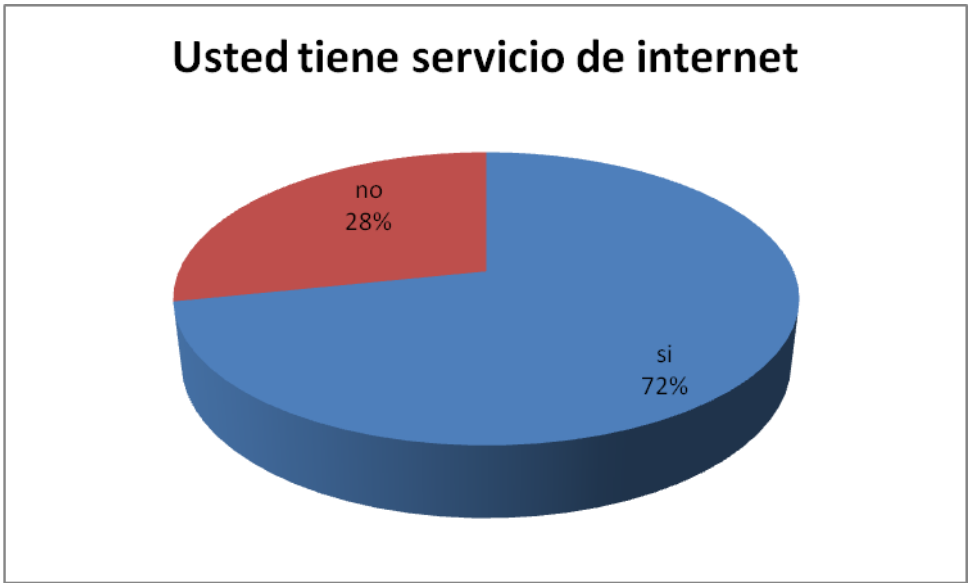


Figura 3. 2 Datos Tabulados sobre la pregunta 1

El objetivo de esta pregunta tiene como razón conocer la cantidad de personas que pueden acceder al internet, dependiendo de este resultado se puede analizar la factibilidad de brindar servicio de internet en el área encuestada.

Pregunta 2: *Usted en que lugares cuenta con internet*

Centro Comercial (13%)

Universidad (41%)

Casa (27%)

Trabajo (19%)

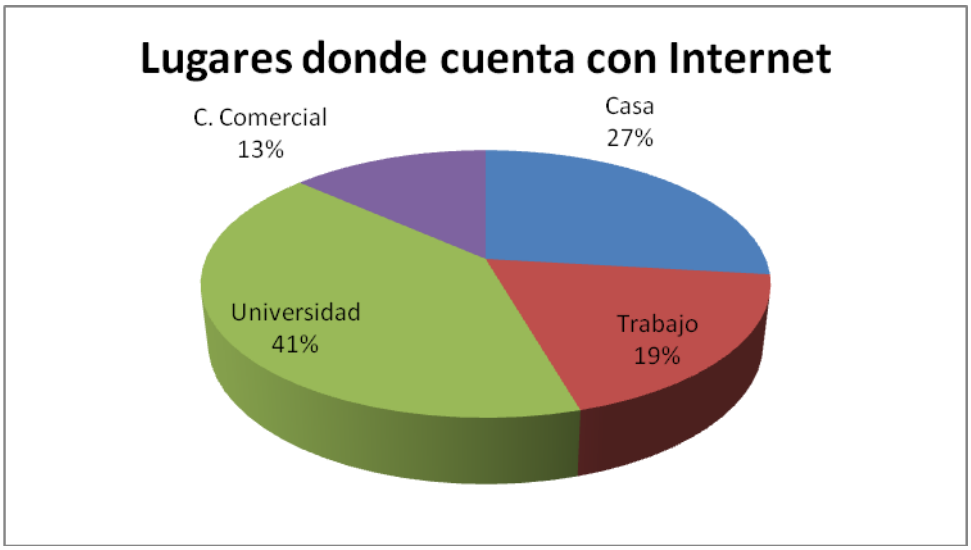


Figura 3. 3 Datos tabulados sobre la pregunta 2

El objetivo de esta pregunta tiene por efecto conocer los lugares donde la poblacion cuenta con servicio de internet ya sean publicos o privados, y en base a estos datos conecer las necesidades de la poblacion encuestadas

Pregunta 3: *Con que frecuencia usa el internet*

Siempre (Al menos una vez al día) (62%)

Una vez por semana (34%)

Una vez por mes (4%)

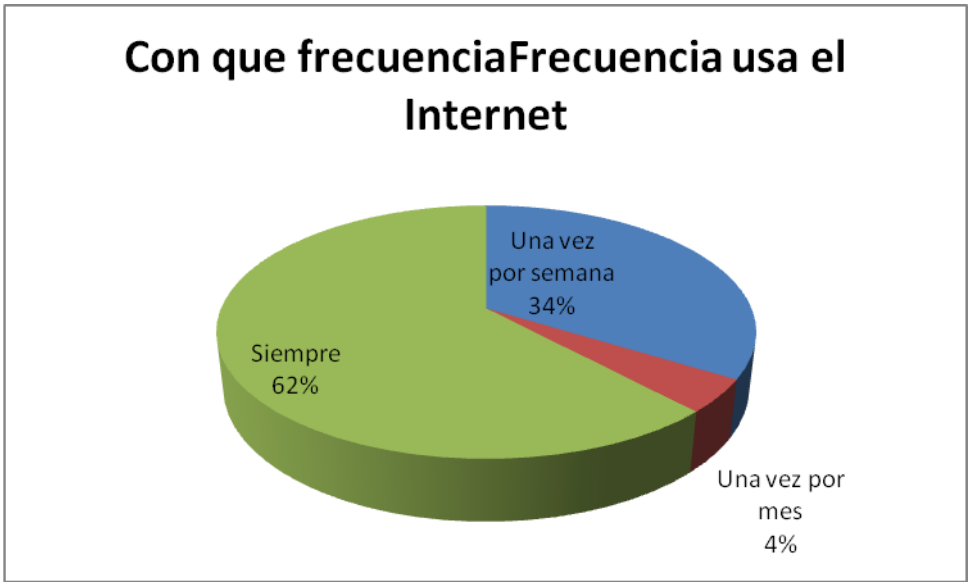


Figura 3. 4 Datos tabulados de la pregunta 3

El objetivo de esta pregunta es conocer la necesidad de la poblacion hacia un servicio de internet, conociendo la existencia de uso de internet y a que zona de interes dirigir al proyecto

Pregunta 4: *Sabe usted acerca de empresas que brinden servicio de internet portatil en su ciudad. El internet portátil le permite poseer conexión de internet en cualquier parte de la ciudad con un mismo ordenador.*

Si(24%)

No(76%)

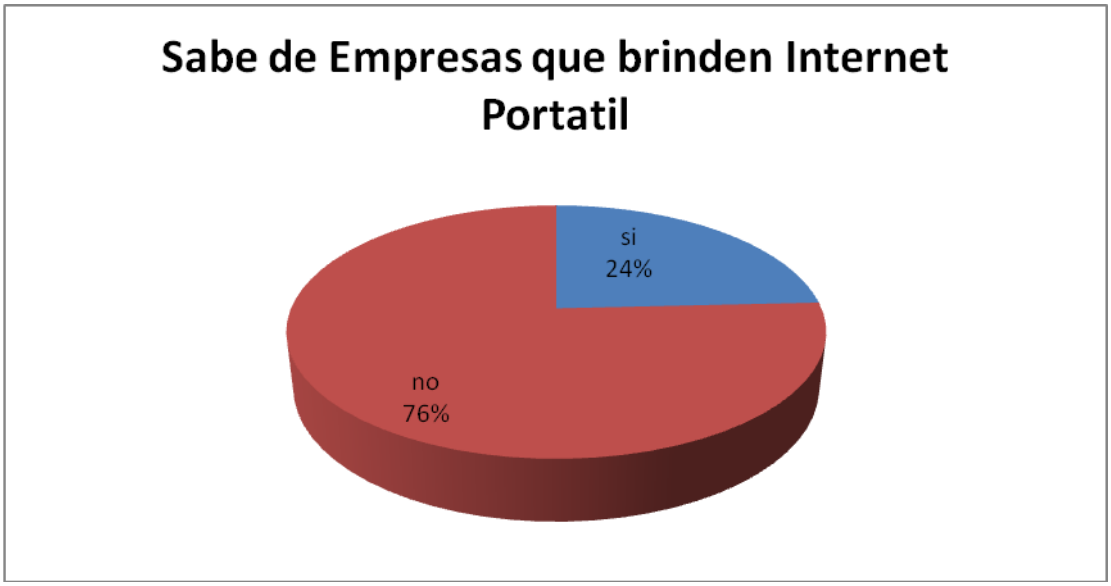


Figura 3. 5 **Datos tabulados a la pregunta 4**

El objetivo es analizar el mercado de servicio de internet portatil en la zona de interes en la ciudad de Manta, para tener una idea de la posible competencia de este tipo de servicio

Pregunta 5: *Le gustaría poseer servicio de internet portátil en cualquier sitio de la ciudad usando su mismo ordenador.*

Si (97%)

No (3%)

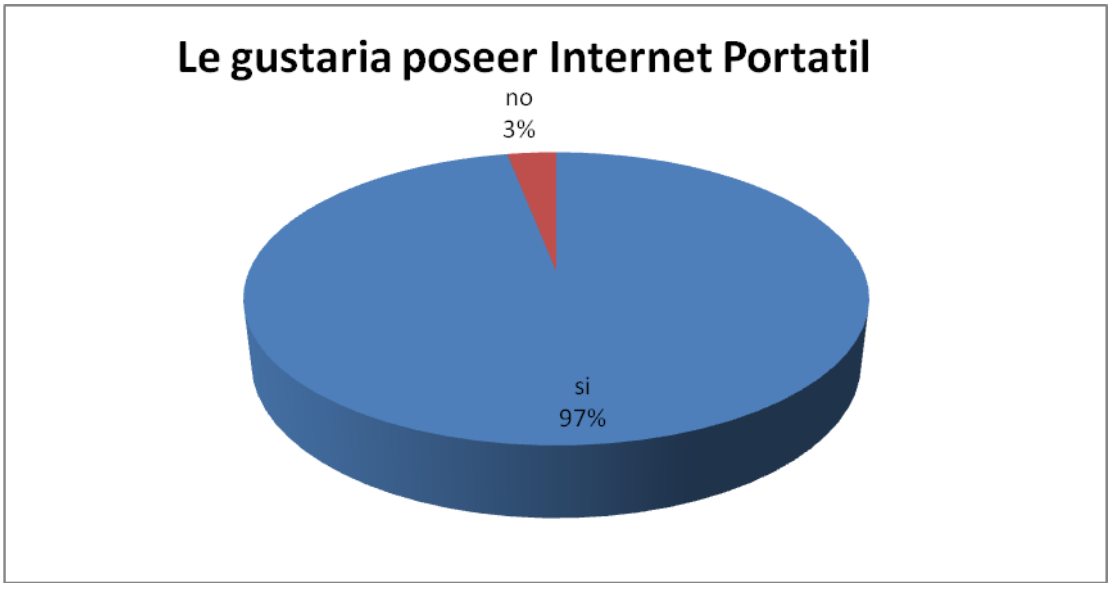


Figura 3. 6 **Datos tabulados sobre la pregunta 5**

El objetivo de esta pregunta es saber la afinidad de la población a hacia un nuevo servicio de internet portátil, para conocer nuestro posible mercado

Pregunta 6: *Como desearía su servicio de internet portátil en su ciudad,*

Veloz (26%)
Sin restricciones (13%)
Sin límites de descarga (6%)
Todos(55%)

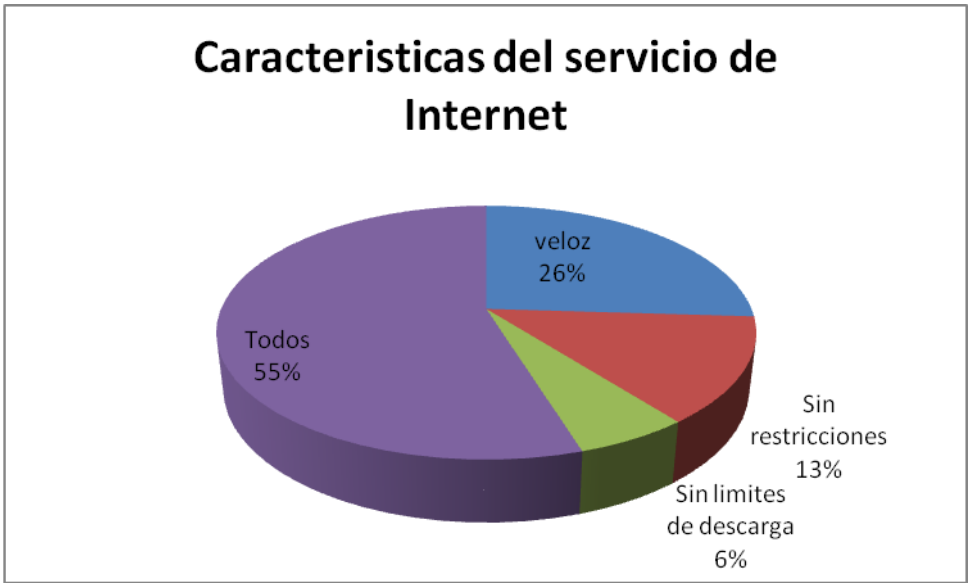


Figura 3. 7 **Datos Tabulados sobre la pregunta 6**

El objetivo de esta pregunta es conocer los requerimientos técnicos que son necesarios para brindar internet portátil con calidad de servicio.

Pregunta 7: *Donde le gustaría usar internet portátil en su ciudad.*

Centro Comercial (7%)
Malecón (5%)
Lugar de trabajo (2%)
Playa (4%)
Residencia (6%)
Todos (76%)

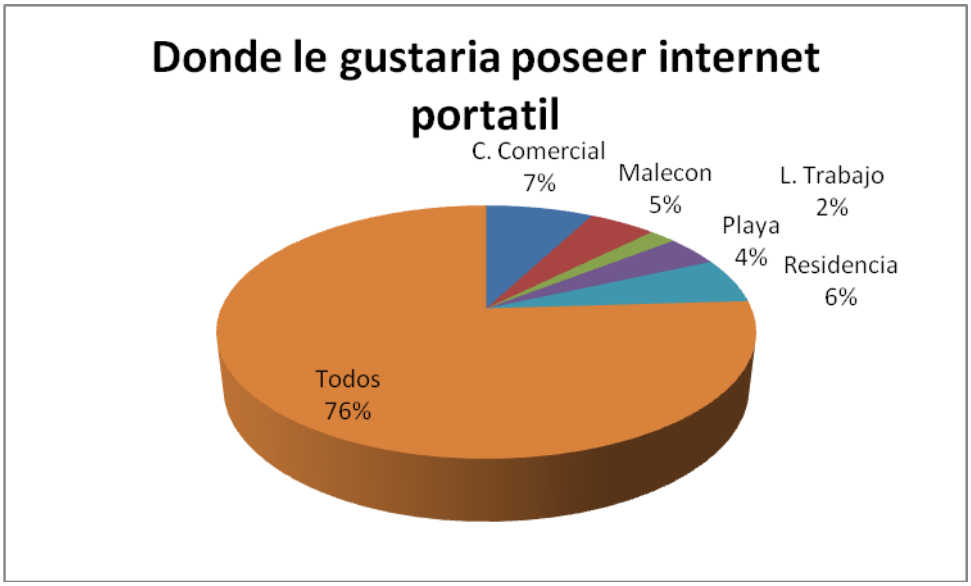


Figura 3. 8 **Datos tabulados sobre la pregunta 7**

El objetivo de esta pregunta es conocer los sitios en donde se ubicaran los nodos para satisfacer las necesidades de la población.

3.2.5 Análisis de los resultados obtenidos de la encuesta

Se realizo la encuesta a un total de 1000 personas, esto es una muestra de la población que vive y trabaja en la zona comercial escogida para este estudio. Las encuestas se realizaron dando prioridad a estudiantes de nivel superior.

- El análisis de la muestra indica que el 72 por ciento de la población accede a un servicio de internet, sabiendo que si se brinda una opción que mejore las prestaciones de un ISP como la portatibilidad se pudiera competir con las empresas de internet ubicadas en la ciudad de Manta.

- De acuerdo a la muestra de la población indica que la mayoría de personas (76 %) que cuentan con servicio de internet no conocen de empresas que brinden servicio inalámbrico en la ciudad, por lo cual les pareció atractivo que una nueva empresa brinde ese servicio (97%), se verifico que la necesidad de la población se encuentra ubicada a lo largo del área comercial y turística dentro de la ciudad, prevaleciendo su

interés en que el servicio pueda ser utilizado en cualquier parte de la urbe (55%) (Residencia, Malecón, Playa, Centro Comercial, Lugar de Trabajo).

- La calidad de servicio de acuerdo a las necesidades de la población indica que desea un servicio que cumpla con todas las características necesarias para poder acceder al internet de manera eficaz (55%).

3.3 FABRICANTES DE EQUIPOS PARA REDES ENMALLADAS INALAMBRICAS

La Alianza Wi-Mesh es un grupo de compañías cuyo objetivo consiste en establecer con rapidez un estándar para WLANs en malla que permita una comunicación fluida entre los usuarios de dispositivos inalámbricos. La propuesta de la Alianza Wi-Mesh se desarrolló de acuerdo con los lineamientos de la Asociación de Estándares IEEE.

Asimismo, se basa en los protocolos 802.11 pendientes para permitir la reutilización y la compatibilidad de tecnología. De la Tabla 3.1 se estudiaran los equipos de los fabricantes para seleccionar el dispositivo más adecuado para el desarrollo del proyecto

Tabla 3. 1 Principales fabricantes de tecnología mesh

	Enlace del cliente	Frecuencia	Radios por Router	Tipo de red
Belait Network	802.11b/g	5Ghz	1,2 o 4	MAN
Cisco Systems	802.11b/g	5Ghz	2	MAN
Firetire	Ethernet	2.4Ghz, 5Ghz	1	MAN/LAN
Nortel Networks	802.11a/b/g, Bluetooth	5Ghz	2	MAN
Strix Systems	802.11b/g	2.4Ghz, 5Ghz	2 a 6	MAN/LAN
Tropos Netwoks	802.11a/b/g/n	2.4Ghz, 5Ghz	1 o mas	LAN

3.3.1 Firetide

Firetide es una empresa de tecnología inalámbrica especializada en redes malladas que desarrolla equipamiento con altas prestaciones, escalabilidad y fácil de instalar.

• Equipo HotPort 3203 Outdoor *Wireless* Mesh Nodes, Figura 3.9

Los equipos HotPort 3203 trabajan en las bandas de 2.4 GHz y 5 GHz, tienen capacidad de hasta 25 Mbps, con 100 mW de potencia de salida, poseen encriptación avanzada (WEP / AES), tienen 2 puertos Ethernet 10/100, compatibles con IEEE802.3af (*PoE*) y 2 antenas omnidireccionales de 4 dBi, con posibilidad de utilizar antenas de mayor ganancia, su alcance máximo es de 100 metros.

Figura 3. 9 HotPort 3203

3.3.2 Tropos Networks

.

La arquitectura de Tropos MetroMesh[23] proporciona la flexibilidad máxima en la instalación y la capacidad de reaccionar y de responder a las fallas sin interrupción del *backhaul* inalámbrico.

- AP-3210 (Figura 3.10) trabaja tanto en b como en g, aparte trabaja tanto en la banda de 2.4 así como de 5 Ghz, tiene un radio de cobertura de 200 metros, posee seguridades como WEP TKIP AES

Figura 3. 10 AP-3210

[23] http://tropos.com/products/metromesh_os.htlm

3.3.3 Skypilot

Su estrategia está enfocada a dotar de cobertura WiFi a grandes áreas como pueden ser un municipio. Skypilot se caracteriza por la utilización en sus diferentes nodos de un arreglo de 8 antenas para conseguir mejores zonas de cobertura y capacidades superiores a sus competidores.

Usando el sistema de localización global (GPS), la tecnología SyncMesh coordina las transmisiones simultáneas a través de la red *Mesh.*

- SkyGateway DualBand (Figura 3.11)**:** Conecta la infraestructura *wireless Mesh* con Internet., pero además da cobertura Wi-Fi. El *backhaul* funciona en la banda de 5GHz y Wi-Fi en la banda de 2.4GHz, su radio de cobertura es de 250 metros, utiliza encriptaciones tales como WEP, WPA2.

Figura 3. 11 ***SkyGateway DualBAnd***

3.3.4 Locustworld

Mesh LocustWorld está diseñado para proveer acceso inalámbrico a áreas geográficas muy amplias, fundamentalmente por medio del uso de 802.11b, ya

que se adapta mejor para instalaciones a la intemperie y también porque los dispositivos que usan 802.11b pueden conseguirse en cualquier parte y son de muy bajo costo.

- Mesh Box (Figura 3.12) Trabaja en la banda de 5 Ghz, el acceso de usuario a los servicios del Internet es controlado con la conexión de la red, el MAC address o la conexión del PPTP VPN, cubre un radio de cobertura de 300 metros con línea de vista.

Figura 3. 12 Mesh Box

3.3.5 Nortel

La solución *Wireless* Mesh Network de Nortel se ha implementado en empresas, universidades y agencias gubernamentales, tales como las ciudades de Taipei y Kaohsiung en Taiwán, la Universidad de Arkansas, la Universidad Edith Cowan en Australia, su tecnología pretende ser compatible con las modificaciones futuras al rendimiento 802.11n.

- Nortel Wireless Access Point 7215 (Figura 3.13) *wireless* b y g alimentación vía PoE, tiene encriptación WEP, WAP2, su radio de cobertura es de 300 metros.

Figura 3. 13 AP-7215

3.3.6 MOTOROLA

- AP 51-31 (Figura 3.14) posee dos radios: uno en 2.4 GHz compatible con 802.11b/g y otra en 5.8 GHz compatible con 802.11a, que pueden configurarse en un nodo de radio única (para brindar cobertura y servicio de bajo costo) o de radio dual (para brindar mejor rendimiento con atenuación de interferencias). Además, el sistema HotZone Duo cumple con la norma 802.11e, convirtiéndose en una de las pocas soluciones de redes *Mesh* que ofrece priorización de voz y video especializado para el operador, y que proporciona sólidas aplicaciones inalámbricas de Voz sobre IP y *streaming* de video. Posee seguridades como WPA. WEP, WPA2, WPA2-CCMP (802.11 i), su radio de cobertura es de 300 metros.

Figura 3. 14 AP-5131

A continuación en la tabla 3.2 se indica los equipos que pueden considerarse dentro del proyecto de estudio como parte en el diseño de la infraestructura de la red.

Tabla 3. 2 Características de equipos mesh

Marca	Equipo	Especificaciones	Seguridad	Precios USD
Skypilot	SkyGateway DualBand	• 802.11 b/g • Sensibilidad • 0^0 C a 40^0C	• WEP, WPA	880.99
Nortel	Access Point 7215	• 802.11 b/g • Sensibilidad -90 dBm • -10^0 C a -50^0C	• WEP, WPA2	787.99
Firetide	HotPort 3103	• Auto mesh FIretide protocol DSSS y OFDM • Sensibilidad hasta -96 dBm • 0^0C a 40^0C	• Encriptación 104 bit WEP keys, 128 bit, 256 bit AES keys • Class of Service	1095
Locustworld	Mesh-Box	• 802.11 a/b/g • -20^0C a 40^0C	• WEP, WPA	250
Tropos	AP-3210	• 802.11 b/g DSSS y OFDM • Sensibilidad -91dBm • -10^0C a 50^0C	• 802.11 i • WPA/WPA/2 • Encriptacion WEP TKIP AES • VPN • Lista de control de acceso po MAC	1090
Motorola	AP-5131	• 802.11 a/b/g DSSS y OFDM • Soporta hasta 127 dispositivos • -20^0C a 50^0C	• 802.11 i • WPA/WPa2 • Encriptación 3DES/AES IP-sec • VPN • Servidos AAA	600

3.3.7 Selección del equipo a utilizarse

De acuerdo a los resultados de la encuesta se necesita cubrir dos zonas de interés en la ciudad de Manta, en relación a la distancia los equipos tienen un radio similar de cobertura, mientras que en seguridades están a la par sólo Motorola y Tropos. Como COMPUATEL S.A tiene un convenio con el distribuidor de Motorola en la ciudad de Quito, el equipo AP 51-31 de la marca Motorola es el escogido para la solución del proyecto.

3.4 Características del software de administración y seguridades

3.4.1 AP-5131

El software del AP-5131 fue diseñado para ambientes interiores pero por su capacidad y costo es atractivo para el proyecto en cuestión. Es de configuración avanzada, es decir, puede ser configurado de manera grafica o por líneas de comando.

3.4.2 Características del software.

Desde su versión inicial (1.1) el software del AP-5131 posee las siguientes características:

- Modos de operación de radio y radio dual
- Puertos separados LAN y WAN
- Múltiples opción de montaje
- Antena que soportan radios de 2.4 y 5.2 GHz
- Dieciséis WLANs configurables
- Soporta 4 BSSIDs por radio
- Calidad de servicio (QoS)
- VLAN
- Múltiples opciones de accesibilidad y administración

- Firmware actualizable
- SNMP v1/v2/v3 programable.
- Priorizacion de voz.
- Soporta tanto CAM (modo autoconsciente) y PSP (ahorro de energía).
- Estadísticas de las redes.
- Control de transmisión de potencia
- Capacidad de registro de sucesos avanzados
- Configuración de archivos.
- Soporte DHCP.

3.4.2.1 Modos de operación de radio y radio dual

Existen dos posibles configuraciones dependiendo del modelo usado. Este modo de operación está habilitado para los radios 802.11a y/o 802.11b/g.

3.4.2.2 Puertos LAN y WAN separados

El Ap-5131 tiene un Puerto LAN y un Puerto WAN, cada uno con su dirección MAC. Debe manejar todo el tráfico a través de conexión LAN cuidadosamente como cliente DHCP, cliente BOOTP, servidor DHCP y dirección IP estática.

La WAN está dispersa en la red de telecomunicaciones. En un ambiente corporativo, el puerto WAN puede ser conectado a una red corporativa. Para pequeños negocios el puerto WAN puede ser conectado a un modem DSL o de cable para acceder a Internet. Independientemente, la información de la red debe ser configurado para el modo previsto de operación.

3.4.2.3 Antenas para radios 2.4 y 5.2 GHz

El equipo soporta varias antenas para radio 80.11a y 802.11b/g. Se puede seleccionar la antena más adecuada para los requisitos de cobertura.

3.4.2.4 Dieciséis WLANs configurables.

La red de área local inalámbrica es un sistema de comunicación de datos que extiende y flexibiliza las funciones de una LAN cableada. Una WLAN no requiere de línea de vista para la transmisión, por tanto son deseables para una red inalámbrica. Los usuarios pueden pasar de una red a otra como un sistema de telefonía celular.

Las WLANs pueden por tanto ser configuradas de acuerdo a grupos específicos de usuarios, aun cuando no se encuentren cerca. Dieciséis WLANs pueden ser configuradas en cada AP

3.4.2.5 4 BSSIDs[24] por Radio.

El AP-5131 soporta un máximo de 8 BSSIDs, cada BSSID tiene su dirección MAC correspondiente. La primera dirección MAC corresponde al primer BSSID, las direcciones MAC para las otras tres son derivadas añadiendo uno a cada una respectivamente. Por ejemplo si la dirección MAC del primer BSSID es 00:A0:F8:72:20:DC ; entonces los demás BSSID del radio tendrá los BSSID como se muestra en la tabla 3.3

Tabla 3. 3BSSID

BSSID	Direccion MAC	Adición Hexadecimal
BSSID #1	00:A0:F8:72:20:DC	El mismo com la dirección MAC del radio
BSSID #2	00:A0:F8:72:20:DD	Dirección MAC+1
BSSID #3	00:A0:F8:72:20:DE	Dirección MAC+2
BSSID #4	00:A0:F8:72:20:DF	Dirección MAC+3

[24] **BSSID** (**B**asic **S**ervice **S**et **ID**entifier)

3.4.2.6 Calidad deServicio (QoS)

La implementación calidad de servicios proporciona aplicaciones que se ejecutan en los diferentes dispositivos inalámbricos de una variedad de niveles de prioridad para transmitir datos desde y hacia el AP. La igualdad de prioridad en la transmisión de datos es adecuada para el tráfico de datos como navegadores web, transferencia de archivos o correo electrónico, pero es inadecuada para las aplicaciones multimedia. Voz sobre IP (VoIP), videos y juegos interactivos son muy sensibles al incremento de la latencia y la disminución de rendimiento, la priorización de el trafico de datos puede beneficiar significativamente la calidad de servicio. La aplicación WMM (*The WiFi Multimedia Extension QoS*) es usada para acortar los tiempos entre la transmisión de datos de alta prioridad que es conveniente para las aplicaciones multimedia. La WMM define cuatro categorías de acceso están priorizadas para un mejor soporte multimedia de la siguiente manera:

1. Voz
2. Video
3. Mejor esfuerzo
4. Fondo.

3.4.3 Características Extras del Software de Administración.

3.4.3.1 Redes Mesh

El AP está en capacidad de manejar redes *mesh*, funciona como un puente para conectar dos redes, o como un repetidor para extender el área de cobertura de la red, sin cableado adicional. Las redes *mesh* se pueden

configurar de dos modos, como un punto cliente o como servidor que acepta las conexiones de sus clientes (Estos dos modos no son excluyentes).

En el modo cliente, el punto de acceso busca el servidor usando el ESSID. El punto de acceso debe pasar por el proceso de asociación y autenticación para establecer una conexión inalámbrica. El proceso de asociación de redes *mesh* es idéntico al proceso de la estación final con el AP. Una vez que el proceso está completo, el AP en modo cliente añade la conexión como un puerto en el modulo de puente para comenzar de reenvió de información al AP servidor. El AP servidor permite el acceso de los AP clientes por medio de radio.

Los puentes se comunican usando STP, que determina el camino a la raíz y detecta si la conexión actual es parte de un lazo con otra conexión. Una vez que el STP converge comienza el proceso de aprendizaje, permitiendo enviar trafico inteligentemente.

Una vez que el AP cliente realice al menos una conexión inalámbrica se empieza a dirigir y aceptar conexiones inalámbricas para apoyar a los usuarios portátiles, lo mismo sucede cuando este AP está configurado en modo cliente/servidor permitiendo que la red mallada se construya a si misma con el tiempo y la distancia. Como consecuencia de esto puede generar enlaces redundantes y algoritmo STP es el encargado de deshabilitar los mismos para evitar tormentas de *broadcast.*

3.4.3.2 Red Lan Adicional

En un típico ambiente de oficina donde coexisten una LAN y WLAN es necesario segmentar a la LAN en dos subredes para separar el tráfico inalámbrico. El AP posee una segunda LAN que permite al administrador segmentar su red en dos subredes separadas. Ahora el usuario tiene la capacidad de elegir entre las dos LANs su punto de acceso a internet.

Cada LAN tiene diferente nombre así como su configuración, siendo independiente una de otra.

3.4.3.3 Servidor de autenticación RADIUS

El AP tiene la habilidad de trabajar como un servidor RADIUS para proveer información de la base de datos y autenticación de usuarios. En el menú de configuración grafica de STP se encuentra la configuración de servidor RADIUS, permitiendo configurar la base de datos y las políticas de acceso.

La viñeta de Radius server permite al administrador definir la fuente de datos, el tipo de autenticación y asociar los certificados digitales con el esquema de autenticación.

La viñeta LDAP permite al administrador configurar un servidor LDAP externo para usarlo con el AP

Una viñeta de Política de Acceso permite al administrador setear acceso a WLAN basado en grupos de usuarios sin usar la viñeta de Base de Datos, cada usuario tiene autorización basado en las políticas de acceso.

3.4.3.4 Soporte en HOTSPOT

El AP permite operaciones HOTSPOT para proveer autenticación y registro de usuarios. El AP usa un navegador como una autenticación de seguridad sencilla en vez de crear políticas de seguridad con privilegios de asociación.

3.4.3.5 RIP (Protocolo de Información de Ruta)

RIP es un protocolo interior que especifica como los APs intercambian la información de tabla de enrutamiento, en la configuración el administrador puede elegir el tipo de RIP y el tipo de autenticación a usar.

3.4.3.6 Configuración de fecha y hora

Como una alternativa a un servidor NTP los APs pueden configurar manuelmente la fecha y hora.

3.4.3.7 DNS dinámicos

El AP soporta servicio dinámico de DNS (DynDNS), es una característica ofrecida por www.dyndns.com que permite el mapeo de nombres de dominio dinámicamente asignados cuando la dirección IP del cliente cambia la nueva IP es enviada al servicio DynDNS y el trafico del dominio especifico es ruteado a la nueva dirección IP.

3.4.3.8 Autonegociación

Habilita al AP la intercambiar información automáticamente de los puertos WAN y LAN, la velocidad de transmisión y capacidad DUPLEX, la auto negociación es de ayuda cuando los APs se encuentran en ambientes con diferentes dispositivos.

3.4.4 Seguridades del Equipo

Soporta numerosas técnicas de encriptación y de autenticación para proteger la transmisión de datos de la red inalámbrica.

Las técnicas de autenticación son:

- Autenticación Kerberos.
- Autenticación EAP.

Las técnicas de encriptación son:

- WEP
- Encriptación KeyGuard
- WPA usando encriptación TKIP
- WPA2-CCMP (802.11 i)

Características adicionales de seguridad:

- Seguridad Firewall
- VPN
- Filtro de contenidos

3.4.4.1 Autenticación Kerberos

La autenticación significa verificar la información que es transmitida de una fuente segura, conociendo el creador de la información y sabiendo que no fue alterada a lo largo de la transmisión. La autenticación es crítica para la seguridad de cualquier red inalámbrica. La autenticación para redes alambricas no es la adecuada para una red inalámbrica done un usuario no autorizado no puede controlar el tráfico de red. Es necesario el uso de una autenticación fuerte para no revelar las contraseñas, en este caso el protocolo de autenticación de Kerberos (especificado en el RFC1510) para identificar usuarios y distribuir de forma segura las claves de cifrado y descifrado. Por

defecto el AP opera en una red de sistema abierto donde cualquier dispositivo inalámbrico puede asociarse con un punto de acceso sin autorización.

La autenticación Kerberos requiere de un dispositivo autenticado para ingresar a la red inalámbrica.

3.4.4.2 Autenticación EAP

El protocolo de Autenticación Extendido (EAP) provee a los AP y sus clientes una seguridad adicional para transmisión de datos a través de una red inalámbrica. El uso de esta autenticación entre dispositivos se las realiza mediante el intercambio y verificación de paquetes certificados.

El EAP es un método de autenticación mutua es decir tanto el AP como sus clientes están obligados a identificarse. El cliente solicita una conexión a la red inalámbrica a través del EAP, luego pide identificación y la reenvía a un servidor de autenticación, luego el servidor pide una prueba de autenticación al AP proporcionada por el cliente y luego transmite los datos del usuario al servidor para completar la autenticación, siendo el cliente incapaz de acceder a la red sin que fuera autenticado.

EAP solo es compatible con dispositivos móviles que usen Windows XP, Windows 2000 (con *Service Pack #4*) y Windows Mobile 2003.

3.4.4.3 WEP

Todos los dispositivos WLAN enfrentan el robo de información, sucede cuando un usuario no autorizado obtiene información de manera ilegal, la ausencia de conexiones físicas vuelve a las redes inalámbricas más propensas a este tipo de robo. La mayoría de WLANs se basan en la encriptación en varios grados, la encriptación implica la codificación y decodificación de la información normalmente con algoritmos matemáticos, el dispositivo realiza la encriptación, un usuario no autorizado puede conocer el algoritmo pero no interpretar los

datos sin la clave adecuada. Solo el AP y un cliente autorizado conocen la clave de la encriptación,

WEP *Wired Equivalen Privacy* es un protocolo de encriptación de seguridades especificado en la *Wireless* IEEE *Fidelity* (Wi-Fi) que soporta el AP.

WEP está diseñado para proporcionar a la WLAN una seguridad y privacidad comparada a una LAN cableada, el nivel de protección que brinda está determinado por la longitud y clave del algoritmo, siendo la clave una cadena de caracteres usada por el algoritmo para cifrar y descifrar los paquetes de datos transmitidos.

3.4.4.4 Encriptación *KeyGuard*

Esta encriptación es usada para proteger las llaves de encriptación de ser descubiertas por hackers, son usadas entre la asociación de los APs y sus clientes, Esta encriptación solo es usada entre los APs y clientes Motorola es decir es solo un mecanismo de seguridad único de Motorola.

3.4.4.5 WPA usando TKIP

Wi-Fi *Protected Access* es un estándar de seguridad para sistemas operativos con una conexión inalámbrica Wi-Fi , WEP carece de mecanismos de autenticación de usuario que existen en WPA, comparado con WPE WPA es superior en encriptación de datos y autenticación de usuarios.

WPA mejora a WPE en las siguientes características:

- Una clave de función por paquete.
- Un control de integridad de mensaje.

- Un vector extendido de iniciación con reglas de secuencia.
- Un mecanismo de reenvió de claves.

WPA utiliza un método de encriptación llamado TKIP (*temporal Key Integrity Protocol)* y también emplea EAP.

3.4.4.6 WPA 2 CCMP (802.11i)

Es un nuevo estándar 802.11i que proporciona una seguridad más fuerte en redes inalámbricas que WPA y WEP. *Counter Mode CBC-MAC protocol* o CCMP es el estándar de seguridad utilizado por el *Advanced Encryption Estándar* (AES) que tiene la misma función que TKIP en WPA-TKIP.

CCMP calcula un control de integridad de mensaje (MIC) con el resultado código de autenticación del bloque de información (CBC-MAC).

WAP2-CCMP se basa en el concepto de una red de seguridad solida (RSN), que define una jerarquía de llaves con una vida útil similar a la de TKIP. Al igual que TKIP, las llaves que provee el administrador son usadas para crear nuevas llaves, los mensajes son encriptados usando una llave secreta de 128 bits y otros 128 bits para datos, teniendo un resultado final como un esquema de encriptación tan segura como cualquier otro.

3.4.4.7 FIREWALL

Un *FIREWALL* es una barrera que mantiene la información personal fuera de los hackers. Mantiene la información sospechosa fuera de la red, el desempeño de
NAT (*Network Address Translation*) en paquetes pasando desde y hacia el puerto WAN, esta combinación provee mejoras en la seguridad de la transmisión de datos.

3.4.4.8 VPN (Virtual Private Network)

Las redes privadas virtuales son redes basadas en IP mediante la encriptación y la utilización de un túnel para el acceso remoto de usuarios a una LAN segura. En esencia es una relación de confianza entre una red LAN pasando por una red pública hacia otra red LAN.

3.4.4.9 Filtrado de Contenido

El filtrado de contenidos permite al administrador de la red tener un control selectivo sobre el contenido de la red y es una herramienta de detección de largo alcance.

Permite el bloqueo de hasta 10 extensiones URL y permite el bloqueo de determinados sitios HTTP, SMTP, FTP y otras peticiones.

3.5 Requisitos legales previos a la implementación y comercialización de la red de internet portátil.

3.5.1 Sistemas de Modulación Digital de Banda Ancha

Sistemas de radiocomunicaciones que utilizan técnicas de codificación o modulación digital en una anchura de banda asignada con una densidad espectral de potencia baja compatible con la utilización eficaz del espectro.

Son aprobados para la operación los sistemas de radiocomunicaciones que utilicen técnicas de Modulación Digital de Banda Ancha en las siguientes bandas de frecuencias:

Tabla 3. 4 Banda de Frecuencias

BANDA (MHz)

902 - 928
2400 - 2483.5
5150 – 5250
5250 – 5350
5470 – 5725
5725 - 5850

3.5.2 Redes privadas

Son aquellas utilizadas por personas naturales o jurídicas en su exclusivo beneficio, con el propósito de conectar distintas instalaciones de su propiedad o bajo su control, por lo cual se servirá demostrar que las instalaciones a implementarse son de su propiedad o están bajo su control remitiendo una copia del título de propiedad o contrato (convenio) de arrendamiento del lugar donde se ubicarán los equipos y especificando el tipo de instalación a implementarse (estación repetidora o terminal) y la finalidad de la estación terminal (matriz, sucursal, bodega, oficina).

En este caso los requisitos que se usarán son los que corresponden a una persona jurídica.

- Solicitud dirigida al Señor Secretario Nacional de Telecomunicaciones.
- Escritura de constitución de la compañía domiciliada en el país.
- Nombramiento del Representante Legal, debidamente inscrito en el Registro Mercantil.
- Copia del RUC.
- Copia de la cédula de identidad del Representante Legal.
- Copia del último certificado de votación, del Representante Legal.
- Anteproyecto técnico elaborado y suscrito por un ingeniero en electrónica y/o telecomunicaciones.
- Otros documentos que la SENATEL solicite.

A fin de demostrar la viabilidad de la solicitud el Anteproyecto Técnico deberá contener lo siguiente:

- Descripción técnica detallada del o los servicios que soportará la red, especificando el tipo de información que cursará sobre ella.
- Diagrama funcional de la red, que indique claramente los elementos activos y pasivos de la misma. Describir su funcionamiento basado en el diagrama.
- Gráfico esquemático detallado de la red a instalarse, el cual debe estar asociado a un plano geográfico, en el que se indiquen la trayectoria del medio físico de transmisión o los enlaces radioeléctricos que se van a utilizar. Dicho gráfico deberá contener las direcciones exactas de las instalaciones.
- Especificaciones técnicas del equipamiento a utilizarse y de los medios físicos que se emplearían. Incluir una copia de los catálogos técnicos.
- Indicar los recursos del espectro radioeléctrico requeridos, especificando la banda en la cual se va a operar, así como los requerimientos de ancho de banda. (Adjuntar una copia de los formularios de solicitud debidamente llenados).
- Si se requiere el arrendamiento de circuitos, deberá adjuntarse la carta compromiso otorgada por la empresa que va a proveer los mismos, que indique las características técnicas de operación.
- Requerimiento de conexión. (Interna o Externa)

3.5.3 Derechos del permiso

Mediante Resolución 072-03-CONATEL-2002 el Consejo Nacional de Telecomunicaciones resuelve determinar como valor de permiso para la prestación de servicios de valor agregado el valor de USD 500 dólares de los Estados Unidos de América.

3.5.4 Duración

El plazo de duración de un permiso para la operación de Redes Privadas será de 5 años, prorrogables por igual período, a solicitud escrita del interesado, presentada con tres meses de anticipación al vencimiento del plazo original, siempre y cuando haya cumplido con los términos y condiciones del título habilitante. Cumplido el plazo el permiso se caducará ex *lege.*

3.5.5 Instructivos

La Secretaría Nacional de Telecomunicaciones ha establecido los formularios necesarios para el trámite correspondiente a la obtención, ampliación y/o modificación del permiso de operación de RED PRIVADA; estos están organizados de la siguiente forma:

- Formulario ST-1A-DGGST (Formulario de Información General).- Este formulario debe ser incluido en cualquier solicitud obtención, ampliación y/o modificación del permiso de operación de RED PRIVADA. En este formulario se debe registrar toda la información legal del solicitante y el responsable técnico.

- Formulario ST-2A-DGGST (Formulario para Información características técnicas y control de documentación).- Este formulario debe ser incluido en cualquier solicitud de obtención, ampliación y/o modificación del permiso de operación de RED PRIVADA. Se debe indicar las características técnicas generales de la RED PRIVADA y describir todos los documentos técnicos - legales (formularios) que se presentan con la solicitud que para el efecto han sido establecidos por esta Secretaría.

3.5.6 Formularios

ST-1A. FORMULARIO PARA INFORMACIÓN LEGAL

OBJETIVO DE LA SOLICITUD. Solicitar el Permiso de Operación de Red Privada, así como ampliaciones y/o modificaciones del mismo (marcar solamente una).

MEDIO DE TRANSMICIÓN DEL SISTEMA. Se refiere al medio de transmisión que se utilizará para comunicar las estaciones (pueden marcarse los tres de ser el caso).

DATOS DEL SOLICITANTE Y PROFESIONAL TECNICO

PERSONA NATURAL. Nombres, apellidos y número de cédula de identidad en los casilleros correspondientes, de acuerdo a la identificación presentada. Adjuntar copia de la cédula de identidad.

PERSONA JURÍDICA, NOMBRE DE LA EMPRESA. Denominación legal de la empresa.

REPRESENTANTE LEGAL. Nombres, apellidos y número de cédula de identidad en los casilleros correspondientes, de acuerdo a la identificación presentada. Adjuntar adicionalmente copia del nombramiento del representante legal.

CARGO. De acuerdo al nombramiento presentado con la solicitud.

ACTIVIDAD DE LA EMPRESA. Labor principal a la que se dedica la empresa. Se deberá además, especificar el número de RUC de la empresa en el casillero correspondiente.

DIRECCIÓN. Provincia, Ciudad y Dirección exacta, ya sea de la persona natural o empresa, en donde se recepte la correspondencia enviada. Consta además, la dirección electrónica (E-MAIL), casilla y teléfono.

CERTIFICACIÓN DEL PROFESIONAL TÉCNICO (RESPONSABLE TÉCNICO). Se deben establecer los datos del profesional a cargo del sistema de telecomunicaciones. La certificación representa una autorización, para que la persona encargada del sistema pueda representar al solicitante en cualquier requerimiento técnico que la SENATEL realice. El profesional a cargo debe ser un Ingeniero en Electrónica y Telecomunicaciones afiliado a uno de los colegios profesionales del país; deberá adjuntarse a este formulario una copia de la licencia profesional actualizada del responsable técnico.

CERTIFICACIÓN DE LA PERSONA NATURAL O REPRESENTANTE LEGAL. Esta certificación representa una declaración de que la Persona Natural o Jurídica acepta las condiciones del estudio técnico presentado y delega la responsabilidad sobre el mismo al responsable técnico.

OBSERVACIONES: En caso de que el solicitante requiera hacer una aclaración a la información declarada, deberá especificarla brevemente en este campo.

PARA USO DE LA SENATEL. Campo reservado para uso exclusivo de la SENATEL, por lo tanto no debe ser llenado.

ST-2A. FORMULARIO PARA INFORMACIÓN TÉCNICA

CONFIGURACIÓN DEL SISTEMA: En el caso de requerir de uso de espectro radioeléctrico (sistemas de modulación digital de banda ancha), indicar la configuración del sistema que desea operar.

COBERTURA. Nombre de las provincias, ciudades o poblaciones que cubre el sistema solicitado.

CARACTERISTICAS DEL SISTEMA. Se deberá colocar el número de estaciones, repetidoras, el número de enlaces de cobre, el número de enlaces de fibra óptica, el número de enlaces de Sistemas de Modulación Digital de Banda Ancha (SMDBA), el número de enlaces del Servicio Fijo por Satélite (FMS) y el número total de enlaces. Por ejemplo si un sistema está compuesto por: 3 estaciones y 1 repetidor; 3 enlaces de los cuales 2 utilizan SMDBA y el restante el medio de transmisión es físico (fibra óptica), el formulario deberá estar lleno de la siguiente forma:

Tabla 3. 5 Formulario características del sistema

4) ***CARACTERISTICAS DEL SISTEMA***						
No. ESTACIONES	No. REPETIDORES	No. ENLACES FISICOS		ENLACES INALAMBRICOS		No. TOTAL DE ENLACES
		COBRE	FIBRA OPTICA	FMS	SMDBA	
3	1	-----	1	----	2	3

FORMULARIOS QUE SE DEBEN ADJUNTAR: El solicitante marcará con una (X) al frente de cada formulario que contiene su solicitud.

Tabla 3. 6 Formularios de información (Provistos por la SENATEl)

SISTEMAS DE MODULACIÓN DIGITAL DE BANDA ANCHA (SMDBA)	
FORMULARIO RC-1B FORMULARIO PARA INFORMACIÓN LEGAL	( )
FORMULARIO RC-3A FORMULARIO PARA INFORMACIÓN DE ANTENAS	( )
FORMULARIO RC-9A FORMULARIO PARA LOS SISTEMAS DE SMDBA (ENLACES PUNTO-PUNTO)	( )
FORMULARIO RC-9B FORMULARIO PARA LOS SISTEMAS DE SMDBA (ENLACES PUNTO-MULTIPUNTO)	( )
FORMULARIO RC-2A FORMULARIO PARA LA INFORMACIÓN DE LA INFRAESTRUCTURA	( )
FORMULARIO RC-4A FORMULARIO PARA INFORMACIÓN DE EQUIPAMIENTO	( )
FORMULARIO RC-9B FORMULARIO PARA LOS SISTEMAS DE SMDBA (SISTEMA PUNTO-MULTIPUNTO	( )
FORMULARIO RC-15ª FORMULARIO DE EMISIONES DEL RNI	( )

SISTEMA SERVICIO FIJO POR SATÉLITE (FMS)	
FORMULARIO RC-1A FORMULARIO PARA INFORMACIÓN LEGAL	( )
FORMULARIO RC-3A FORMULARIO PARA INFORMACIÓN DE ANTENAS	( )
FORMULARIO RC-11A FORMULARIO PARA LOS SISTEMAS FIJO POR SATÉLITE	( )
FORMULARIO RC-2A FORMULARIO PARA LA INFORMACIÓN DE LA INFRAESTRUCTURA DEL SISTEMA	( )
FORMULARIO RC-4A FORMULARIO PARA INFORMACIÓN DE EQUIPAMIENTO	( )
FORMULARIO RC-15A FORMULARIO DE EMISIONES DEL RNI	( )

CAPITULO 4

DISEÑO, PRUEBAS Y RESULTADOS EXPERIMENTALES DE LA RED DE INTERNET PORTATIL

Introducción

Este capítulo aborda el diseño de una red WMNs para las áreas seleccionadas, tomando en cuenta o identificando los diferentes requisitos tecnológicos y necesidades de la población que conlleva diseñar dicha red.

4.1 Diseño teórico de la red de internet portátil

Una vez seleccionada el área de interés donde se pretende brindar servicio de internet portátil que cubre un terreno de 1916400 metros cuadrados aproximadamente y de acuerdo a las características técnicas dadas por el proveedor del equipo que indica que la cobertura máxima teórica del AP 5131 es de 300 metros de radio, se realiza un diseño teórico en base a estas carateristicas para tener una idea clara de cuantos nodos (APs) se deben utilizar para cubrir el área de interés.

Para que un usuario pueda desplazarse dentro de la red inalámbrica sin que pierda conectividad en el área de servicio es recomendable un sobrelapamiento de las celdas de cobertura (Entre APs) del 10 al 15% como se muestra en la figura 4.1.

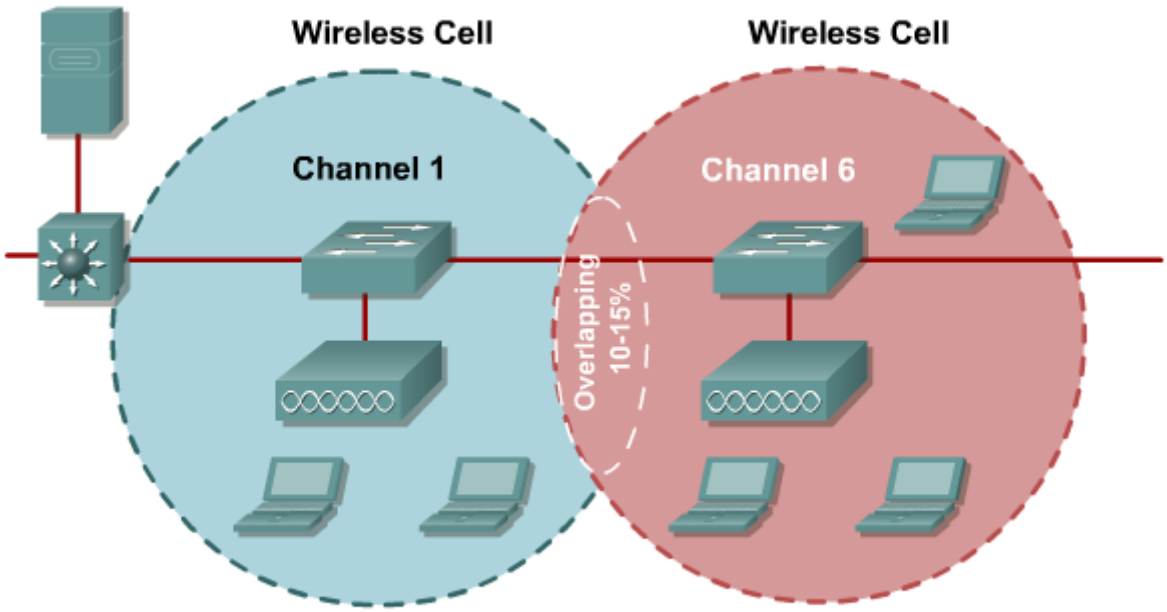


Figura 4. 1Sobrelapamiento entre celdas [25]

El área efectiva de cada nodo usando las características técnicas del AP 5131 con un 15% de sobrelapamiento es de 0.24 kilometros cuadrados.

Para conocer el número de nodos teóricos necesarios para cubrir el área de interés, se lo realiza en el siguiente proceso.

Área a cubrir aproximadamente: 1.91 km^2
Máxima cobertura teórica 300 metros de radio.
Area efectiva por nodo con sobrelapamiento del 15% es de 0.24 km.

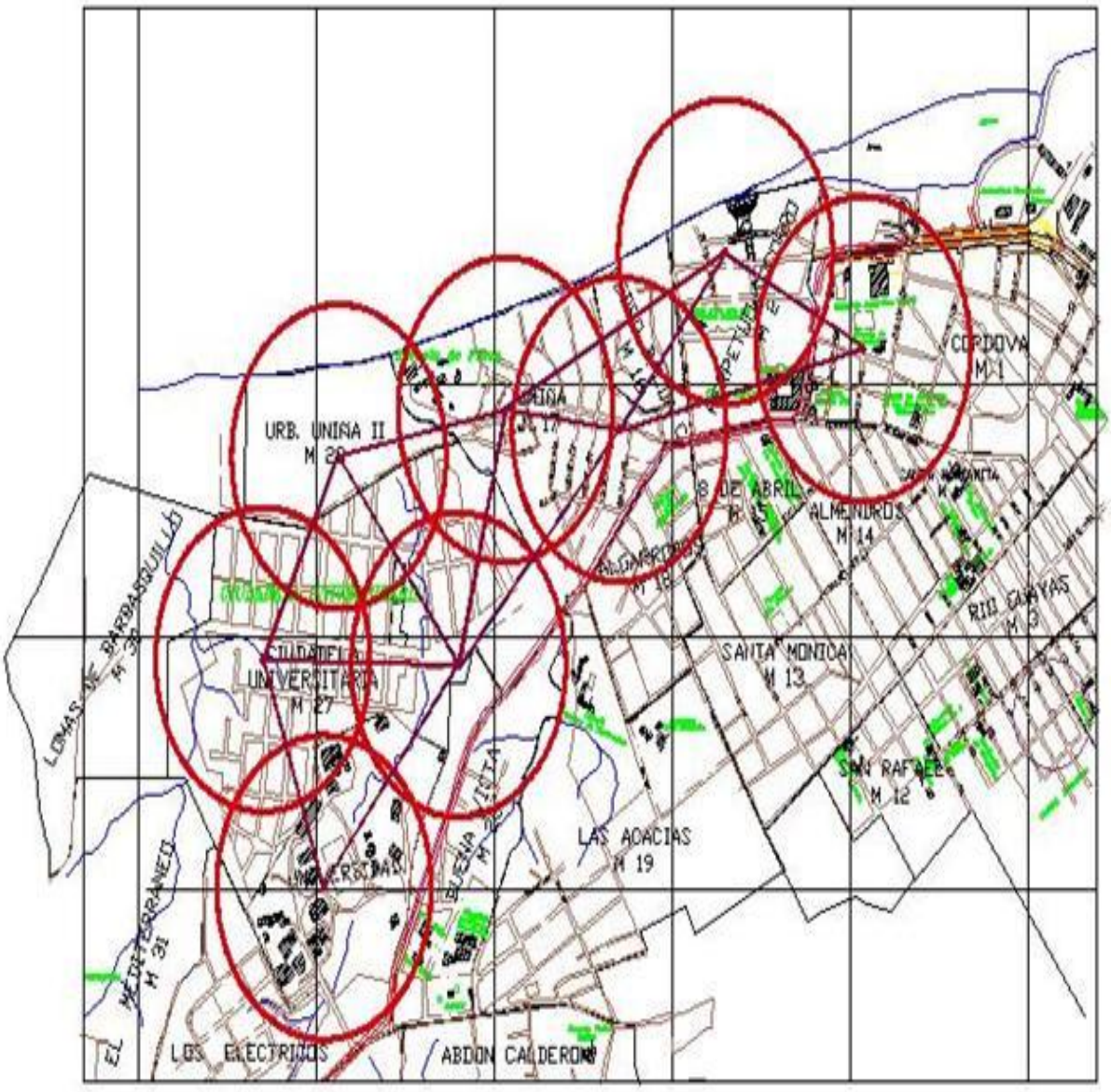
Ecuación 4. 1 Numero de Nodos

$$No\ de\ Nodos = \frac{Area\ a\ cubrir}{Area\ efectiva\ por\ nodo} = \frac{1.91}{0.24} = 7.95$$

[25] http://ev-iip.netacad.net/virtuoso/servlet/org.cli.delivery.rendering.servlet.CCServlet/LMS_ID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=en,Version=1,RootID=knet-lcms_ccnp3_en_50,Engine=static/CHAPID=null/RLOID=null/RIOID=null/ch6/main.html

De acuerdo a la ecuación 4.1 el número de nodos necesarios para cubrir el área de interés es 8. A continuación se muestra en la Figura 4.2 un diseño de la red de internet portátil.

Figura 4. 2 Diseño teórico de la red de internet portátil


URB. UNIMA II
M 28
CIUDADELA
UNIVERSITARIA
M 27
CORDOVA
M 1
8 DE ABRIL
M 15
ALMENDROS
M 14
SANTA MONICA
M 13
RIO GUAYAS
M 3
SAN RAFAEL
M 12
LAS ACACIAS
M 19
LOMAS DE BARBASQUILLO
M 30
EL MEDITERRANEO
M 31
LOS ELECTRICOS
ABDON CALDERON

4.2 Estudio de campo

El estudio de campo permite observar las condiciones reales en la cual va a ser implementada la red de internet portátil, además permite comprobar la cobertura máxima efectiva del equipo (incluido antenas y amplificadores) en condiciones reales

Los equipos utilizados en las pruebas de campo fueron los siguientes:

- Mapa político de la ciudad de Manta para tener una referencia de las zonas potenciales de cobertura.
- 2 equipos AP-5131
- 4 antenas direccionales de 20 db.
- 4 antenas omnidireccionales de 17 db.
- 2 amplificadores de potencia.
- 2 LAPTOP se utilizaron para hacer pruebas en tiempo real.

4.2.1 Configuración del AP-5131 para una red mesh básica AP-5131.

Un AP-5131 puede ser configurado en dos modos para soportar la configuración tipo MESH, como repetidor o base (que acepta equipos clientes), tanto la base como el repetidor pueden ser usados como APs al mismo tiempo por clientes fijos.

Un repetidor siempre busca otros APs usando WLAP ESSID, luego es necesario pasar por el proceso de asociación y autenticación para establecer una conexión inalámbrica con los dispositivos localizados. Una vez que está completo el proceso los clientes se añaden a la conexión como un puerto en el repetidor. Este permite que el repetidor empiece a enviar paquetes al AP base, y este a la vez empieza a comunicarse con el repetidor utilizando *Spanning Tree Protocol* (STP).

Tanto los APs configurados como base o repetidor funcionan para transmitir datos con Mus en el área de cobertura y también enviando trafico a otros Aps en la red *Mesh.*

El STP determina el camino a la raíz y detecta si la conexión es parte de un lazo con otro sistema, una vez que el *spanning tree* converge los repetidores empiezan a alimentar su tabla de enrutamiento.

Por lo tanto la red tipo *MESH* puede conectarse simultáneamente con otras redes de manera que el lazo no está creado y por la tanto la conexión no está bloqueada, una vez que los repetidores establecen una conexión comienzan a establecer otras conexiones como que estén libres, así el repetidor establece enlaces redundantes.

Para configurar un AP para soporte de una red *mesh* se debe realizar lo siguiente:

- Configurar la red LAN para un soporte *mesh*
- Configurar las redes WLAN para un soporte *mesh*
- Configurar los radios para un soporte *mesh*

4.2.1.1 Configurar la red LAN para un soporte *mesh*

Como el protocolo STP menciona, cada red *mesh* mantiene los temporizadores para los paquetes *hello, forward delay y max age.* El equipo definido como raíz impone los temporizadores a través de la red, el administrador no necesariamente debe cambiar estos valores, si embargo, es importante definir un equipo como BASE y como puente raíz configurando la prioridad de puente.
Para definir la red LAN para un soporte de red se siguen los siguientes pasos:

1. Selecciona del menú ***Network Configuration -> LAN***
2. Habilita la LAN usada para las redes *mesh*. Verifica si la LAN habilitada esta apropiadamente nombrada para su función

3. Selecciona del menú ***Network Configuration -> LAN -> LAN1 or LAN2***
4. Selecciona ***Mesh STP Configuration*** que se encuentra en la parte inferior de la pantalla
5. Define los parámetros para la red *mesh*

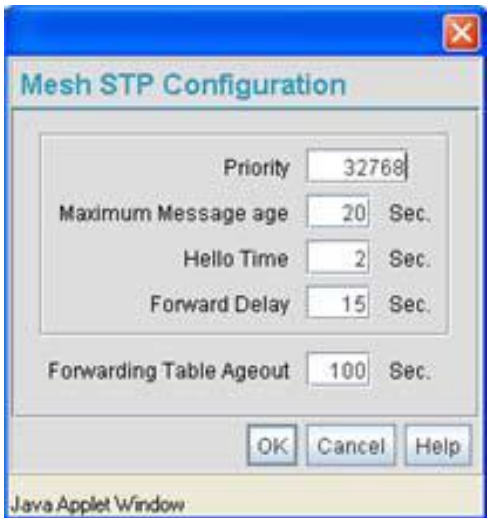


Figura 4. 3 CONFIGURACION STP

Priority: Se recomienda asignar al AP base con la prioridad lo más bajo posible para forzar al dispositivo como la raíz. Si la raíz ya existe cambia las propiedades de acuerdo a la de la raíz. Cada dispositivo empieza con una prioridad por defecto de 32678.

Maximum Message age: Este temporizador es usado junto al temporizador *age*. El temporizador *age* sirve para regular la información de los BPDU que se encuentran grabadas en los puertos. Una vez que el tiempo excede los paquetes BPDU son eliminados.

Hello time: Es el tiempo de envío entre los BPDU. Este tiempo por defecto es equivalente a 2s. pero puede cambiar de 1 a 10 s. El estándar 802.1d recomienda que el *hello* time debe ser puesto a un valor menos a la mitad del valor de *Max Message age.*

Forward Delay: Es el tiempo que se demora en cambiar del estado escucha al estado de aprender. Por defecto el tiempo es equivalente al 15s, pero puedes cambiar desde 4 a 30s. El estándar 802.1d recomienda que el *forward delay* deba ser mayor a la mitad del valor *Max Message Age*.

Forwarding Table Ageout: Define el tiempo máximo que una dirección se va a mantener en la tabla de envío antes de ser borrada debido a su falta de uso. Si la dirección es usada siempre el tiempo no será usado. Sin embargo, si el destino no es usado el comienza el contador hasta que llegue al tiempo máximo, una vez que excede este tiempo la dirección es borrada de la tabla de envío.

4.2.1.2 Configuración WLANs

Cada AP base o repetidor en la misma red *MESH* debe poseer iguales tanto el ESSID, políticas de seguridad, política de calidad de servicio.

Motorola recomienda que una del las 16 WLAN que posee el equipo sea destinada exclusivamente para realizar *MESH*

Para definir los parámetros de la WLAN que van a poseer tanto la base como los repetidores de la red *MESH* se siguen los siguientes pasos.

- En *NETWORK CONFIGURATION -> Wireless* del menú del AP -5131 se despliegan las WLANs en la tabla.
- Se selecciona el botón *Create* para configurar una nueva WLAN para que soporte únicamente *MESH*, o puede ser editada una WLAN ya existente de la lista.

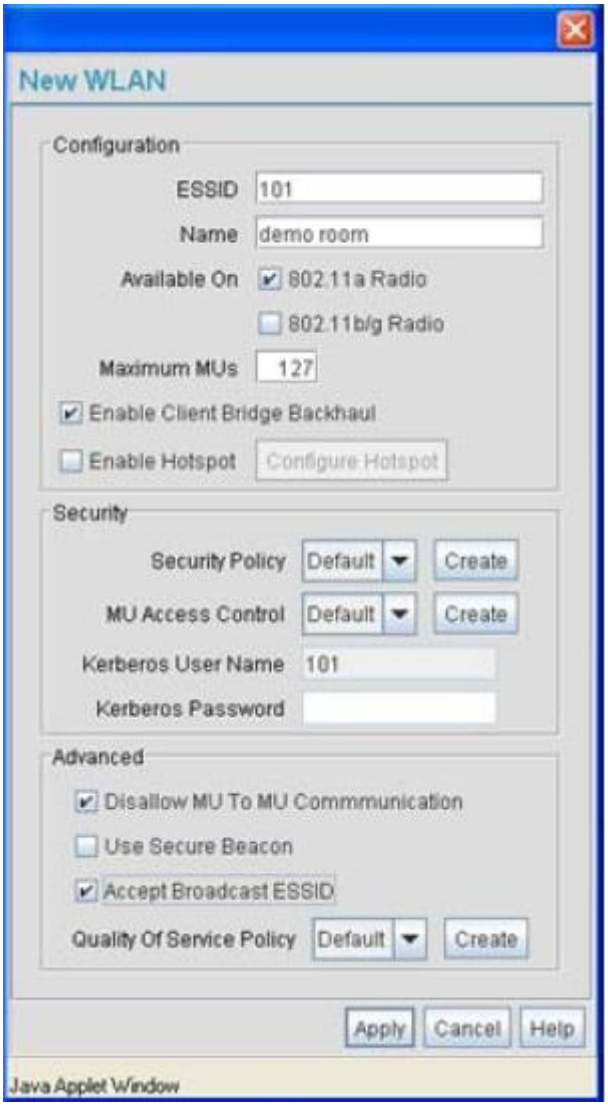


Figura 4. 4 Configuración de WLANs

- Se asigna un ESSID y un nombre a la WLAN que cada AP va a usar para la parte MESH, siendo en cada AP el mismo ESSID.

- Usar *Available On* para especificar los radios usados con la WLAN en la red MESH, para permitirle trabajar como base o repetidor, si el radio va a ser usado como repetidor el botón *Available On* no debe ser seleccionado.

- Se usa *Mamimum MUs* para definir el máximo de equipos que pueden asociarse con esta WLAN, este número debe ser definido basado en el número de repetidores en la red *mesh,* este valor puede crecer como crezca la red *mesh* y dispositivos sean agregados.

- Se selecciona *Enable Client Bridge Backhaul* para permitir a esta WLAN en la pestaña de *MESH Network Name* del menú de la pantalla de Radio *Configuration.*

- Se refiere las políticas de seguridad de la WLAN que va a ser usada para *MESH*, debe ser configurada cuidadosamente de forma que tenga todas las WLANs de los APs las mismas seguridades.

- Las políticas de las listas de acceso deben ser configuradas para negar un rango de direcciones MAC para trabajar en la red MESH.

- Se selecciona *Disallow MU to MU Communication* para restringir la comunicación entre MUs en la misma WLAN,

- Se selecciona *Use Secure Beacon* para no transmitir el ESSID a los APs y dispositivos sin que se encuentren en la red *MESH*. Si un hacker trata de encontrar un ESSID a través de un MU, el ESSID del AP no se muestra a menos que el dispositivo se encuentre registrado en la red.

- Se selecciona *Accept Broadcast* ESSID para asociar MUs que tienen en blanco el ESSID (sin importar cual ESSID está usando el AP).

- Si existen ciertos requerimientos para datos se selecciona una política de calidad de servicio que se adapte mejor a los requerimientos de la red MESH.

- Luego se pulsa el botón de aplicar para finalizar el proceso en la parte WLAN.

4.2.1.3 Configuración de los radios para un soporte *mesh.*

Un radio destinado al uso de una red *mesh* requiere de una configuración única en comparación a un radio con un configuración por defecto, esta sección describe como configurar un radio para un optimo soporte de red *mesh.*

Para configurar un radio para un soporte *mesh* se siguen los siguientes pasos:

1. Selecciona del menú ***Network configuration→ Wireless→Radio Configuration.***

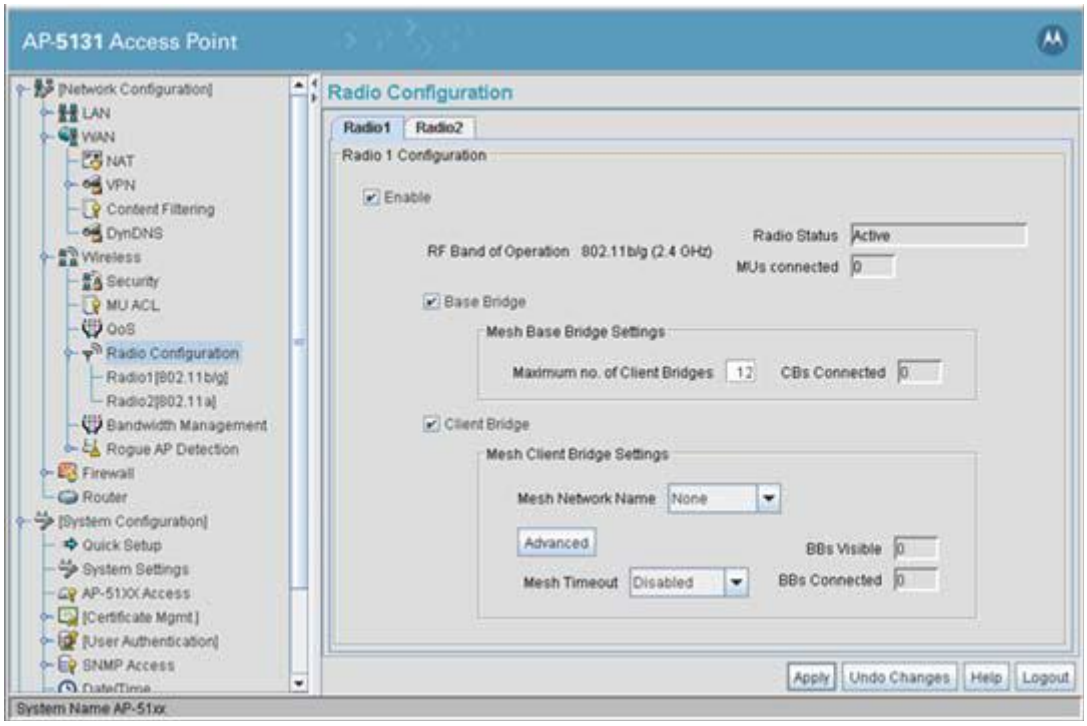


Figura 4. 5 Configuación de radio

2. Habilita el radio usando el *Enable checkbox(es)* para radio 1 o 2. Asegura que estas habilitando el radio correcto ya sea 802.11a o 802.11b. Una vez configurado estos parámetros los valores de estado del radio y los clientes que están conectados al mismo se actualizarán automáticamente en tiempo real.

3. Selecciona la opción equipo base (*Base Bridge*) para permitir que otros dispositivos se conecten por medio de este radio en modo repetidor (*Client Bridge*). La base es el que acepta la petición de conexión más no el que la inicia.

4. Si la opción de equipo base ha sido seleccionada, usa el parámetro de número máximo repetidores para definir la carga de repetidores máxima para este equipo base. El número máximo de repetidores por radio es de 12 repetidores siendo 24 el máximo para el equipo base. Una vez configurado estos parámetros se realiza una actualización para saber cuántos repetidores están conectados al radio, estos valores se actualizan en tiempo real.

5. Selecciona la opción repetidor (*Client Bridge*) para iniciar la petición de conexión a la red *mesh* en la misma WLAN. Si la opción de repetidor es seleccionada, usa el parámetro de Nombre de la red (*Mesh Network Name*) para seleccionar a que WLAN el repetidor de establecer una conexión. WLAN específicamente para la red *mesh* separándola de las demás WLAN que no soportan la redes *mesh*, realizado este paso se actualiza y se muestran los equipos bases disponibles en tiempo real.

6. Selecciona la opción de avanzados para definir la prioridad de los equipos bases a la cual el repetidor debe establecer una conexión.

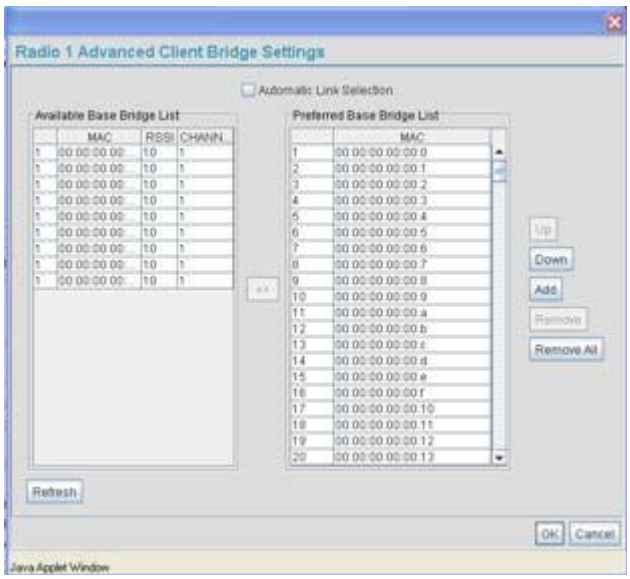


Figura 4. 6 Configuración avanzada

7. Selecciona la opción automático (*Automatic Link Selection*) para permitir a los equipos seleccionar sus enlaces para la red *mesh*.

8. Con respecto a la lista de equipos bases disponibles se dispone de la siguiente información.

    a. **MAC:** Este campo muestra la dirección física del equipo.

    b. **RSSI:** El RSSI (*Relative Signal Strength Indicator*) muestra la fuerza de la señal del dispositivo con respecto al repetidor. Esta información es útil para el administrador para cambiar su lista de enlaces prioritarios.

    c. **CHANN:** Muestra el nombre canal que se está usando. Los repetidores solo se conectan con los equipos bases que se encuentran en el mismo canal.

9. Presiona OK para regresar a la configuración de radio, *Apply* para guardar los cambios realizados y *Cancel* para regresar a la configuración anterior.

4.2.2 ANALISIS DE RESULTADOS

Para las pruebas de campo se escogieron tres localidades diferentes que representan la mayoría de las características urbanas de la zona de interés de este proyecto.

Una vez instalado el equipo AP 5131 en el lugar establecido se procedió a realizar las mediciones de cobertura usando una laptop con una tarjeta inalámbrica estándar.

La tarjeta inalámbrica, en sus propiedades nos permite observar y monitorear el estado del enlace como se puede apreciar en la Figura 4.7

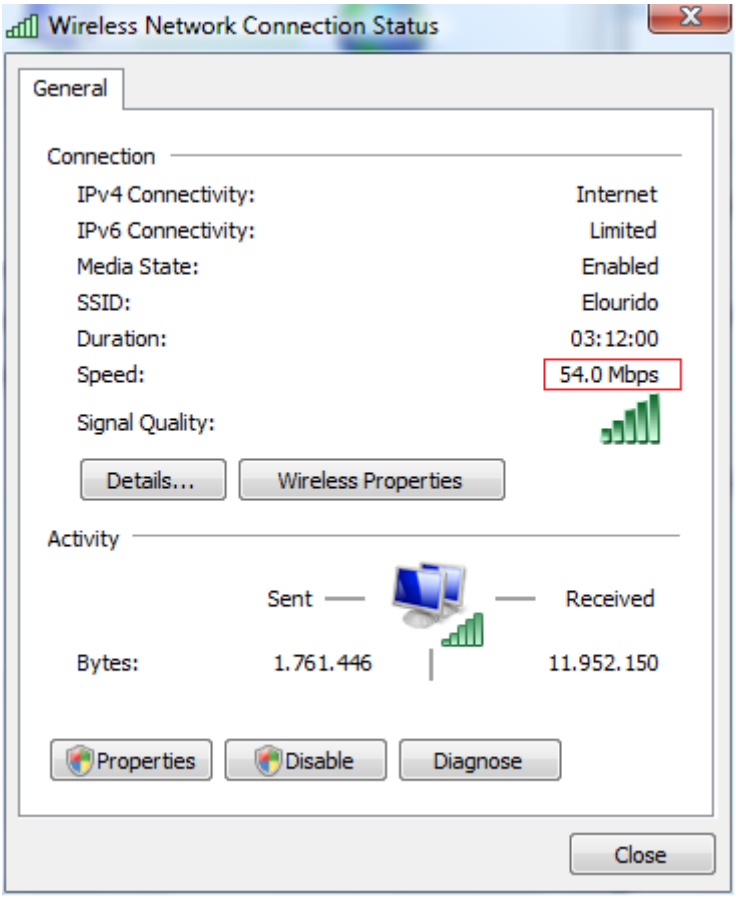


Figura 4. 7 Estado del Enlace

Al desplazarse alrededor del nodo y realizando pruebas de descarga se obtuvieron los siguientes resultados

Se debe tener en cuenta que las Figuras mostradas a continuación son una aproximación a la cobertura real y se las muestra de manera didáctica.

4.2.2.1 Prueba de cobertura Hotel Oro Verde

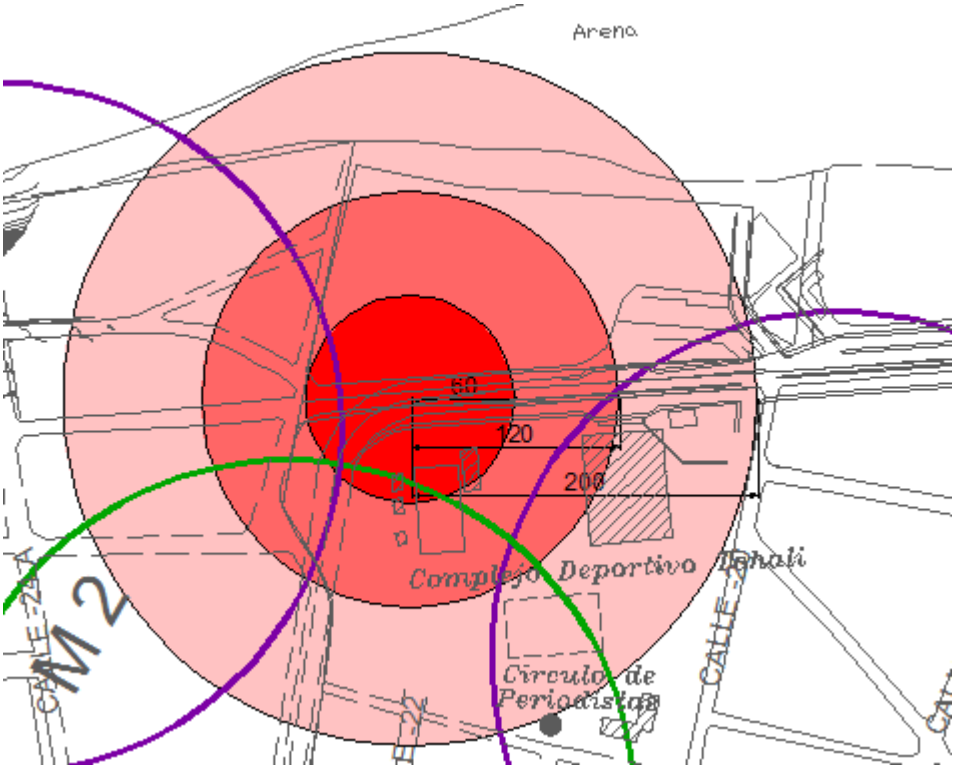


Figura 4. 8 **Cobertura del nodo Oro Verde**

Locación 0°59´29.76´´S: Este nodo se encuentra localizado en las terrazas del hotel Oro Verde la calle 23 y avenida malecón con una altura de 20m sobre el nivel de mar. Las características de radiación del radio 802.11g se presentan a continuación.

- Se obtiene una excelente cobertura con una tasa de transmisión de 54 Mbps en las distancias de radio 0-60 m.
- Se obtiene una cobertura buena con una tasa de transmisión que varía desde 54-24 Mbps a distancias de radio 60-120m aproximadamente
- Se obtiene una cobertura dentro de los límites de operación con una tasa que varía desde 24-6 Mbps a distancias de radio 120-200 m aproximadamente.

4.2.1.2 Prueba de cobertura ULEAM

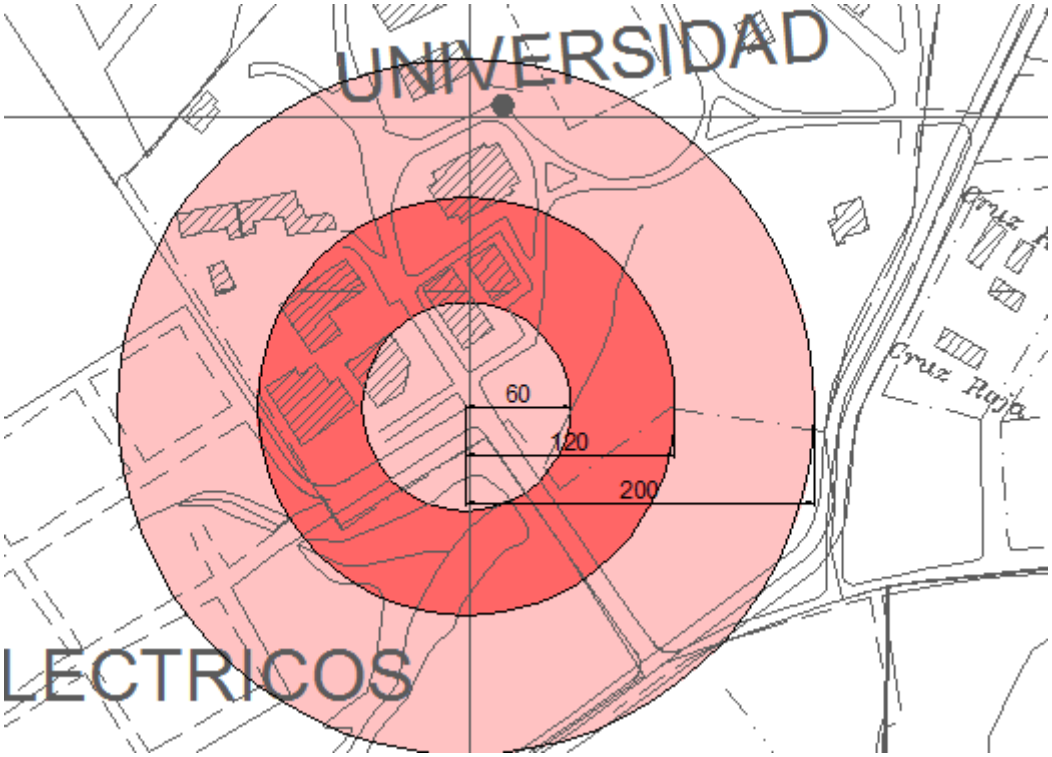


Figura 4. 9Cobertura del nodo ULEAM

Locación 0°57´12.20´´S: Este nodo se encuentra en el edificio de la facultad de medicina de la Universidad Laica Eloy Alfaro (ULEAM) con una altura de 30m sobre el nivel del mar y abarca la zona del campus universitario y alrededores. Las características de radiación del radio 802.11g se muestra a continuación.

- Se obtiene una excelente cobertura con una tasa de transmisión de 54 Mbps en las distancias de radio 0-57 m.
- Se obtiene una cobertura buena con una tasa de transmisión que varía desde 54-24 Mbps a distancias de radio 57-116m aproximadamente
- Se obtiene una cobertura dentro de los límites de operación con una tasa que varía desde 24-6 Mbps a distancias de radio 116-194 m aproximadamente.

4.2.1.3 Prueba de cobertura *Global Dental*

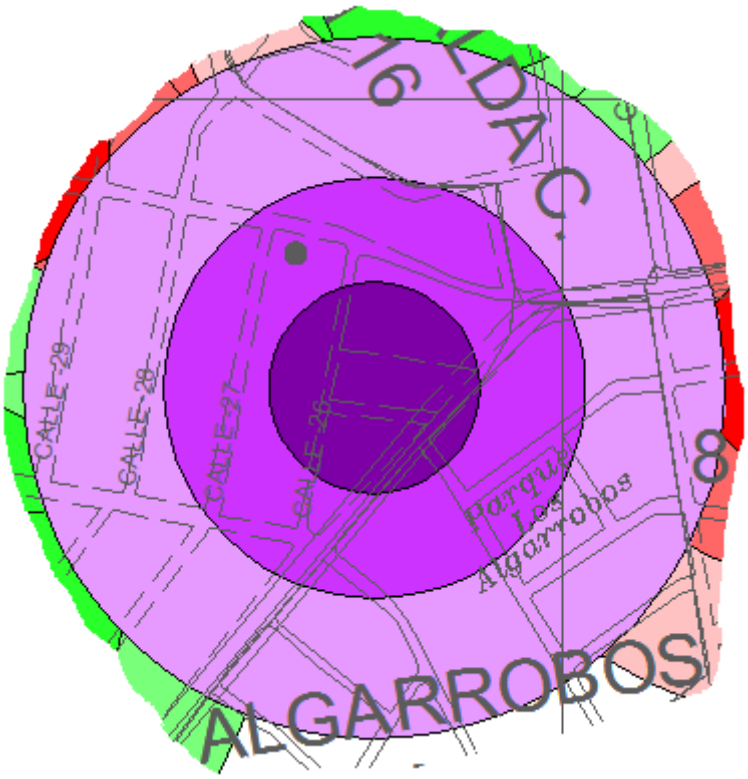


Figura 4. 10 **Cobertura del nodo *Global Dental***

Locación 0°56´34.94´´S: Este nodo se encuentra en la torre del edificio de *Global Dental* con una altura de 17m sobre el nivel del mar y abarca parte de la zona residencial del conjunto Pedro Balda Cucalón. Las características de radiación del radio 802.11g se muestra a continuación.

- Se obtiene una excelente cobertura con una tasa de transmisión de 54 Mbps en las distancias de radio 0-68 m.
- Se obtiene una cobertura buena con una tasa de transmisión que varía desde 54-24 Mbps a distancias de radio 68-131m aproximadamente
- Se obtiene una cobertura dentro de los límites de operación con una tasa que varía desde 24-6 Mbps a distancias de radio 131-207 m aproximadamente.

4.2.3 Resultados

Los resultados obtenidos dentro de las pruebas de campo en coordinación con la empresa COMPUATEL S.A mostraron que se puede obtener una señal excelente a una tasa de 54 Mbps en un promedio de 60 metros con un límite de cobertura de 200m a una tasa de 6 Mbps en tres locaciones diferentes donde se hicieron las pruebas.

El área efectiva de cada nodo real del AP 5131 con un 15% de sobrelapamiento es de 0.10 kilómetros cuadrados.

Para conocer el número de nodos necesarios para cubrir el área de interés, se lo realiza en el siguiente proceso.

Área a cubrir aproximadamente: 1.91 km^2
Máxima cobertura práctica 200 metros de radio.
Área efectiva por nodo con sobrelapamiento del 15% es de 0.10 km.

Ecuación 4. 2 Número de nodos reales

$$No\ de\ Nodos = \frac{Area\ a\ cubrir}{Area\ efectiva\ por\ nodo} = \frac{1.91}{0.10} = 19.10$$

De acuerdo a la ecuación 4.2 el número de nodos necesarios para cubrir el área de interés es 20.

A continuación se muestra en la Figura 4.12 un diseño de la red de internet portátil que cumple con el alcance real del equipo AP 5131.

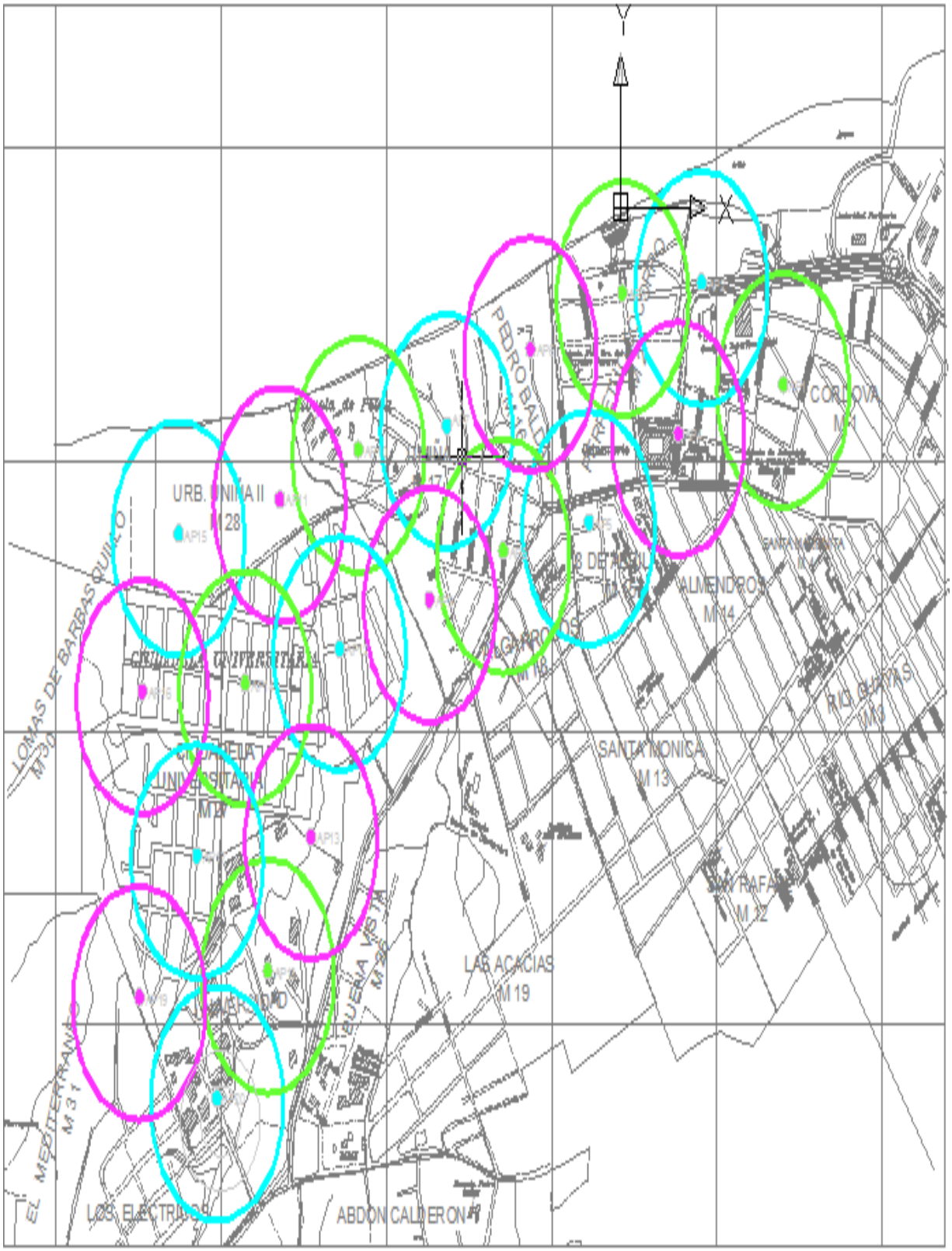


Figura 4. 12 Diagrama de cobertura tentativo

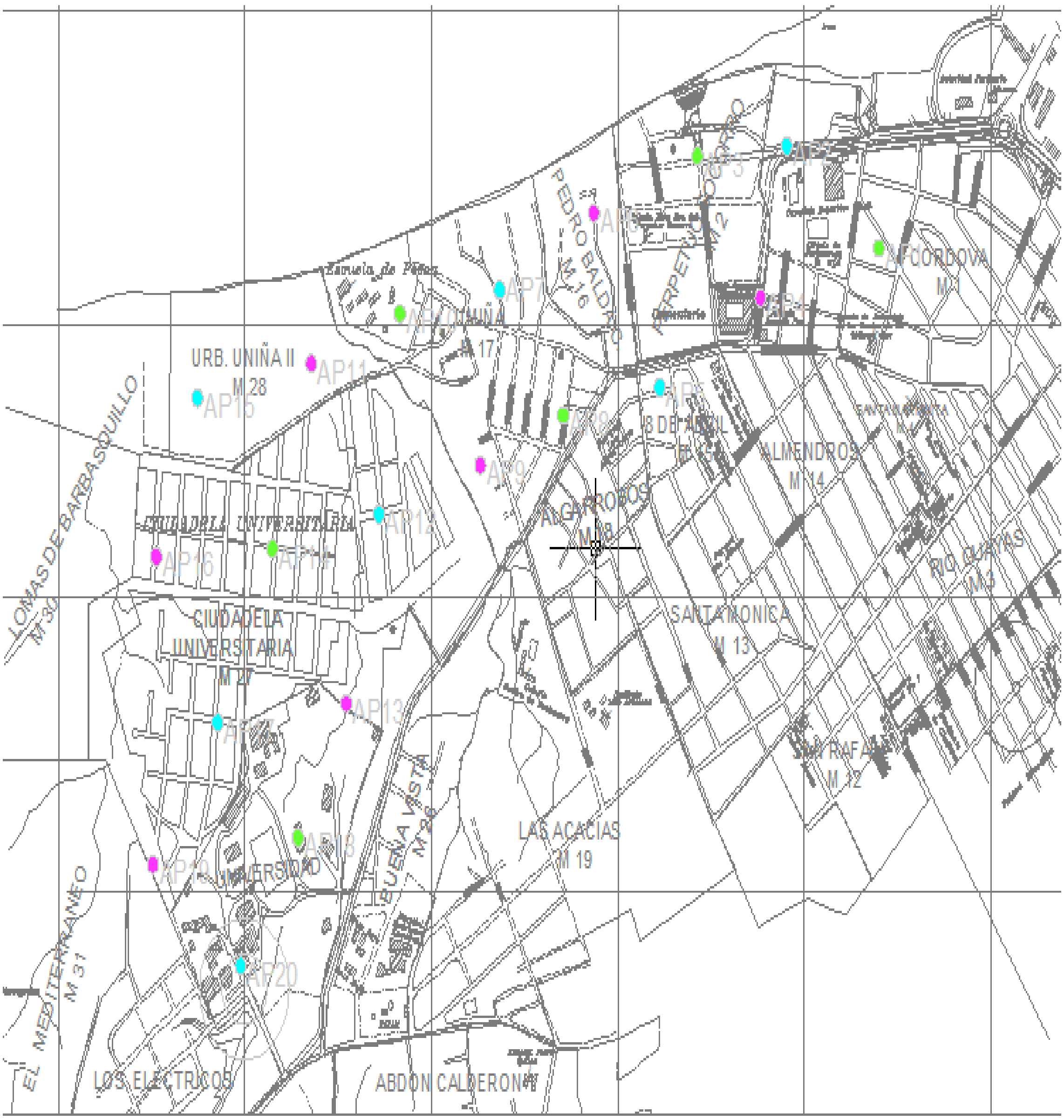


Figura 4. 13 Locación tentativa de los nodos

4.2.3.1 Locación Tentativa de los nodos

A continuación se muestra en la tabla 4.1 la ubicación tentativa de los nodos usando la herramienta Google Earth.

Tabla 4. 1 Locación tentativa de los nodos

Simbología	Coordenadas
AP1	0°56'36.16"S
AP2	0°59´29.76´´S
AP3	0°56´30.70´´S
AP4	0°56'38.58"S
AP5	0°56'43.78"S
AP6	0°56'35.68"S
AP7	0°56'38.18"S
AP8	0°56'44.94"S
AP9	0°56´48.99´´S
AP10	0°56'38.84"S
AP11	0°56'42.35"S
AP12	0°56'49.81"S
AP13	0°56'57.58"S
AP14	0°56´55.64´´S
AP15	0°56'41.24"S
AP16	0°56'54.91"S
AP17	0°57'1.36"S
AP18	0°57´12.20´´S
AP19	0°57'14.48"S
AP20	0°57'20.80"S

4.3 Limitaciones

4.3.1 Redes WI-FI para largas distancias

La familia de estándares IEEE 802.11 a/b/g, más conocida como Wi-Fi, tiene asignadas las bandas ISM (*Industrial, Scientific and Medical*) 2.400-2.4835 GHz, 5.725-5.850 GHz para uso en las redes inalámbricas basadas en espectro ensanchado con objeto de lograr redes de área local inalámbricas (WLAN).

El gran ancho de banda (entre 1 y 11 Mbps para 802.11b y hasta 54Mbps para (802.11a/g), lo presenta como una de las mejores opciones para la transmisión de datos en forma inalámbrica. Este estándar, puede ser utilizado (bajo ciertas

condiciones) para implementar redes inalámbricas que requieren de enlaces de larga distancia. Por ejemplo en Perú se ha logrado establecer enlaces de alrededor de 40Km de distancia utilizando el estándar IEE802.11. Las ventajas e inconvenientes que se presentan el uso de esta tecnología se indican a continuación.

- Al ser una tecnología creada para redes de corto alcance, hay que solventar ciertos problemas relacionados con su utilización para distancias de decenas de Kilómetros.
- El número de colisiones aumenta en relación con el número de usuarios.
- Tiene un número limitado de canales no interferentes, 3 en 2.4 GHz y 8 en 5.8 GHz.

4.3.2 Problemática del uso de WI-FI para largas distancias

Dado que la familia de estándares IEEE802.11 en su inicio fue diseñada para redes locales, la mayor dificultad reside en su aplicación para largas distancias.

Cuando se quiere usar WI-FI para enlaces más largos de los previstos en el estándar, cabe preguntarse donde están las limitaciones de distancia y prestaciones.

Los límites físicos de distancia alcanzable con Wi-Fi dependerán de los siguientes
Parámetros:

- La máxima potencia que podamos transmitir (PIRE).
- Las pérdidas de propagación.
- La sensibilidad de recepción.
- La mínima relación señal a ruido que se esté dispuesto a aceptar como suficiente.

El propio estándar determina que los límites de potencia que se puede transmitir dependen de los procesos en la banda de frecuencias ISM para cada región geográfica.

Además, hay algunos aspectos que deben ser tomados en cuenta para obtener una mayor estabilidad en el enlace:

Velocidad: El protocolo IEEE802.11 recoge distintas velocidades según el modo de funcionamiento: 1, 2, 5.5 y 11 Mbps para 802.11b; 6, 9, 12, 18, 24, 36, 48 y 54 Mbps para 802.11a, y el conjunto de todas las anteriores para el modo 802.11g.

Estos modos usan diferentes tipos de modulación y codificación, de forma que cuanto mayor sea la velocidad, mayor es la potencia necesaria en recepción para mantener un enlace con un BER bajo. Está potencia, llamada sensibilidad, obliga a usar velocidades bajas si se quiere lograr enlaces de larga distancia con una cierta estabilidad. La diferencia en la sensibilidad de recepción entre 1 y 11Mbps, suele ser de más de 10 dB, lo cual equivale prácticamente a cuadruplicar con 1Mbps el alcance que se tiene con 11Mbps. Si además se tiene en cuenta que la banda de 2.4 GHz impone limitaciones en cuanto al nivel de potencia que es legal transmitir, es fácil comprobar que para enlaces muy largos normalmente deben usarse las velocidades más bajas de 802.11b para tener estabilidad y buena calidad. La aparición de tarjetas con mejores sensibilidades o el estándar 802.11g pueden ayudar a lograr velocidades mayores.

Fenómenos meteorológicos: En las zonas rurales es frecuente encontrar condiciones meteorológicas adversas. Aunque tradicionalmente se suele decir que las lluvias influyen “de forma sensible” a partir de los 10GHz, cuando los enlaces son muy largos una pequeña atenuación en dB/Km acaba siendo importante. Los estudios que se han realizado no parecen conceder mucho peso a la atenuación de nubes y nieblas, pero todo depende de la distancia.

Polarización: El mejor comportamiento se da con polarización vertical, pero las condiciones atmosféricas y el terreno pueden producir una cierta despolarización, con lo que la recepción de la señal empeora y su atenuación aumenta.

Interferencias: En zonas urbanas se pueden ver afectados por este problema.

4.3.3 Enlaces para WI-FI

Debido a que el diseño de red se basa en tecnología WI-FI el estudio que se hace en esta sección está enfocado concretamente a esta tecnología, pues existen estudios más rigurosos para el estudio de radio enlaces sin especificar el tipo de tecnología que se está empleando.

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.

La mayor parte de la potencia de la señal de radio se perderá en el aire. Aún en el vacío, una onda de radio pierde energía, porque su energía se irradia en direcciones diferentes a la que puede capturar la antena receptora. Nótese que esto no tiene nada que ver con el aire, la niebla, la lluvia o cualquier otra cosa que puede adicionar pérdidas. La Pérdida en el Espacio libre Lp, mide la potencia que se pierde en el mismo, sin ninguna clase de obstáculo. La señal de radio se debilita en el aire debido a la expansión dentro de una superficie esférica. La Pérdida en el Espacio libre es proporcional al cuadrado de la distancia y también proporcional al cuadrado de la frecuencia.

Hay que señalar también que los canales disponibles en la banda 2.4 GHz y 5.8 GHz varían entre países; los canales comunes a todo el mundo son 11 canales, en saltos de 5MHz, para la banda 2.4 GHz, si bien cada canal tiene en realidad un ancho de banda de 22 MHz Se recomienda usar canales separados 25 MHz cuando se necesita que sean mutuamente no interferentes por trabajarse dentro de un mismo dominio de colisión, lo cual nos deja un total de tres canales usables en esas condiciones (Canales 1, 6 y 11). Mientras que en la banda 5.8 GHz existe un total de 8 canales no interferentes.

También para la pérdida en el camino está dada por la atenuación. Esto ocurre cuando parte de la potencia de la señal es absorbida al pasar a través de objetos sólidos como árboles, paredes, ventanas y pisos de edificios. La atenuación puede variar mucho dependiendo de la estructura del objeto que la señal está atravesando, y por lo tanto es muy difícil de cuantificar. La forma más conveniente de expresar está contribución a la pérdida total es agregando una “pérdida permitida” a la del espacio libre. Por ejemplo, un análisis estadístico demuestra que los árboles suman de 10 a 20dB de pérdida por cada uno que esté en el camino directo, mientras que las paredes contribuyen de 10 a 15dB dependiendo del tipo de construcción. A lo largo del trayecto del enlace, la potencia de RF (radio frecuencia) deja la antena transmisora y se dispersa. Una parte de la potencia de RF alcanza a la antena receptora directamente, mientras que otra rebota en la tierra. Parte de esa potencia de RF que rebota alcanza la antena receptora. Puesto la señal reflejada tiene un trayecto más largo, llega a la antena receptora más tarde que la señal directa. Este efecto es denominado multitrayecto, desvanecimiento o dispersión de la señal. En algunos casos las señales reflejadas se añaden y no causan problemas. Cuando se suman fuera de la fase, la señal recibida es prácticamente nula. En algunos casos, la señal en la antena receptora puede ser anulada por las señales reflejadas. Este fenómeno es conocido como *anulación*. Existe una técnica simple utilizada para tratar con el multitrayecto, llamada diversidad de antena. Consiste en agregar una segunda antena al radio. De hecho, el Multitrayecto es un fenómeno muy localizado. Si dos señales se suman fuera de fase en una locación, no lo harán en otra locación

en las cercanías. Si tenemos dos antenas, al menos una de ellas será capaz de recibir una señal utilizable, aún si la otra está recibiendo una señal distorsionada.

Cuando hacemos el cálculo de la potencia recibida por el receptor debemos tomar en cuenta los siguientes criterios: La potencia TX debe ser sumada sólo en uno de los lados del enlace. Si está utilizando diferentes radios en cada lado del enlace, debe calcular la pérdida para cada dirección (utilizando la potencia TX adecuada para cada cálculo). Para determinar si el enlace es viable PRX debe ser mayor a la sensibilidad del receptor.

Hay que recordar que el RSL (sensibilidad del receptor) 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 10-15dB 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. Una vez que se ha calculado el presupuesto del enlace en una dirección, debe hacer lo mismo en el otro sentido.

Como regla general una red inalámbrica a 2.4 GHz, pierde 100 dB en el 1er kilómetro y la señal es reducida a 6 dB cada vez que la distancia se duplica. Esto implica que un enlace de 2 km. tiene una pérdida de 106 dB y a 4km tiene un pérdida de 112 dB, etc.

Tabla 4. 2 Pérdidas en Espacio Abierto en dB para diferentes distancias y frecuencias

DISTANCIA	**915**	**2,4**	**5,8**

[Km]	MHz	GHz	GHz
1	92 dB	100 dB	108 dB
10	112 dB	120 dB	128 dB
100	132 dB	140 dB	148 dB

Estos valores son teóricos y pueden muy bien diferir de las mediciones tomadas, El término “espacio libre” no es siempre tan “libre”, y las pérdidas pueden ser muchas veces más grandes debido a las influencias del terreno y las condiciones climáticas. En particular, las reflexiones en cuerpos de agua o en objetos conductores pueden introducir pérdidas significativas.

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 de transmisión de un dispositivo dado debe ser especificada en los manuales provistos por el fabricante, pero algunas veces puede ser difícil de encontrar. Algunas veces los datos en línea pueden ayudarlo, una de ellas es la provista por Seattle *Wireless*[26].

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

[26] http://seatle*wireless*.net/hardwarecomparison.

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

Conocido como sensibilidad del receptor (RSL) y se expresa 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 ser 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.

4.4 DISEÑO DE LA RED WMNS

De los resultados obtenidos en el capítulo anterior, resume un conjunto de características sobre la situación actual de las comunicaciones en el cantón Manta correspondiente a la provincia de Manabí.

Nos centraremos exclusivamente en diseñar una red WMNs para dar servicios de internet a usuarios comprendidos en las zonas de cobertura.

Uno de los retos para el diseño será describir y justificar la arquitectura de la red. La idea principal es construir una red troncal en malla que constituye la columna vertebral de la red a ser diseñada y que garantice la conectividad en las zonas seleccionadas, el estándar empleado para los enlaces de la red troncal será IEEE 802.11. La figura 4.13 muestra un ejemplo de la arquitectura que implementaremos para el diseño de la red WMNs.

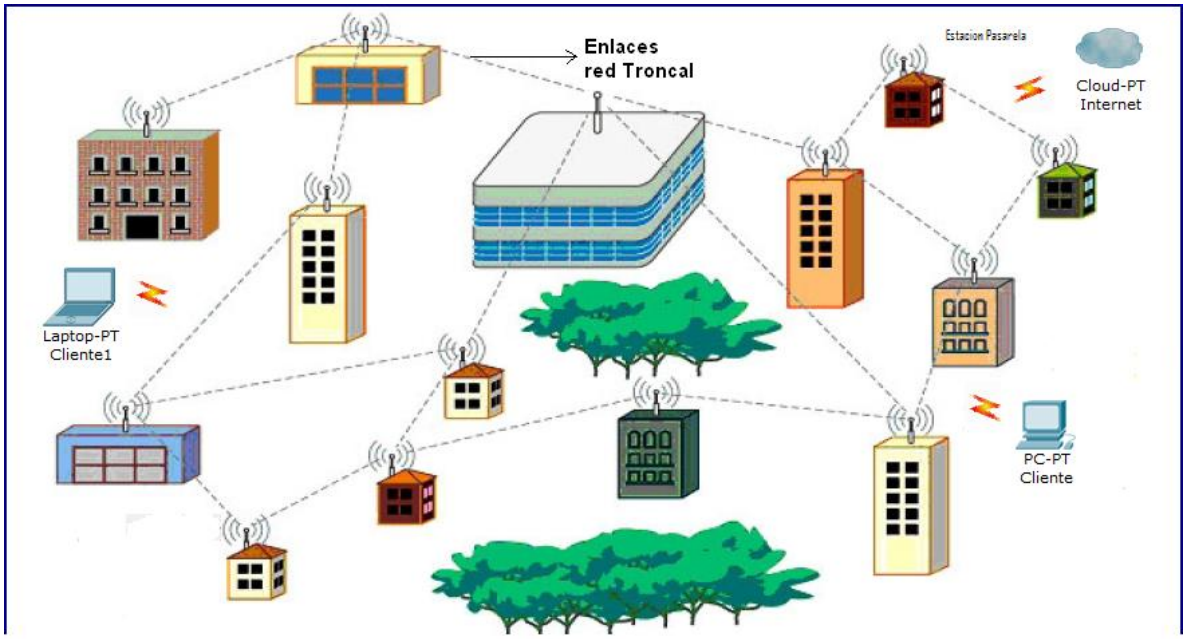


Figura 4. 14 Arquitectura de una red mesh[27]

Las Redes Inalámbricas *Mesh* (WMNs) consisten en dos tipos de nodos los repetidores y los clientes, donde los repetidores tienen movilidad mínima y forman la red transporte de la red WMNs. Estás redes pueden integrarse a otras como Internet, IEEE 802.11, IEEE 802.15, IEEE 802.16, etc. Los clientes pueden ser estáticos o móviles y pueden crear una red mallada entre ellos mismos o con los repetidores. Estás redes solucionan las limitaciones y mejoran el rendimiento de las redes ad hoc.

Gracias a la posibilidad de conectarse a distintos puntos de acceso en lugar de uno sólo, se aumenta el ancho de banda que puede tener cada cliente, también resulta mucho más estable, ya que puede seguir funcionando aunque caiga un nodo, en cambio en las redes habituales si cae un punto de acceso los usuarios de ese punto de acceso se quedan sin servicio.

27

http://images.google.com.ec/imgres?imgurl=http://www.rcsystems.com/images/firetide_diag.jpg&imgrefurl=http://www.rcsystems.com/integrated/wireless.php&usg=__kjvIKJ63CltHAE_8K2kHZnw9QYY=&h=503&w=577&sz=207&hl=es&start=5&itbs=1&tbnid=DJ8Hg7Lv2OFgEM:&tbnh=117&tbnw=134&prev=/images%3Fq%3Dmesh%2Bnetworks%26gbv%3D2%26hl%3Des%26sa%3DG

4.4.1 Requisistos para el diseño de la red WMNs

4.4.1.1 Requisitos Generales

Se identificaron los siguientes requisitos generales para la red WMNs:

- **Fácil despliegue**

  Los nodos de la red deben ser de fácil instalación y configuración.

- **Robustez**

  La red debe ser sólida y ofrecer suficiente redundancia de rutas, también debe ser de auto detección y corrección de problemas que existan dentro de la red

- **Los servicios de banda ancha**

Mensajes de texto y servicios de voz, imagen, vídeo con calidad de servicio

(QoS), por ejemplo priorización de tráfico deben aplicarse con el fin de ajustar la red a las necesidades de estos servicios.

- **El uso del protocolo estándar**

  Protocolos de comunicación estándar son preferibles con el fin de facilitar la interoperabilidad entre los dispositivos de comunicación.

- **Equipo asequible**

  Se prefiere el uso de la tecnología de fácil adquisición, a fin de construir una red WMNs a bajo precio.

4.4.1. 2 Requisitos Específicos

- **Requisitos de radio y topología de la red**

  Múltiples interfaces de radio: El uso de múltiples interfaces de radio y diferentes canales, podrá maximizar la capacidad de la red WMNs, con múltiples canales de radio disponibles, uno de ellos puede dedicarse a fines de *backhaul*[28], mientras que los otros canales disponibles pueden ser utilizadas para la comunicación entre los nodos de la red troncal y clientes. Además, lo que permite evitar el uso de una frecuencia con interferencia, está característica hace que el WMNs sea más robusta.

  Tecnología de interfaz de radio: La banda de 2,4 GHz y 5.8 GHz son útiles para conectar ordenadores portátiles a una red WMNs, la conectividad inalámbrica de los dispositivos de este tipo se basa actualmente en el estándar IEEE 802.11b/g.

- **Requisitos de funcionamiento**

  Latencia de extremo a extremo: El retardo de extremo a extremo debe mantenerse en valores aceptables, ya que afecta el rendimiento de las comunicaciones de datos, sobre todo en tiempo real de servicios tales como las comunicaciones de voz. Por ejemplo para los servicios de VoIP el retardo de extremo a extremo debe ser menor a 150 ms.

  El ancho de banda de extremo a extremo: Nos referimos al ancho de banda disponible en una ruta sin enlaces rotos, debe estar disponible para permitir el uso de varios servicios como voz, video etc. Para las comunicaciones de voz se recomienda un mínimo de 5 Kbps, mientras que para video de 200 Kbps.

[28] Sirve para interconectar redes entre si utilizando diferentes tipos de tecnologías alámbricas o inalámbricas

Retardos a los cambios de Ruta: La conectividad de nuevas rutas deberá reducirse al mínimo, maximizando así la disponibilidad del servicio.

- **Seguridad**

  Servicios de seguridad tales como la privacidad, la autenticación y la integridad, son generalmente deseados.

4.4.2 Descripción de la tecnología a emplearse en el diseño de la red WMNs

4.4.2.1 Arquitectura Mesh para redes WI-FI para larga distancia

Tradicionalmente la topología de red IEEE802.11 más usada ha sido en modo infraestructura. En ella todas las estaciones que forman parte de la red se comunican entre sí a través de un punto de acceso. De esta forma, las estaciones que se encuentran a demasiada distancia una de la otra pueden comunicarse a través de él. El punto de acceso puede además proporcionar acceso a redes exteriores. Sin embargo, la topología más básica de una red Wi-Fi es aquella en la que un conjunto de estaciones (mínimo dos), se conectan entre sí de forma directa. Dicha topología suele recibir el nombre de red Ad-Hoc. En este tipo de redes las estaciones se comunican de forma directa a través del medio inalámbrico sin que medie ninguna otra. Debido a las limitaciones inherentes en el alcance de las transmisiones puede que no todas las estaciones sean capaces de establecer comunicación entre sí, puesto que deberán estar dentro del rango de cobertura.

A partir del concepto de red Ad-Hoc en Wi-Fi se contempla el establecimiento de redes *Mesh*. En una red con topología *Mesh* una estación que desee transmitir a otra estación fuera de su alcance, comprobará en su tabla de

encaminamiento a qué estación dentro de su alcance debe transmitir la información. Dicha estación recibirá el paquete y lo reenviará siguiendo el mismo procedimiento y así sucesivamente hasta alcanzar la estación destino. Esto implica que todos los nodos de la red van a gestionar los paquetes a nivel IP. Esto introduce algo más de retardo, pero es, así como el ancho de banda, se puede gestionar de forma muy avanzada.

Las redes *Mesh* además de incrementar sustancialmente el área de cobertura que puede alcanzar una red (de límite indefinido si la distribución y densidad de la estación es adecuada) tienen la ventaja de ser tolerantes a fallos.

Al añadir un nuevo nodo se debe configurar correctamente sus interfaces inalámbricas, además, si uno o varios nodos tienen conexión a Internet, deben poder operar como pasarelas al exterior para los otros nodos, esto permite establecer una diferenciación funcional de tres tipos de nodos:

Estación pasarela: es una estación dotada de conectividad final a Internet, permitiendo al resto de estaciones de la red inalámbrica acceder a través de ella a los servicios de Internet.

Puede haber una o varias de estas estaciones pasarela en una red inalámbrica, pero lo más frecuente es encontrarnos con una. EL uso de más de una implica el uso de encaminamiento dinámico. Estás estaciones frecuentemente tendrán que desempeñar funciones como NAT (traducción de direcciones de red) o cortafuegos[29] (*Firewall*).

Repetidor: los distintos repetidores se unen formando la red troncal que se encarga de conmutar las comunicaciones con otras estaciones.

Estación cliente: Se encuentra en los puntos de servicio a usuarios. Suele tener conectado una computadora y un teléfono IP. Las estaciones cliente son

[29] Es un aplicación o herramienta que sirve como mecanismo de defensa para evitar cualquier tipo de acceso a un determinado sistema

aquellas que se benefician y hacen uso de todos los servicios que la red pone a su servicio. Estos servicios se basan principalmente en: correo electrónico, acceso a Internet, voz sobre IP y la transferencia de archivos entre todas las computadoras de la red.

4.4.3 Inspección de campo

La inspección tuvo como objetivo constatar la realidad física de las locaciones, y así realizar un diagrama final de la red de internet portátil.

En la inspección de campo se verificaron los lugares donde se ubicarán los nodos realmente, ya que en la Tabla 4.1 no se apreció la factibilidad de la ubicación de los nodos.

A continuación se muestra algunas locaciones finales de los nodos, las mismas se las eligió por su altura y cercanía con la ubicación de los nodos de la Tabla 4.1

Figura 4. 15Nodo Oro Verde

Figura 4. 16 Nodo Miramar II

Figura 4. 17 Nodo Global Dental

Figura 4. 18 Nodo Howard Johnson

4.4.4 Diagrama de red

De acuerdo a los resultados obtenidos en las pruebas de campo se realizo el diagrama red que se muestra en la Figura 4.19 y se tomaron las siguientes consideraciones:

- Locación de nodos
- Rehuso de frecuencias no sobrelapadas
- Pruebas de conectividad.
- Limitaciones en la cobertura

Figura 4. 19 Diagrama de Red

4.4.4.1 Locación de nodos

Los nombres y la ubicación de los nodos se muestran en la tabla 4.2.

Tabla 4. 3 Locación de nodos

Simbologia	Nombre	Dirección	Altura (m)	Coordenadas
AP 1	Cabañas Balandra	Calle 20 y Av. 7	16,8	0°56´34.99´´S
AP 2	Oro Verde	Calle 23 y Av. Malecón	20	0°59´29.76´´S
AP 3	Miramar 2	Calle 24 y Av. Malecón	23	0°56´30.70´´S
AP 4	Manicentro	Calle 23 y Av. 14	32	0°56´36.76´´S
AP 5	Aneta	Calle 22 y Av 25	20	0°56´43.08´´S
AP 6	Globaldental	Calle Balda y Via Circunvalación	17	0°56´34.94´´S
AP 7	Calisto	Calle 30 y Av Umiña	19,6	0°56´39.74´´S
AP 8	Circunvalación 1	Via circunvalación y Av 29	18,7	0°56´43.98´´S
AP 9	Boyaca	Calle 30 y Pasaje A	20,3	0°56´48.99´´S
AP 10	Escuela Pesca	Av Umiña y Calle 36	31,5	0°56´39.94´´S
AP 11	Martinica	Via a Barbasquillo Km 1.2	15,6	0°56´43.60´´S
AP 12	Ciudadela Universitaria 2	Ciudadela Universitaria Calle A	20	0°56´50.90´´S
AP 13	Circunvalación 2	Via Circunvalación Km1	24	0°57´1.66´´S
AP 14	Ciudadela Universitaria 1	Ciudadela Universitaria Calle B	20	0°56´55.64´´S
AP 15	Howard Johnson	Via a Barbasquillo Km 1.5	30	0°56´44.51´´S
AP 16	Ciudadela Universitaria 3	Ciudadela Universitaria Calle C	20	0°56´57.72´´S
AP 17	Ciudadela Universitaria 4	Ciudadela Universitaria Calle E	20	0°57´5.5´´S
AP 18	ULEAM 1	Campus Universitario 1	30	0°57´12.20´´S
AP 19	ULEAM 2	Campus Universitario 2	28	0°57´15.39´´S
AP 20	ULEAM 3	Campus Universitario 3	29	0°57´21.21´´S

La ubicación de los equipos está dispuesta para un máximo de rendimiento en cobertura y calidad de servicio. Las locaciones cuentan con la suficiente altura para asegurar la línea de vista entre los APs y así optimizar la rapidez en el canal de *backhaul*

4.4.4.2 Rehuso de frecuencia no sobrelapadas

Para el diseño de la red se tuvo como problema importante el sobrelapamiento de frecuencias para el estándar 802.11g, como se mencionó anteriormente existen tres canales no interferentes (1, 6, 11), se solucionó este problema en el diseño usando canales diferentes en los nodos adyacentes y rehusando los canales en nodos no adyacentes como se muestra en el Figura 4.20.

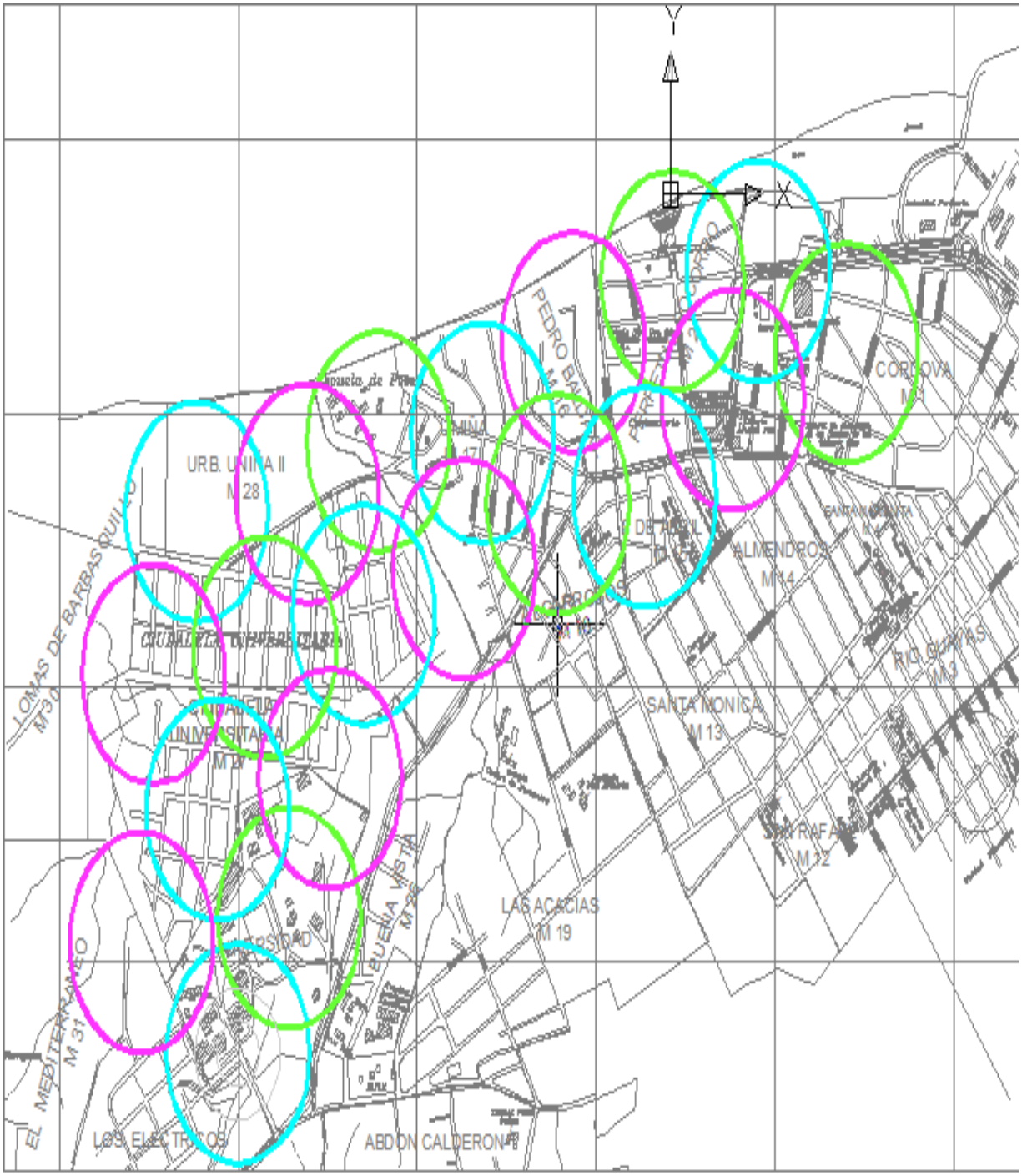


Figura 4. 20 Rehuso de frecuencias

4.4.4.3 Pruebas de conectividad.

Estas pruebas tienes como objetivo verificar la conectividad de un usuario alrededor de la red de internet para verificar la portabilidad del servicio que se pretende brindar.

En estas pruebas se instalaron dos equipos AP 5131 con sus respectivas antenas, para las pruebas se utilizó una laptop marca HP Pavilion.

Se verificó en tres nodos distintos, de dos en dos mientras que la laptop se trasladaba del área de cobertura de uno al otro comprobando que no perdía su conexión.

En las siguientes figuras se muestra el área de cobertura de los 2 equipos.

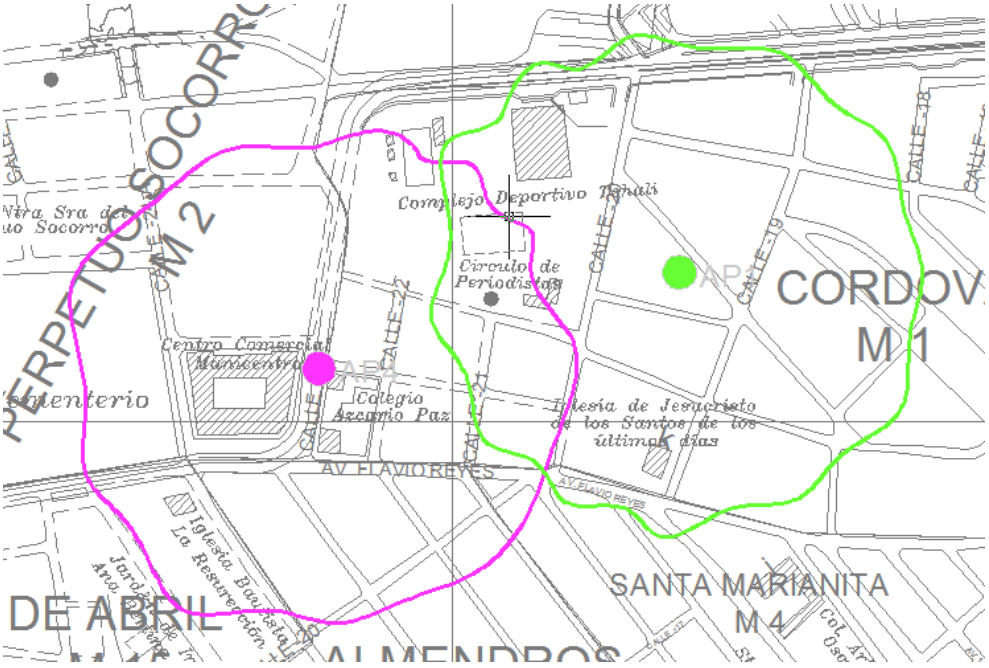


Figura 4. 21 Sobrelapamiento de dos nodos

Se realizaron pruebas de conectividad para comprobar el desempeño de la red que se las hicieron mediante comandos ping y tracert para determinar el número de paquetes perdidos en la red.

En la Figura 4.22 se ve el desempeño de la red.

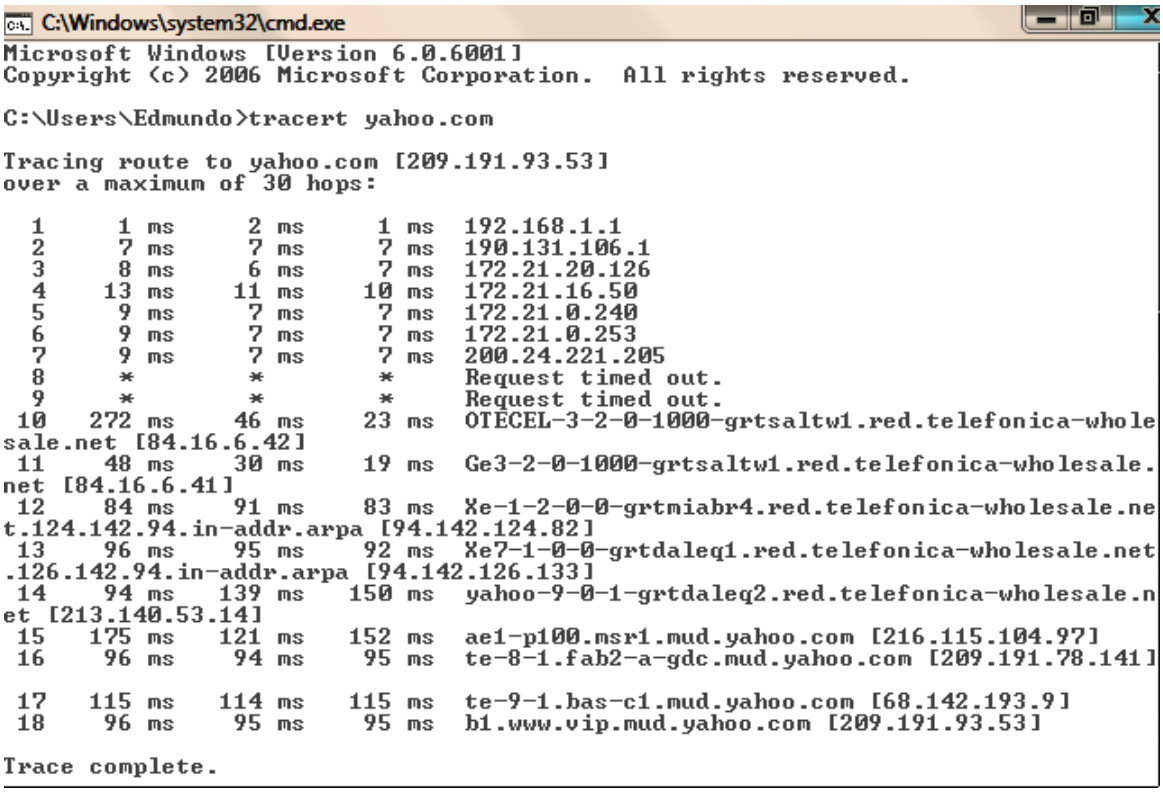


Figura 4. 22Desempeño de la red

4.4.4.4 Limitaciones en la cobertura

El diseño de la red cubre las aéreas seleccionadas, sin embargo, existen lugares donde no existe cobertura. En la Figura 4.21 se muestra el mapa de cobertura en donde se puede ofrecer este servicio.

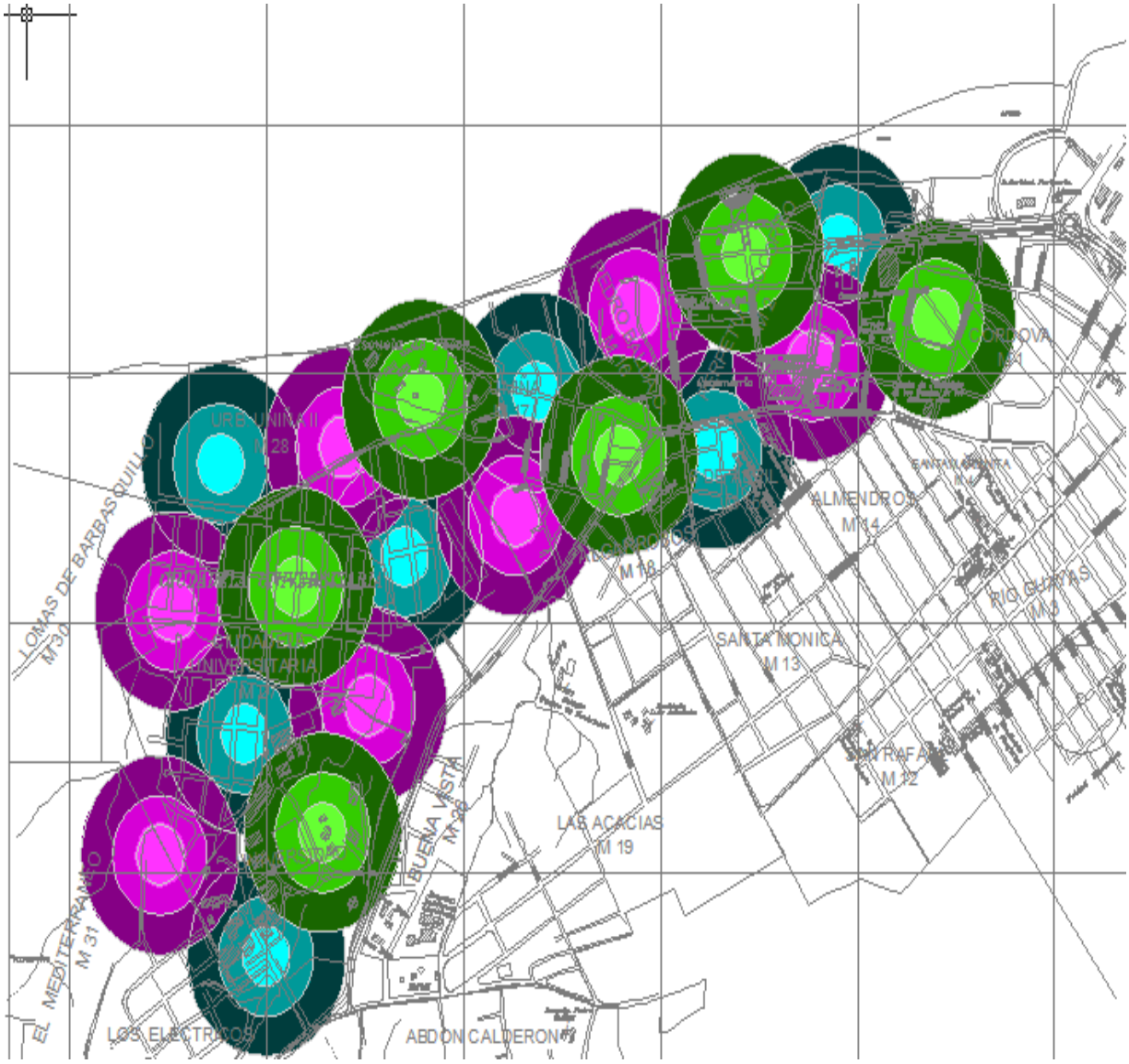


Figura 4. 23 Cobertura de la red de internet portátil

4.5 Requerimientos de ancho de banda de la red WMNs

4.5.1 Requerimientos de tráfico para cada aplicación

Para realizar la estimación de tráfico que cursará para cada aplicación dentro de la red, se realizará un estudio estadístico del uso de cada aplicación, debido a que no existen datos anteriores, ya que muchos de los establecimientos no cuentan con un centro de cómputo con acceso a Internet.

4.5.1.1 Correo electrónico

La información que se intercambia por el correo electrónico, corresponde a información de investigación o trabajos de las diferentes materias que tiene cada estudiante en su centro de educación, información personal, debido a que un documento de solo texto es de tamaño pequeño, aproximadamente 19 Kbyte, en tanto que un documento gráfico posee un mayor tamaño, de acuerdo al formato de la imagen que se desee transmitir teniendo un promedio para este de 400 Kbyte, se considera que el tamaño promedio de los archivos que se envían es de 500 Kbyte. Para el acceso al correo electrónico, se ha estimado que cada usuario revisa un promedio de dos correos en una hora. Tenemos así que el tráfico que maneja un correo electrónico para un usuario es:

Ecuación 4. 3

$$V_{correo} = \frac{500Kbyte}{correo} * \frac{8bits}{1byte} * \frac{2correos}{1\ hora} * \frac{1hora}{3600s}$$

$$V_{correo} = 2.22kbps$$

4.5.1.2 Acceso a Internet

Para utilizar este servicio se ha considerado que una página web tiene un peso aproximado de 25 Kbyte, incluyendo texto e imágenes medianas, además se ha estimado que un usuario accederá a 1 página Web en 30 segundos, debido a que se brindará Internet de banda ancha. Considerando esto se tiene.

Ecuación 4. 4

$$V_{INTERNET} = \frac{25Kbytes}{pagina} * \frac{8\ bits}{1\ byte} * \frac{1\ pagina}{30\ seg}$$

$$V_{INTERNET} = 6.66\ Kbps$$

4.5.1.3 Voz por Internet

Para transportar la voz por Internet (VPI), se requiere un ancho de banda de 13 Kbps[30] por cada usuario potencial del servicio.

4.5.1.4 Vídeo sobre IP

Para utilizar los servicios que proporciona el Vídeo sobre IP, como el Vídeo *Broadcast* se requiere un ancho de banda de 128 Kbps (VoIP).

4.5.1.5 Estimación total de la capacidad del tráfico

La capacidad total se obtiene de las sumas parciales del ancho de banda para cada aplicación como son: el servicio de correo electrónico, el tráfico generado por el servicio de voz por Internet (VoIP) y Vídeo sobre IP (VPI) y la capacidad para ofrecer servicios adicionales.

Ecuación 4. 5

$$C_{total} = C_{correo} + C_{internet} + C_{VPI} + C_{VoIP} + C_{adicional}$$

Donde:

C=capacidad

[30] Resultados del códec G.729

Para poder calcular la capacidad con esta ecuación es necesario hacer un análisis estadístico de cada aplicación que utilizarán los potenciales usuarios que estén conectados a la red.

La empresa COMPUATEL S.A tiene que por requisito previo para la apertura de un nodo de estas características: un mínimo de 10 clientes, como se puede apreciar en nuestro diseño del diagrama de red en la Anexo 3 posee 20 nodos por lo cual empezaría esta red con un total de 400 personas como mínimo por lo cual para asegurar un funcionamiento garantizado de la red internet portátil se necesita una capacidad de ancho de banda que se muestra a continuación:

Ecuación 4. 6

$$C_{total} = C_{correo} + C_{internet} + C_{VPI} + C_{VoIP} + C_{adicional}$$

$$C_{Total\,Usuario} = 2.22 + 6.66 + 26 + 137 = 171.88\ Kbps$$

Se necesita de 171.88 Kbps por usuario para garantizar el servicio de internet, vale la pena resaltar que este valor por usuario es el máximo que utilizaría un usuario al realizar todas las aplicaciones antes mencionadas.
Como nuestra solución de servicio de internet inalámbrico tendría en un inicio de 200 personas, la capacidad inicial para mantener un servicio de internet portátil garantizado es:

$$C_{total} = C_{total\,usuario} * Numero_{\ usuarios}$$
$$C_{total} = 17.188 * 400 = 68752\ kbps$$

La empresa COMPUATEL S.A como política interna garantiza a sus usuarios una compartición de 6 a 1 en ancho de banda, es decir, que la capacidad inicial total es reducida a 11.458 Mbps. De acuerdo con este resultado nuestro ISP (*Internet Service Provider*) debe ofrecer este ancho de banda para nuestra red

4.5.1.6 Administración de ancho banda de la red

Los planes ofrecidos por la empresa COMPUATEL S.A para la red de internet portátil son los siguientes, 128,256 y 512 kbps.

Para la asignación de los planes a los clientes, el AP 5131(Figura 4.24) puede crear una WLAN para cada plan independientemente una de la otra como se explica anteriormente. La asignación de ancho banda en la WLAN se configura de la siguiente manera:

- En *NETWORK CONFIGURATION -> Wireless* del menú del AP -5131. Se elige la opción *Bandwidht Management*

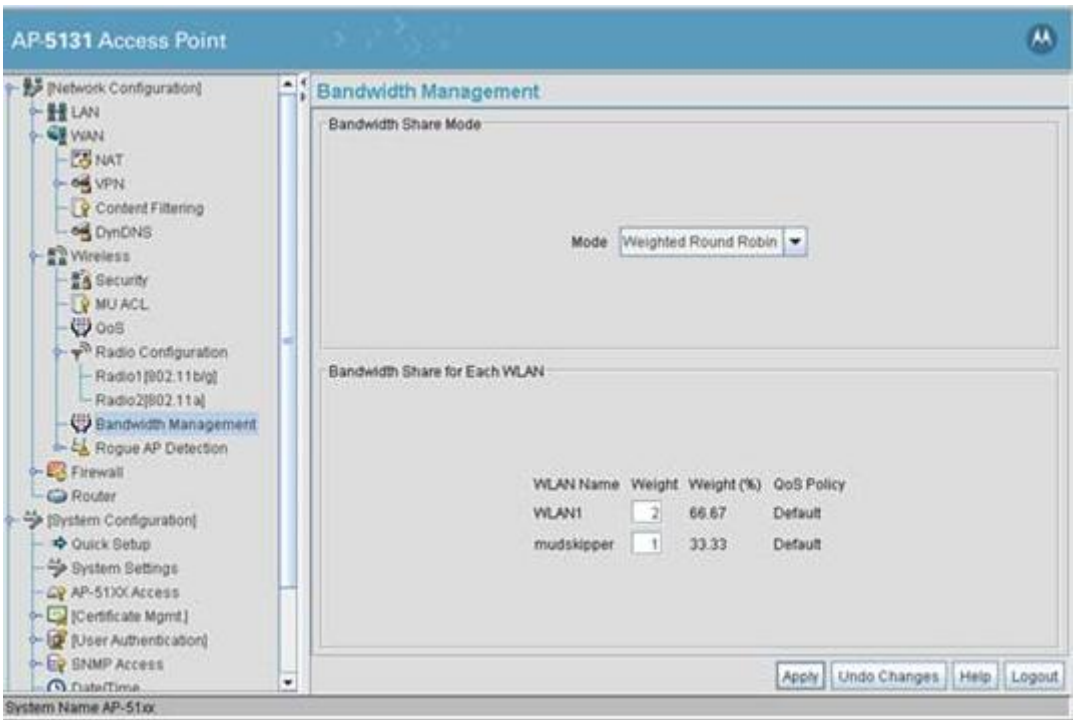


Figura 4. 24Administración de ancho de banda

- Se asigna el porcentaje de ancho de banda para cada WLAN, dependiendo del plan que se pretenda asignar.
- Se guarda los cambios hechos en la configuración del equipo.

4.6 AP BASE o Estación Pasarela

COMPUATEL S.A se encargará de proporcionar el enlace de internet por medio de fibra, así como los equipos frontera, el AP pasarela estará enlazado al equipo frontera por medio de cable UTP.

En la red puede haber una o varias estas estaciones pasarelas. La estación tiene que desempeñar funciones como NAT (traducción de direcciones de red) o cortafuegos.

En un inicio la red contará con un solo AP BASE que se encuentra ubicado en la Nodo Escuela de Pesca (AP10), el motivo de la elección como estación pasarela es por su ubicación central dentro de la región de interés, para mantener tiempos de respuesta simétricos a los extremos de la red.

Al extenderse la red se puede ubicar una segunda estación pasarela ubicada en el mismo nodo AP10 para evitar los costos de instalación y paso de fibra, brindando redundancia y balanceo de cargas. Para el balanceo de cargas se puede utilizar la sectorización, es decir, direccionar clientes o grupos de clientes a cada AP BASE y de esta manera mejorar el desempeño de la red.

CAPITULO 5

ANÁLISIS DE COSTOS

5.1 COSTOS DE EQUIPAMIENTO E INFRAESTRUCTURA

Los estudios previos de diseño dan una referencia de los costos para la infraestructura de la red *mesh* en la cuidad de Manta. De acuerdo al diagrama de red Anexo 3 existen una estación base (Estación pasarela) y 7 repetidores para se hace necesita una estimación de costos del proyecto dividiéndolos en varios grupos de la siguiente forma

- Costos de equipos
- Costo de infraestructura
- Costos totales estimados para la implementación de la red *mesh*
- Costos de Mantenimiento

5.1.1 Costos de equipos

La red propuesta cuenta con los siguientes equipos:

Tabla 5. 1 Costos Totales de Equipos[31]

Equipo	P unitario [$]	Cantidad	Subtotal
Ap-5131	600	20	12000
Antena Sectorial	180	40	7200
Antena Omnidireccional	120	40	4800
Amplificador de potencia	35,5	80	2840
Protector de linea	20	1	20
		Total [$]	26860

Antena Sectorial: 120 grados, 5.8 GHz y 20 dBi

Antena Omnidireccional: 2.4 GHz y 15 dBi

Amplificador de potencia: 20 dB.

5.1.2 Costos de infraestructura

Dentro de la infraestructura se consideran los costos de conexiones, mástil de 3 metros de piso, ups y cajas herméticas.

Equipo	Descripcion [$]	P unitario	Cantidad	Subtotal
Mastil 3m	Mástil para sujeción de antenas	12	40	480
UPS	Equipo de suministro de enegia de	1200	1	1200

[31] Costos de los equipos proporcionados por COMPUATEL.SA

	emergencia			
Caja hermetica	Protección de equipo contra el ambiente	15	20	300
Abrazaderas	Sujeción para el mastil y antena	3,3	160	528
Protector de línea		20	20	400
			Total [$]	2908

Tabla 5. 2 Costos totales de infraestructura

5.1.3 Costos totales de estimados para la implementación de la red *mesh*

Los costos de los equipos de comunicación de datos así como la infraestructura necesaria para los mismos están descritos en la tablas 5.1 y 5.2.

El costo total para la creación de la red mesh es :

Costos de equipos	26860
Costos de infraestructura	2908
Total USD	29768

5.1.4 Costos de operación y mantenimiento

Los costos de operación y mantenimiento son los que se pagarán durante todo el tiempo de vida del sistema. El sistema parte desde el ISP de la empresa COMPUATEL.SA, que es quien dotará de conectividad final a Internet.

Estos costos implican

- Pago anual del servicio de Internet.
- Alquiler por el espacio físico de equipos
- Creación de la red privada (una vez cada 5 años)

Tabla 5. 3 Tarifas de internet

Creación de la red privada	500
Pago internet anual	61873,2
Alquiler espacio físico primer año	24000
	$86373,2

5.2 Costos de Licenciamiento y software de administración.

La empresa COMPUATEL. SA usa como sistema operativo para sus redes el LINUX RED HAT 9.0 por lo cual los costos de licencias por este software son nulos, este sistema operativo puede ser descargado gratuitamente desde el Internet.

El costo para la creación de una red privada en Ecuador es de $500 dólares americanos.

5.3 Financiamiento

El costo del proyecto es asumido en su totalidad por la empresa COMPUATEL.S.A como una oportunidad comercial para entrar en el mercado de la ciudad de Manta.

5.4 Tarifación

El sistema de tarifación empleado por una empresa de servicios constituye uno de los aspectos más importantes a considerar, ya que del mismo dependen los ingresos que se van a obtener y estimar la rentabilidad en el tiempo.

Entre los esquemas de tarifación más utilizados por los proveedores de servicios de Internet encontramos: tarifación basada en el acceso, basada en el tiempo y basada en el volumen.

La tarifación basada en el acceso utiliza como parámetro de cobro el ancho de banda contratado, resultando para el cliente el pago de una tarifa plana por el servicio independiente del tiempo de conexión y volumen de datos transferidos.

La tarifación basada en el tiempo utiliza la duración del acceso al servicio como medida de cobro al cliente. Es utilizada principalmente en esquemas Dial up.

Una tarifación basada en el volumen realiza la facturación tomando en cuenta el volumen de tráfico cursado entre el proveedor de servicio de Internet y el cliente.

Para calcular el costo de la tarifa para un usuario del centro de provisión de internet se utilizará el esquema de tarifa plana por ancho de banda contratado, ya que presenta las siguientes ventajas para el centro y para el cliente:

- Permite tener una estimación exacta de los ingresos mensuales por el servicio.

- No se requiere una compleja estructura en el centro para medir el uso del servicio.

- El cliente conoce la tarifa a pagar independiente del uso del servicio.

Desde que nació el proyecto, el principal objetivo fue dar servicio de comunicaciones a las áreas seleccionadas por lo que se espera obtener rentabilidad.

Se deben generar ingresos económicos que cubran los gastos que generan la red por lo cual es necesario tener una idea clara de cuáles son los gastos mensuales que genera la red por este concepto.

Tabla 5. 4 Costos de mantenimiento mensual y operacion de la red[32]

ITEM	SUBTOTAL
Pago de internet Mensual	5156.1
Pago de Alquiler por espacio Físico	2000
TOTAL	7156.1

[32] Datos proporcionados por COMPUATEL S.A

El costo total de mantenimiento y operación de la red necesariamente tendrá que ser cubierto por los usuarios de la red, Entonces el costo mensual por usuario sin ganancia que generaría COMPUATEL S.A es:

Ecuación 5. 1

$$T = \frac{Gastos\ totales\ de\ mantenimiento\ y\ operacion\ de\ la\ red}{Numero\ de\ usuarios\ de\ la\ red}$$

$$T = \frac{8874.8}{400} = \$17.89$$

En donde T es la tarifa mensual por usuario sin ganancia.

La tarifa final dada por el departamento financiero de la empresa COMPUATEL S.A para brindar este servicio de internet inalámbrico es la de $22.2 que es un incremento del 24.1 %[33].

Sin embargo se específica una tabla con el costo para los enlaces a internet:

Tabla 5. 5 Tarifa mensual por enlace

Tarifa mensual por enlace	
Enlace de 128 kbps	16,53
Enlace de 256 kbps	33,1
Enlace de 512 kbps	66,2

Se debe tener en cuenta que a estos costos se le debe agregar el 12% del I.V.A

A continuación se muestra una tabla en donde se indica el Flujo de fondos del proyecto.

Tabla 5. 6 Flujo de fondos

[33] Tarifa que utiliza COMPUATEL S.A

Flujo de fondos							
Valor	**Item**	**Año 0**	**Año 1**	**Año 2**	**Año3**	Año 4	Año 5
(+)	Ingresos($)		106560	106560	106560	106560	106560
(-)	Costos($)		85873,2	85873,2	85873,2	85873,2	85873,2
	Utilidad Neta($)		20686,8	20686,8	20686,8	20686,8	20686,8
(-)	Costos de inversión ($)	30268					
(-)	Participación a trabajadores (15%de la utilidad)			1665,84	3103,02	3103,02	3103,02
	Flujo de fondos($)		-9581,2	9439,76	17583,78	17583,78	17583,78

Como se puede observar en la tabla luego de la inversión en el año 0 de 30268, a los dos años se pudo recuperar la inversión y empezar a obtener ganancias.

La evaluación del proyecto se la realizará a través de indicadores de rentabilidad para poder tener una base para la toma de decisiones y anticipar al futuro posibles desviaciones o problemas a largo plazo. Los indicadores que se utilizarán para medir la solvencia y sostenibilidad del proyecto son los siguientes:

- Valor Presente Neto
- Tasa Interna de Retorno

La base de tiempo que se tomará en cuenta para el cálculo de estos indicadores es de 5 años.

El Valor Presente Neto (VPN) es muy utilizado por dos razones, la primera porque es de fácil aplicación y la segunda porque todos los ingresos y egresos futuros se transforman a pesos actuales para poder determinar en valores actuales los ingresos y egresos del proyecto.

Si:

VAN > 0, el proyecto es aceptable ya que representa ganancias.

VAN = 0, el proyecto es indiferente.

VAN < 0, el proyecto representa pérdidas frente a un interés de oportunidad o alternativa de inversión.

El VPN es calculado con la fórmula:

Ecuación 5. 2 VPN

$$VPN = \sum_{t=0}^{n} \frac{Flujo\ de\ fondos}{(1+i)^t}$$

FFNIt = Flujo de fondos neto incremental en ese período.
i = tasa de interés de oportunidad. (5.24)[34]
t = período.

VAN=VPN- Inversión

VAN = -9581.2 / (1 + 0.0524)^1 + 9439.76 / (1 + 0.0524)^2 + 17583.79 / (1 + 0.0524)^3 +17583.79 / (1 + 0.0524)^4 +17583.79 / (1 + 0.0524)^5 – 29768

VAN=$12692,5419

El VAN es un indicador financiero que mide los flujos de los futuros ingresos y egresos que tendrá un proyecto, para determinar, si luego de descontar la inversión inicial, nos quedaría alguna ganancia. Si el resultado es positivo, el proyecto es viable.

[34] Fuente http://www.portal.bce.fin.ec/ebi/servlet/fin.bce.ebi.ClsIngresoCalculadora

Como se ve en este caso el resultado es positivo por lo que el proyecto es rentable.

La TIR (Tasa Interna de Retorno) es aquella tasa que hace que el valor actual neto sea igual a cero.

Cuando la TIR es mayor que la tasa de interés, el rendimiento que obtendría el inversionista realizando la inversión es mayor que el que obtendría en la mejor inversión alternativa, por lo tanto, conviene realizar la inversión.

Si la TIR es menor que la tasa de interés, el proyecto debe rechazarse.

Cuando la TIR es igual a la tasa de interés, el inversionista es indiferente entre realizar la inversión o no.

TIR > i => realizar el proyecto

TIR < i => no realizar el proyecto

TIR = i => el inversionista es indiferente entre realizar el proyecto o no.

En este caso del proyecto el TIR es del 35% al ser mayor la empresa COMPUATEL debe realizar el proyecto.

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- El proyecto tiene como objetivo principal brindar servicios de internet portátil en la ciudad de Manta, el diseño de la red se enfoco en la zona de mayor demanda, pudiendo extenderse conforme las necesidades de la población.

- Las redes *mesh* son una solución de bajo costo y escalabilidad prometedora permitiendo a la empresa incursionar en el mercado de internet portátil sin la necesidad de invertir altos capitales en infraestructura.

- El área de cobertura por estación fue limitado a 200m (radio) para garantizar la calidad del servicio en cualquier punto de la red.

- Una de las características más importantes de las redes *mesh* es su gran tolerancia a fallos.

- Un factor importante del proyecto es atender las necesidades del sector que se pretende cubrir, la solución a este problema es tener un contacto directo con las personas afectadas y documentando sus deseos en el servicio de internet.

- El número máximo de usuario por nodo para el AP-5131 es de 127 teniendo en cuenta que a mayor número de usuarios menor desempeño de la red.

- El diseño de la red cumple con las expectativas de cobertura, sin embargo, existen lugares donde no existe cobertura.

- Por las características de la red es posible expandir su área de cobertura de ser necesario gracias a su escalabilidad y tolerancia a fallos.

- Aunque la movilidad de los nodos que forman la red troncal es posible, en nuestro diseño es nulo para mejorar el rendimiento a largas distancias.

- La calidad de servicio en la red está garantizada ya que los equipos utilizados pueden diferenciar los diferentes flujos de tráfico dando prioridad a la voz y video sobre los datos.

6.2 RECOMENDACIONES

- Se recomienda utilizar amplificadores de potencia para mejorar el área de cobertura ya que por ser un proyecto orientado al sector urbano existen elementos atenuantes de la señal.

- Se deben implementar políticas de seguridad, debido a que la tecnología inalámbrica es de fácil acceso de usuarios no deseados.

- Para el equipo *mesh* AP-5131 es recomendable usar un radio exclusivo para la red de *backhaul* de preferencia la banda de 5GHz por la posibilidad de mayores velocidades y la interferencia de otros dispositivos es menor que la banda de 2.46GHz

.

6.3 REFEENCIAS BIBLIOGRAFICAS

LIBROS:

- Atul Adya, Paramvir Bahl, Jitendra Padhye, Alec Wolman, Lidong Zhou, “A Multi-RadioUnification Protocol forIEEE 802.11 *Wireless* Networks”, Julio 2003.
- DIANA MARGARITA ACUÑA MARTINEZ Y RAFAEL JULIO RONCALLO KELSEY,”REDES INALAMBRICAS ENMALLADAS METROPOLITANAS” Colombia 2007.
- MOTOROLA, “AP-51xx Access Point Product Reference Guide”, Abril 2007

TESIS:

- JUAN PABLO QUINAPALLO MORALES, “Diseño de una red inalámbrica para interconectar la matriz de la cadena farmacias Pharmacy´s con sus diferentes sucursales ubicadas en la ciudad de Quito”, Agosto 2006.

- CHILUISA PILA MILTON JAVIER Y ULCUANGO QUIMBIAMBA JORGE GEOVANNY, “Diseño de una red inalámbrica para las parroquias rurales del cantón Latacunga”, Quito Marzo 2008

PAGINAS WEB:

- http://motorola.motowi4solutions.com/support/mesh/docs/duo/WMS_1_0_User_Guide.pdf
- www.motorola.com/emea/mesh
- http://www.wi-fi.org/
- http://www.ieee802.org/11/
- http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/9907/4395224/04395237.pdf?arnumber=4395237
- http://www.huawei.com/es/catalog.do?id=562
- www.locustworld.com
- www.meshnetworks.com
- www.olsr.org

- www.troposnetworks.com
- www.ubnt.com/downloads/ls5_datasheet.pdf
- www.*wireless*summit.org
- www.wilac.net/tricalcar