ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS, DISEÑO Y PROTOTIPO DE UNA RED INALÁMBRICA DE ACCESO A INTERNET

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

EDISON FERNANDO CHILIQUINGA LLIVE

DIRECTOR: ENRIQUE MAFLA, PHD

Quito, noviembre del 2007

DECLARACIÓN

Yo, Edison Fernando Chiliquinga Llive, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Edison Fernando Chiliquinga Llive

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Fernando Chiliquinga Llive, bajo mi supervisión.

_____

Dr. Enrique Mafla

DIRECTOR DEL PROYECTO

AGRADECIMIENTO

A la Escuela Politécnica Nacional y los diferentes docentes que fueron quienes impartieron su conocimiento y experiencia.

Al Dr. Enrique Mafla quien con su acertada dirección ha hecho posible el desarrollo de este proyecto.

Gracias a la vida por haberme puesto un reto grande de superar, lo cual hace que disfrute con mayor alegría la meta alcanzada.

Fernando

DEDICATORIA

A mis padres, Luis Octavio y María Enriqueta, por haber entregado todo su esfuerzo y dedicación para cultivar mis valores y hacer de mi un hombre de bien, por entregarme todo su cariño y comprensión en los momentos más difíciles de mi vida.

A mis hermanos, Gerardo, Washington, Silvia y William con quienes he compartido mi vida y siempre apoyaron todas mis metas y sueños.

A Mónica, quien con su amor y comprensión ha cambiado mi vida.

RESUMEN

Este proyecto comprende el análisis, diseño y prototipo de una red inalámbrica de acceso a Internet. Se desarrolla utilizando la tecnología 802.11, analiza la situación actual de Gigowireless mediante la arquitectura CISCO SAFE, planteando un esquema modular para la agrupación de los dispositivos actuales de la empresa y su posterior análisis.

El diseño de la red se ha proyectado para brindar servicio de Internet a los moradores de la urbanización “El Condado”, para lo cual se ha tomado datos que permitan el dimensionamiento de la red, entre ellos se ha recolectado información sobre: niveles de señal, canales usados, redes cercanas, modo de trabajo y seguridad implementada. Se utiliza software de apoyo como NetStumbler, Ozi Explorer y Google Earth. Para la simulación de las redes se trabajó con Radio Mobile para enlaces punto a punto y Ekahau para la red de acceso inalámbrica. Adicionalmente se utilizo los modelos propuestos por “Okumura-Hata” para realizar la predicción de cobertura de la red de acceso.

El análisis de costos toma en cuenta precios de equipos y tarifas del servicio existentes en el mercado y de este modo generar una propuesta de los diferentes planes de servicios disponibles para los usuarios.

El análisis legal se basa en el marco referencial de las leyes y normas de telecomunicaciones vigentes en el país. Finalmente se implementa un prototipo y se efectúan pruebas de funcionalidad, confiabilidad y rendimiento.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1
INTRODUCCIÓN

En este capítulo se presenta la definición del problema, el objetivo general y los objetivos específicos, alcance, metodología a seguir y el marco teórico que define la tecnología a utilizar. Este proyecto contempla el análisis, diseño e implementación de un prototipo para brindar Internet mediante una red inalámbrica. Los datos que se tomarán para el desarrollo del proyecto son reales y de uso de la empresa Gigowireless. Esta se localiza en la ciudad de Quito, su área de cobertura se limita a sectores puntuales del norte de la ciudad. El proyecto será aplicable para la urbanización “El Condado”, los datos recopilados para el diseño de la red inalámbrica serán tomados del sector.

1.1 PARÁMETROS DEL PROYECTO

1.1.1 DEFINICIÓN DEL PROBLEMA

Actualmente Gigowireless cuenta con una infraestructura tecnológica implementada para la transmisión de datos hacia Internet. Además tiene varias redes inalámbricas que están implementadas sin ningún estudio técnico que avalice el correcto funcionamiento de la red de acceso, no existe estudios de cobertura e interferencias, características de equipos a usar, niveles de seguridad, métodos de acceso, capacidad de la red. Actualmente la empresa utiliza 802.11b e implementa encriptación WEP como método de seguridad para la red inalámbrica. Las redes inalámbricas al usar un medio de transmisión no seguro pone en riesgo la privacidad de la comunicación debido a que puede existir intrusiones en la red, por esto al momento de diseñar e implementar una red es necesario conocer diferentes

protocolos y mecanismos de seguridad existentes con el fin de evitar afectar el rendimiento, seguridad y disponibilidad en la red.

Los niveles de seguridad que se necesitan en las redes de acceso de los proveedores de Internet son diferentes a las utilizadas en redes privadas, esto se debe a que tienen mayor libertad para filtrado de tráfico y control de aplicaciones; en contraste con una red pública, legalmente no se debe realizar ningún bloqueo de tráfico, ya que está prohibido por la Ley de Telecomunicaciones. Por este motivo se debe hacer un estudio y análisis de requerimientos de los usuarios finales antes de poner en marcha cualquier implementación.

1.1.2 OBJETIVO GENERAL

El objetivo del proyecto consiste en realizar el análisis, diseño e implementación del prototipo de una red inalámbrica de acceso a Internet, tomando en cuenta requerimientos de funcionalidad, rendimiento, disponibilidad y seguridad para un ISP.

1.1.3 OBJETIVOS ESPECÍFICOS.

- Analizar los requerimientos de funcionalidad, rendimiento, disponibilidad y seguridad tanto de los potenciales usuarios del servicio como de los dueños del negocio (ISP).

- Diseñar e implementar el prototipo de una red inalámbrica de acceso a Internet que satisfaga los requerimientos de funcionalidad, rendimiento y seguridad tanto de los usuarios como de Gigowireless, utilizando 802.11b u 802.11g.

- Considerar normas y tecnologías nuevas tales como IEEE 802.1X y Captive Portal en el diseño de la red.

- Probar la funcionalidad, rendimiento, disponibilidad y seguridad del prototipo implementado.

- Analizar aspectos legales para la implementación de una red inalámbrica.

- Realizar el análisis costo-beneficio del proyecto.

1.1.4 METODOLOGÍA

La metodología para el desarrollo del proyecto consta de cinco fases: definición de marco teórico, análisis de la situación actual, análisis de requerimientos, diseño, implementación de prototipo y pruebas.

1.1.4.1 Fase I: Marco Teórico

En esta fase se definirá la tecnología con la que se va ha desarrollar el proyecto, que permitirá generar un sustento teórico para el mismo. Se hará una revisión de fundamentos de sistemas inalámbricos esto contempla: estándares, organismos, métodos de seguridad y métodos de acceso.

1.1.4.2 Fase II: Análisis de la situación Actual

Para el análisis de la situación actual se tomará en cuenta el modelo de referencia OSI que permite identificar tres macro capas: capa física, lógica y aplicaciones. Para desarrollar y analizar la capa física se tomará como referencia la arquitectura planteada por CISCO SAFE (el modelo se detalle en el ANEXO A) la misma que

propone una arquitectura modular permitiendo desarrollar el análisis previo al diseño de la red.

En base a SAFE se describirá la infraestructura tecnológica actual de la red, se agrupará y ubicará los dispositivos en los diferentes módulos.

El análisis lógico se desarrollará en base a los siguientes parámetros: direccionamiento y enrutamiento, posteriormente se analizará las aplicaciones que contemplará los servicios que se encuentran disponibles en la red.

1.1.4.3 Fase III: Análisis de requerimientos

En esta fase se efectuará el análisis de los requerimientos para la implementación de una red inalámbrica en el sector del CONDADO, se tomará en cuenta el tipo de usuarios que se tendrá potencialmente, se recopilará datos mediante MRTG de varios clientes actuales, se ejecutará el análisis del tipo de tráfico que utilizan y la capacidad de canal que es ocupada en promedio. Se hará un análisis del área a cubrir en la cual se manejarán mapas que ayuden a identificar la topografía del terreno y determinar el número de equipos necesarios para que los usuarios tengan acceso al servicio de Internet. Se analizará el entorno para verificar la cantidad de redes inalámbricas cercanas, número de canales usados, nivel de señal a ruido, seguridad implementada y modo de trabajo. En esta fase se obtendrán datos exactos para el diseño de la red inalámbrica para servir de Internet a este sector.

1.1.4.4 Fase IV: Diseño

En esta fase se ejecutará el diseño funcional de la red de acceso inalámbrico en base a los requerimientos encontrados en la fase anterior. Este diseño contemplará los siguientes parámetros: red física y lógica, sistema de seguridad, sistema de

autenticación, posteriormente se describirá varios productos existentes en el mercado, finalmente se hará un análisis legal y de costos para el proyecto. El diseño de la red física y lógica tomará como referencia los módulos de la arquitectura SAFE, el sistema de seguridad y autenticación se basarán en los datos obtenidos en la fase III. El análisis de costos incluirá productos existentes en el mercado y el análisis legal se apoyará en el marco referencial de telecomunicaciones vigente en el país.

1.1.4.5 Fase V: Prototipo y pruebas.

Esta fase comprende la implementación de un prototipo que cumpla con los requerimientos mínimos del estudio. Y tiene como objetivo demostrar la funcionalidad del diseño planteado en la fase IV, en la implementación del prototipo se utilizará equipos básicos que ayuden a simular la red planteada en el diseño, posteriormente se efectuarán pruebas para verificar su funcionalidad, rendimiento, disponibilidad y seguridad. Los resultados de las pruebas permitirán ajustar el prototipo implementado.

1.1.5 ALCANCE

Este proyecto brindará una solución confiable para el acceso inalámbrico a Internet, puede ser aplicable en otras áreas como son aeropuertos, centros de convenciones y sitios turísticos. Se considerarán estándares y tecnologías modernas, tales como IEEE 802.1x, Captive Portal, análisis de la situación actual de Gigowireless, verificación de los requerimientos para el diseño de una red inalámbrica de acceso a Internet en la urbanización “El Condado” y posteriormente implementación de un prototipo para demostrar la funcionalidad del estudio. Se hará un análisis legal y económico del proyecto; se complementará el proyecto con las conclusiones y recomendaciones adquiridas mediante la experimentación.

1.2 MARCO TEÓRICO: SISTEMAS INALÁMBRICOS

1.2.1 INTRODUCCIÓN

La masiva popularidad de las redes inalámbricas ha llevado a una disminución continua en el costo del equipamiento, mientras que la capacidad del mismo continúa incrementándose. Esta es una ventaja que debería aprovecharse al momento de implementar una infraestructura de comunicaciones.

Mediante este proyecto se pretende dar una idea íntegra de cómo implementar una red inalámbrica para proveer de servicio de Internet, tomando en cuenta la red física y lógica, sin perder de vista la parte legal y económica; mostrar una metodología para llegar a dimensionar e implementar una red inalámbrica, dando a conocer la información y herramientas necesarias.

1.2.2 ORGANIZACIONES Y ESTÁNDARES DE REDES INALÁMBRICAS.

1.2.2.1 Organizaciones

Entre las organizaciones principales se tiene a WIFI como asociación internacional sin fines de lucro creada para certificar la interoperabilidad de productos WLAN en base a la especificación IEEE 802.11.

La FCC es una agencia gubernamental independiente de los EE.UU. y es responsable de regular las comunicaciones interestatales e internacionales por radio, televisión, teletipo, satélite y cable. Existen exclusiones al requisito de licencia y las regulaciones de la Parte 15 de PTT permiten el funcionamiento sin ellas de dispositivos de espectro de difusión en las bandas de frecuencias de: 902 MHz a 928

MHz, 2,4 GHz a 2,5 GHz, y 5,8 GHz a 5,9 GHz. Estas tres bandas de frecuencias se han asignado para varias aplicaciones industriales, científicas y médicas.

1.2.2.2 Bandas ISM y UNII

- **ISM - Industrial Scientific Medical Bands.**

La FCC indica un intervalo de frecuencia para las WLAN en la industria, científica y médica, con licencias libres que se describen a continuación:

Banda ISM 900 MHZ.- Este Rango de Frecuencias está definido desde los 902 MHZ a 928 MHZ, con un intervalo de +/- 13 MHZ. Son usadas por los teléfonos o sistemas de cámaras inalámbricas. Los dispositivos que trabajan en esta frecuencia tienen un alto costo y su velocidad está limitada a 1 Mbps.

Banda ISM 2,4 GHZ.- Utilizada por los estándares 802.11, 802.11b, 802.11g. Este rango de frecuencias es usado para las comunicaciones en redes inalámbricas, tiene una variación de 100 MHZ.

Banda ISM 5,8 GHZ – El estándar 802.11a utiliza este rango de frecuencia que está definido desde 5,725 GHZ hasta 5,875 GHZ.

- **UNII - Unlicenced National Information Infrastructure Bands**

Existen varias bandas en 5 GHZ y tienen una separación de 100 MHZ, son usadas en los dispositivos que operan con 802.11a. Las tres bandas existentes se las conoce como baja, media y alta; tienen cuatro canales no sobrelapados OFDM, cada uno separado 5 MHZ. La FCC indica que la banda baja debe usarse para interiores,

la banda media puede ser usada en interiores u exteriores y la banda alta es usada en exteriores.

Banda Baja.- Se halla en el rango de frecuencias que está entre 5,15 GHZ a 5,25 GHZ, la FCC específica que tiene un máximo de potencia de salida de 50 mW, para 802.11a la IEEE específica que la potencia de salida de los dispositivos sea 40 mW, esto hace que los equipos sean usados para interiores.

Banda Media.- Se halla en el rango de frecuencias que va desde 5,25 GHZ a 5,35 GHZ, la FCC especifica una potencia máxima de salida de 250 mW. Para 802.11a la IEEE recomienda que la potencia de salida de los dispositivos sea de 200 mW, esto hace que los equipos sean usados para interiores o exteriores. Es utilizada frecuentemente para enlazar edificios en espacios cerrados.

Banda Alta.- Comprende el rango de frecuencias que está entre 5,725 GHZ a 5,825 GHZ y la FCC específica que tiene un máximo de potencia de salida de 1000 mW, para 802.11a la IEEE recomienda una potencia de salida 800 mW. Está reservada para enlaces exteriores.

1.2.2.3 Estándares IEE 802.11

La tecnología principal utilizada actualmente para la construcción de redes inalámbricas de bajo costo es la familia de protocolos 802.11, también conocida como Wi-Fi. El hecho de que exista un estándar permite que los costos de los dispositivos disminuyan y puedan ser adquiridos por una mayor cantidad de personas existiendo interoperabilidad entre ellos.

El protocolo IEEE 802.11 es un estándar de comunicaciones del IEEE que define la capa física y de enlace para una transmisión inalámbrica. El estándar original fue

publicado por el IEEE en 1997 y es conocido como *IEEE 802.11-1997*, dos años más tarde se actualizó dando lugar al *IEEE 802.11*. Las velocidades de transferencia permitidas son de 1 Mbps, 2 Mbps y trabajaban en la banda ISM a una frecuencia de 2,4 GHz.

Existen muchos protocolos en la familia 802.11 y no todos están relacionados específicamente con el de radio. Los tres estándares implementados actualmente en la mayoría de los equipos disponibles son:

- **IEEE 802.11b**

Ratificado por IEEE el 16 de septiembre de 1999, el protocolo de redes inalámbricas 802.11b, trabaja con frecuencias en el rango de 2.4 Ghz es decir; en la banda ISM, maneja distintas velocidades de transmisión: 1 Mbps, 2 Mbps, 5.5 Mbps y 11 Mbps. Además implementa DRS (*Dynamic Rate Shifting*) para ajustar las velocidades según las condiciones del entorno, estos valores se consiguen debido al uso de la modulación CCK (*Complementary Code Keying*) que da una mayor eficiencia que la antigua modulación utilizada (código Barker). A esto se incorpora el uso de la técnica de espectro ensanchado DSSS (*Direct Sequence Spread Spectrum*).

Los problemas que encuentra esta tecnología es el no soportar mecanismos de calidad de servicio y se halla en una franja de frecuencias muy utilizada por teléfonos inalámbricos o dispositivos Bluetooth. Como principales ventajas cabe destacar el bajo costo de la tecnología que ha impulsado una fuerte implantación, que trabaja en una banda de frecuencias de uso gratuito.

- **IEEE 802.11g.**

El protocolo 802.11g es hoy un estándar de facto en la redes inalámbricas. Utilizado como una característica común en todas las laptops y muchos de los dispositivos de escritorio. Ocupa el mismo rango de frecuencias que 802.11b, pero con el esquema de modulación denominado Orthogonal Frequency Division Multiplexing (OFDM). Tiene tasas de transmisión de 6 a 54 Mbps y mantiene compatibilidad con 802.11b gracias al soporte de las velocidades inferiores.

- **IEEE 802.11a.**

Ratificado por la IEEE el 16 de septiembre de 1999, este estándar OFDM tiene una tasa de transmisión máxima de 54 Mbps. Opera entre 5,725 GHZ - 5,825 GHZ y en una porción de la banda UNII entre 5,15 GHZ – 5,35 GHZ. Esto lo hace incompatible con 802.11b y 802.11g.

La multiplexión por división de frecuencia ortogonal (OFDM) es una técnica que divide un canal de comunicaciones en cierta cantidad de bandas de frecuencia que se encuentran separadas por el mismo espacio, usa 52 subportadoras que se encuentran separadas 312,5 KHZ. Los datos se envían por 48 portadoras simultáneamente, donde cada subportadora transporta una porción de los datos del usuario, cuatro de ellas se utilizan como pilotos y son ortogonales entre sí.

El tiempo para transmitir cada bit se incrementa en proporción a la cantidad de portadoras. Esto hace al sistema menos sensible a la interferencia multiruta, que es una fuente importante de distorsión.

1.2.2.4 Arquitectura de Redes 802.11

- **Identificación de redes**

Identificador de conjunto de servicios (SSID - service set identifier).- Es un código incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red, tiene una longitud de 2 a 32 caracteres alfanuméricos, todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID. Este identificador puede servir para segmentar redes inalámbricas, es conocido comúnmente como el nombre de la red, es enviado siempre en las tramas: beacons, requerimiento y respuesta.

Existen algunas variantes principales del SSID, las redes *ad-hoc*, consisten en máquinas de clientes sin un punto de acceso y utilizan el BSSID (*Basic Service Set Identifier*), mientras las redes infraestructura incorporan un punto de acceso que usa el ESSID (E de extendido) como identificador. Un método básico para proteger una red inalámbrica es desactivar el broadcast del SSID, ya que para el cliente no aparecerá como una red en uso.

Beacons.- Son tramas cortas que se envían cada 100ms desde los puntos de acceso a las estaciones (modo infraestructura) o entre estaciones (modo ad-hoc), contienen la información necesaria para identificar las características de la red y poder conectar con el punto de acceso deseado.

- **Tipos de servicios**

Sistema de distribución (DS-Distribuction System).- Es la interconexión de dos o más BSS (basic service set), permite incrementar la cobertura de la red, el ingreso al sistema de distribución se hace mediante puntos de acceso y puede ser cableado o

inalámbrico, LAN o WAN. La arquitectura WLAN IEEE 802.11 se especifica independientemente de las características físicas del DS (distribution system), el mismo habilita el soporte para dispositivos móviles proporcionando servicios necesarios para manipular el mapeo de dirección a destino y la integración sin fisuras de múltiples BSSs. Los datos se desplazan entre un BSS y el DS a través de un AP.

Conjunto de servicios básicos (BSS- Basic Service Set)- Es el bloque constructor básico de una LAN IEEE 802.11. La Figura 1.1 muestra un BSS con tres estaciones y un access point (AP) trabajando en modo infraestructura, el círculo representa área de radio frecuencia o celda, a medida que una estación se va alejando la velocidad de datos disminuye, cuando sale del área de cobertura ya no puede comunicarse con otros miembros. El Punto de acceso coordina la comunicación entre las estaciones.

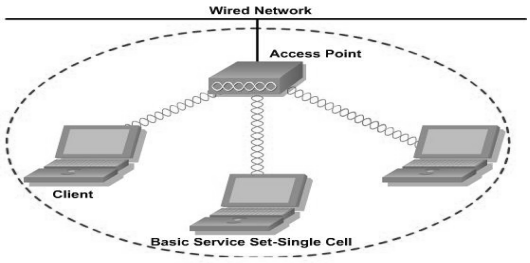


Figura 1.1 BSS

Conjunto de servicios extendido (ESS- Extended Service Sets).- Se define como dos o más BSSs conectados por medio de un DS común, como lo ilustra la Figura 1.2, permite la creación de una red inalámbrica de tamaño y complejidad arbitrarios, al igual que sucede con un BSS, todos los paquetes de un ESS deben atravesar uno de los puntos de acceso.

Las estaciones que se encuentran dentro de un ESS pueden comunicarse entre si y pueden desplazarse de un BSS a otro (dentro del mismo ESS), de manera transparente a LLC.

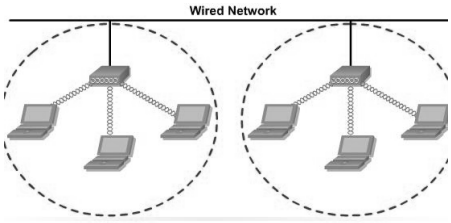


Figura 1.2 ESS

Conjunto de servicios básicos independiente (IBSS- Independen Basic Service Set).- Es el tipo más básico de LAN IEEE 802.11, consiste en dos estaciones. En este modo de operación ellas se comunican directamente, ya que este tipo de LAN IEEE 802.11 se forma generalmente sin pre-planificar y se denominan redes ad hoc.

Roaming.- Es el proceso o capacidad de un cliente inalámbrico de desplazarse de una celda, o BSS, a otra, sin perder conectividad con la red. Los puntos de acceso se entregan el cliente entre si y son invisibles al mismo. El estándar IEEE 802.11 no define como debería llevarse a cabo el roaming, pero sí define los bloques de construcción básicos, que incluyen la búsqueda activa y pasiva y un proceso de re-asociación. La re-asociación con el AP debe tener lugar cuando una STA hace roaming de un AP a otro Autenticación y Asociación.

- **Conjunto de servicios de distribución en redes inalámbricas**

Para que una estación pueda unirse a un BSS debe elegir un AP y asociarse. El estándar 802.11 define servicios de distribución y son los siguientes:

Reasociación.- Permite a una estación asociada poder moverse entre diferentes puntos de acceso.

Desasociación.- Finaliza la asociación de una estación.

Privacidad.- Protege a los mensajes que son transmitidos para que estos no sean accedidos sino por la persona a la cual esta emitido.

- **Autenticación y Asociación.**

La conexión a una red inalámbrica consiste en dos sub-procesos; estos siempre ocurren en el mismo orden y son llamadas autenticación y asociación.

Autenticación: mediante Open System (autenticación nula, o bien no requiere clave de acceso) y mediante Shared Key (utilizada para WEP). El primer paso para conectarse a una red inalámbrica es la autenticación, este es un proceso para comprobar la identidad de un adaptador en la red para aceptarlo o rechazarlo. El estándar 802.11 especifica dos formas de autenticación: el sistema abierto y el sistema basado en una clave compartida.

Asociación: mediante Open Network (red disponible para cualquier cliente mediante el broadcast del SSID) y mediante Closed Network (disponible sólo para aquellos clientes conocedores del SSID del Access Point). La asociación es un proceso por el cual el punto de acceso reserva recursos y sincroniza con una estación-cliente. Una vez que el adaptador de red se ha autentificado, tiene que asociarse al punto de acceso antes de poder transmitir tramas de datos. La asociación es importante para sincronizar a ambos elementos con información importante como por ejemplo las tasas de transmisión admitidas.

El adaptador inalámbrico inicia el proceso enviando una trama de solicitud que contiene elementos como el SSID y tasas de transferencia admitidas. El punto de acceso reserva memoria para ese cliente y le asigna un identificador. Una vez que el adaptador de red y el punto de acceso hayan completado el proceso de asociación pueden comenzar a transmitir tramas de datos entre ellos.

Estados de autenticación y asociación

Desautentificado y desasociado, en este estado el usuario esta totalmente desconectado de la red e imposibilitado de pasar tramas para validarse ante el AP.

Autentificado y desasociado, en este segundo estado el cliente puede pasar al proceso de autenticación, pero no se halla asociado con el punto de acceso.

Autentificado y asociado, en este estado final el nodo se halla conectado totalmente a la red, el punto de acceso verifica en su tabla de asociación que el cliente se halle autentificado y asociado, para poder pasar tramas al punto de acceso.

- **Modos de Autenticación**

Sistema Abierto (Open System).- No posee un algoritmo de autenticación como tal. El punto de acceso responde a todas las peticiones de autenticación sin pedir ningún tipo de validación, se basa en la encriptación posterior que se va a hacer de los datos enviados a través de la red inalámbrica. Aunque un cliente pueda validarse contra el punto de acceso, si no conoce las claves de encriptación de los datos no podrá enviar información. Sin embargo, si el administrador de la red no configura encriptación WEP (por defecto esta desactivada), cualquier usuario puede utilizar la red inalámbrica sin necesidad de suministrar cualquier tipo de credencial.

Clave compartida (Shared Key Authentication). - Es el segundo método de autenticación definido en el estándar 802.11. Este mecanismo necesita que tanto clientes como puntos de acceso tengan configurada una clave WEP estática. Para evitar el envío de la clave WEP a través del medio inalámbrico se utiliza un mecanismo del tipo petición/respuesta. En este caso el punto de acceso envía al cliente un texto aleatorio para que sea cifrado con la clave WEP, el mismo envía una respuesta, el punto de acceso descifra el mensaje con su clave y comprueba si coincide con el texto aleatorio original, si coinciden el clientes es validado, este tipo de validación requiere la configuración de una clave WEP estática y precompartida entre los clientes y los puntos de acceso. El problema conlleva, que ante el robo de uno de los portátiles es necesario que el administrador de la red se encargue de modificar manualmente la clave WEP de todos los clientes y de los puntos de acceso.

1.2.3 MODOS DE OPERACIÓN

1.2.3.1 Modo Infraestructura

Es conocido también como modo Punto de acceso o Infraestructura, es utilizado para crear un servicio de acceso tradicional. El dispositivo inalámbrico crea una red con un canal y un nombre específico (llamado SSID), para ofrecer sus servicios. En el modo maestro, las tarjetas inalámbricas administran todas las comunicaciones de la red (autentificación de clientes inalámbricos, control de acceso al canal y repetición de paquetes).

1.2.3.2 Modo Ad-hoc

Permite la creación de una red multipunto a multipunto, donde no hay un único nodo maestro o AP. En el modo ad-hoc, cada tarjeta inalámbrica se comunica

directamente con sus vecinas. Cada nodo debe estar dentro del alcance de los otros para comunicarse, concordar en un nombre y un canal de red.

En el modo monitor, las tarjetas inalámbricas no trasmiten datos. Se utiliza para analizar problemas en un enlace inalámbrico o para observar el uso del espectro en el área local. El modo monitor no es usado para las comunicaciones normales.

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

1.2.4 TIPOS DE REDES

1.2.4.1 Punto a punto

Este tipo de redes generalmente se usan para conectarse a Internet donde el acceso no está disponible de otra forma. Uno de los lados del enlace punto a punto estará conectado a Internet, mientras que el otro utiliza el enlace para acceder al mismo. Los puntos que se deben interconectar deberán tener línea de vista para incrementar la confiabilidad del enlace, se puede alcanzar distancias mayores a los 10 Km. Para este tipo de enlaces se usan antenas direccionales tanto para el transmisor como para el receptor. La FCC estipula que por cada 3 dbi en exceso de los 6 dbi de ganancia de la antena, la potencia del radiador debe ser reducido en 1db a partir de los 30 dbm iniciales.

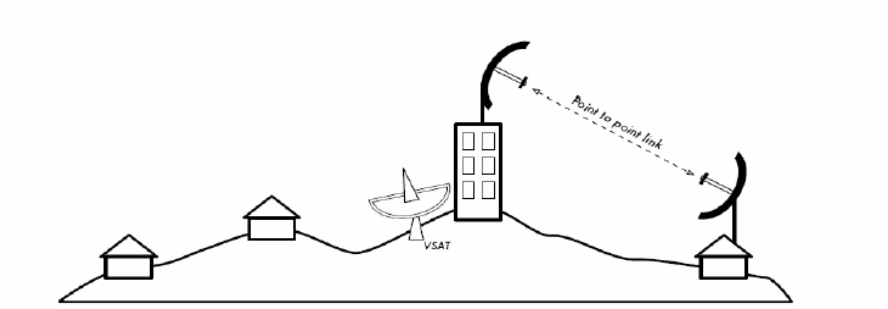


Figura 1.3 Punto a punto

1.2.4.2 Punto a multipunto

Las redes punto a multipunto tiene varios nodos que se comunican con un nodo de acceso central. La FCC limita el EIRP a 4W tanto en las bandas de 2.4 GHZ y 5 GHZ La limitación de potencia para el elemento radiador es 1 watt. Para explicar esto se toma el siguiente ejemplo, si un radio trasmisor de 1 w (+30 dbm) es conectado a una antena de 12dbi omnidireccional, la potencia total es sobre los 4 Watt. La FCC estipula que por cada 3dbi sobre los 6dbi de ganancia inicial de la antena, la potencia del radio debe reducirse 3db por debajo de la potencia inicial de 30 dbm.

Potencia en la antena (dbm)	Ganancia de la antena (dbi)	EIRP(dbm)	EIRP (watts)
30	6	36	4
27	9	36	4
24	12	36	4
21	15	36	4
18	18	36	4
15	21	36	4
12	24	36	4

Tabla 1.1 Limitación de potencia

1.2.4.3 Multipunto a multipunto

Este tipo de redes se denominan también como una red ad-hoc o en malla (mesh). En una red multipunto a multipunto, no hay una autoridad central. Cada nodo de la red transporta el tráfico de tantos otros como sea necesario y todos los nodos se comunican directamente entre si. El beneficio de este diseño de red es que asi ninguno de los nodos sea alcanzable desde el punto de acceso central, igual pueden comunicarse entre si.

En una red mesh multipunto a multipunto, todos los radios operan en modo ad-hoc de manera que puedan comunicarse directamente. En este modo no hay una relación jerárquica entre maestro-cliente, los nodos pueden comunicarse directamente si están dentro del rango de su interfaz inalámbrica. La desventaja del modo ad-hoc es que los clientes no repiten el tráfico destinado a otros clientes, pero pueden hacerlo si se aplica el enrutamiento. Las redes malladas (mesh), tienen como estrategia que cada nodo actúe como un relevo para extender la cobertura de la red inalámbrica. Cuanto más nodos, mejor será la cobertura de radio y rango de la nube mallada. Pero existe una desventaja en este tipo de redes debido a que si el dispositivo utiliza solamente una interfaz de radio, el ancho de banda disponible se ve reducido significativamente cada vez que el tráfico es repetido por los nodos intermedios en el camino desde un punto a otro. Además, existirá interferencia en la transmisión de esos nodos compartiendo el mismo canal. Por lo tanto, las económicas redes malladas ad-hoc pueden suministrar muy buena cobertura de radio a una red inalámbrica comunitaria a expensas de la velocidad, especialmente si la densidad de los nodos y la potencia de transmisión son altas. Si una red ad-hoc tiene pocos nodos que están funcionando simultáneamente, se encuentran estáticos y siempre tienen radio enlaces estables, es posible escribir a mano una tabla de

enrutamiento individual para todos los nodos. Desafortunadamente, esas condiciones raramente se encuentran en el mundo real. Los nodos pueden fallar, los dispositivos WiFi pueden desorientarse y la interferencia puede hacer que los radio enlaces estén inutilizados en cualquier momento. Además, conlleva mucho trabajo el actualizar varias tablas de enrutamiento a mano si se adiciona un nodo a la red, mediante el uso de protocolos que mantienen automáticamente las tablas de enrutamiento individuales de cada nodo involucrado. Los protocolos de enrutamiento más comunes en el mundo cableado (como el OSPF) no funcionan bien en este ambiente porque no están diseñados para tratar con enlaces perdidos o con topologías que cambian rápidamente.

1.3 SEGURIDADES SOBRE REDES INALÁMBRICAS.

1.3.1 INTRODUCCIÓN

En la actualidad, gracias a la movilidad y reducción de costos que aporta la tecnología Wi-Fi, han surgido un gran número de redes inalámbricas en oficinas, centros de trabajo y lugares públicos (hot-spots). Sin embargo muchas veces no se tiene en cuenta la vulnerabilidad de estas redes tanto respecto a la privacidad de las comunicaciones como frente a intrusiones en la red. Por esta razón, a la hora de afrontar el reto de movilidad, es imprescindible conocer los diferentes protocolos y mecanismos de seguridad existentes e implementar medidas de precaución.

Para que un usuario (o posible hacker) pueda enviar datos a una red cableada es necesario que conecte su computador físicamente a uno de los puertos de un dispositivo de red que está brindando servicio a la red dentro de una empresa. En las redes inalámbricas, todo usuario que se encuentre en el área de cobertura se convierte en un posible usuario. Además cabe considerar que éstas áreas de coberturas no suelen respetar las paredes físicas del edificio, con lo que es posible

que un usuario de la red inalámbrica este físicamente situado en un edificio de en frente o en la calle. Ello posibilita lo que se denomina **"ataque del aparcamiento"** (parking lotattack) conceptualmente, el intruso se sienta en el aparcamiento de la empresa (fuera del edificio, pero dentro del alcance de la red) y ataca a las máquinas desde allí, la Figura 1.4 indica este tipo de ataque.

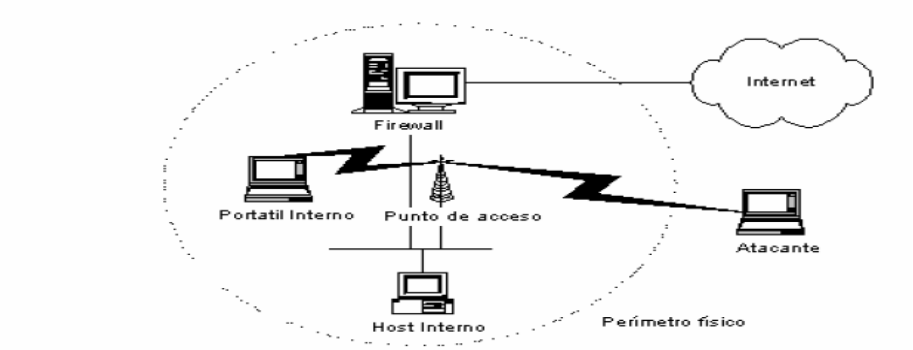


Figura 1.4 Ataque, parking lotattack

1.3.2 AMENAZAS EN LAS REDES WLAN (WIRELESS LOCAL AREA NETWORK)

Las redes inalámbricas están expuestas a varias amenazas, a continuación se detalla varios tipos:

1.3.2.1 Escuchas ilegales.

La principal amenaza en una WLAN es que un tercero no autorizado escuche ilegalmente las señales de radio intercambiadas entre una estación inalámbrica y un punto de acceso, comprometiendo la confidencialidad de información propietaria o sensible. La realización de escuchas ilegales es un ataque pasivo, cuando un

operador de radio envía un mensaje a través de un enlace, todos los usuarios equipados con un receptor compatible y que estén situados dentro del rango de transmisión pueden escuchar el mensaje. Además, dado que quién está escuchando ilegalmente pueda recibir un mensaje sin alterar los datos, el emisor y el receptor del mensaje pueden no darse cuenta de la intrusión. Como las señales de radio emitidas por una WLAN pueden propagarse mas allá del área en la cual han sido originadas, penetrar las paredes de los edificios y otros obstáculos físicos, dependiendo de la tecnología de transmisión utilizada y de la intensidad de la señal, existen equipos capaces de interceptar el tráfico WLAN, en forma de adaptadores inalámbricos y otros productos compatibles con 802.11. La dificultad para los que realizan escuchas ilegales consiste en decodificar una señal digital de 2,4 GHz, porque la mayor parte de los sistemas WLAN utilizan tecnología de expansión de espectro, que es resistente a las escuchas.

1.3.2.2 Acceso no autorizado.

Otro de los problemas es la posibilidad de que un intruso se introduzca en el sistema de una red WLAN disfrazado de un usuario autorizado. Una vez dentro, puede violar la confidencialidad e integridad del tráfico de red; enviando, recibiendo, alterando o falseando mensajes. Esto constituye un ejemplo de **ataque activo** y puede llevarse a cabo utilizando un adaptador inalámbrico que sea compatible con la red objetivo, o utilizando un dispositivo comprometido (por ejemplo: robado) que esté conectado a la red. La mejor protección frente a los accesos no autorizados consiste en poner en práctica mecanismos de autenticación que aseguren que solo los usuarios autorizados puedan acceder a la red. Tales mecanismos se implantan de manera regular en las redes LAN cableadas, no solo para prevenir los accesos no autorizados, sino también para detectar las intrusiones cuando éstas suceden. Descubrir a los intrusos intentando acceder a una red WLAN no es una tarea fácil,

debido a que los ataques que no tengan éxito pueden ser mal interpretados como intentos de conexión legal, pero invalidados, debido a las altas tasas de errores de bit de las transmisiones de radio, o a intentos realizados por estaciones que pertenezcan a otra red.

1.3.2.3 Interferencias aleatorias e intencionadas.

Una tercera amenaza a la seguridad de una red WLAN son las interferencias de radio, que pueden degradar seriamente el ancho de banda (la tasa de transferencia de datos). En muchos casos, las interferencias son accidentales; dado que las redes WLAN utilizan zonas del espectro que no requieren licencia, otros dispositivos electromagnéticos que estuvieren operando en el espectro de infrarrojos o en la banda de radiofrecuencia de 2,4 GHz podrían solaparse con el tráfico de la red WLAN. Las interferencias pueden ser intencionadas, si un atacante dispone de un transmisor potente, puede generar una señal de radio suficientemente fuerte como para cancelar las señales más débiles, interrumpiendo las comunicaciones. Estas interferencias, suponen un ataque de denegación de servicios (DoS).

1.3.2.4 Amenazas físicas.

Las redes WLAN pueden venirse abajo cuando la infraestructura física subyacente sea dañada o destruida. Al igual que una LAN cableada, una WLAN utiliza una serie de componentes físicos, incluyendo los puntos de acceso, cables, antenas, adaptadores inalámbricos y software. Los daños sufridos por cualquiera de estos componentes podrían reducir la intensidad de las señales, limitar el área de cobertura o reducir el ancho de banda, cuestionando la capacidad de los usuarios para acceder a los datos y a los servicios de información.

1.3.3 MECANISMOS DE SEGURIDAD.

1.3.3.1 Seguridad para asociación a la red inalámbrica

- **WEP**

El estándar 802.11 propone el algoritmo WEP para cifrar los datos. WEP son las siglas de Wired Equivalent Privacy (Privacidad Equivalente a redes cableadas). WEP es un mecanismo de cifrado continuo que utiliza clave simétrica, el hecho de utilizarla implica que la clave de encriptación debe ser conocida por los dos extremos. Cabe destacar que el cifrado de información propuesto en 802.11 solo cifra el tramo inalámbrico de la comunicación (entre el cliente inalámbrico y el punto de acceso) y no realiza un cifrado extremo a extremo como sería deseable.

Además el estándar 802.11 especifica que estas claves deben ser estáticas y no indica ningún mecanismo para la distribución automática de ellas, por lo que al final es necesario llevar a cabo una configuración manual.

Una de las debilidades principales del mecanismo básico de seguridad es su naturaleza estática; una vez que se configura una clave para una red, no cambia nunca, lo que significa que cuando se consigue romper, ya puede accederse libremente a la red para siempre. Esta distribución de claves se hace de forma estática, esto significa que mantener una red segura puede suponer una carga administrativa adicional importante. La solución recae en el uso de claves dinámicas que cambien automáticamente.

- **Protocolo de Integridad de Clave Temporal (TKIP)**

Con este protocolo se pretende resolver las deficiencias del algoritmo WEP, este posee un código de integración de mensajes (MIC) el cual cifra el checksum (suma de comprobación) incluyendo las direcciones físicas (MAC) del origen, destino y los datos en texto claro de la trama 802.11 protegiendo con esto cualquier ataque por falsificación.

- **EAP-TLS (Extensible Authentication Protocol with Transport Layer Security)**

Protocolo de autenticación basado en certificados digitales. Ofrece una autenticación fuerte mutua (tanto de la estación como del punto de acceso), credenciales de seguridad y claves de encriptación dinámicas. Requiere la distribución de certificados digitales a todos los usuarios así como a los servidores RADIUS (Remote Authentication Dial In User service).

- **Wifi Protected Access (WPA)**

WPA utiliza el protocolo de integridad de clave temporal (TKIP) para codificar los datos, además Implementa el estándar 802.1x utilizando el protocolo de autenticación extensible (EAP).

- **Wifi Protected Access 2 (WPA2)**

Aprobado por la Wi-Fi Alliance (1 de Septiembre del 2004), basado en el estándar de seguridad para 802.11i cumpliendo con las normas del National Institute of

Standards and Technology (NIST) FIPS 140-2. WPA2 implementa el algoritmo AES a diferencia de WPA que utiliza RC4, sin embargo WPA2 es totalmente compatible con WPA. Los dispositivos modernos deben soportar este protocolo.

1.3.3.2 Access Control List (ACL):

Si bien no forma parte del estándar, la mayor parte de los productos dan soporte a este método. Se utiliza como mecanismo de autenticación la dirección MAC de cada estación, permitiendo el acceso únicamente a aquellas estaciones cuya MAC figura en la lista de control de acceso (ACL).

1.3.3.3 Filtrado SSI

El SSID es necesario para establecer una comunicación ya que cuando un cliente se quiere conectar con el AP necesita conocer el SSID de la red. Entonces si se desea proteger la red para que nadie la vea, se puede proceder a que el SSID no sea emitido.

1.3.3.4 Filtrado por Mac address.

Para evitar que se conecten clientes no deseados, muchos AP ofrecen opciones para crear listas blancas de equipos que se puedan conectar en función de la dirección MAC de los clientes. Para ello, en el AP, se añaden las direcciones de las máquinas que queremos permitir.

1.3.3.5 Firewall

Sistema de defensa basado en la instalación de una "barrera" entre una computadora, un AP o un router y la Red por la que circulan todos los datos. Este

tráfico es autorizado o denegado por el firewall, siguiendo instrucciones previamente configuradas.

1.3.3.6 Virtual Private Network (VPN)

Sistema para simular una red privada sobre una pública, como por ejemplo Internet, La idea es que la red pública sea vista desde dentro de la red privada como un “cable lógico” que une dos o más redes que pertenecen a la red privada

1.4 MÉTODOS DE ACCESO PARA REDES INALÁMBRICAS.

1.4.1 ESTÁNDAR IEEE 802.1X

La especificación IEEE 802.1X es un estándar de control de acceso desarrollado por el IEEE que permite utilizar diferentes mecanismos de autenticación. Su funcionamiento se basa en el concepto de puerto, visto éste como el punto a través del que se puede acceder a un servicio proporcionado por un dispositivo, que en este caso será el punto de acceso. En principio todos los puertos están desautorizados, excepto uno que el punto de acceso utiliza para comunicarse con el cliente. Cuando un nuevo cliente entra en su área de cobertura, le pasa al punto de acceso información de autenticación, dependiente del mecanismo utilizado, que éste reenvía al servidor de autenticación. Cuando le contesta, si la respuesta es que el cliente puede hacer uso de la red, autoriza un puerto para que lo utilice el cliente. La Figura 1.5 muestra la estructura general de un sistema IEEE 802.1X.

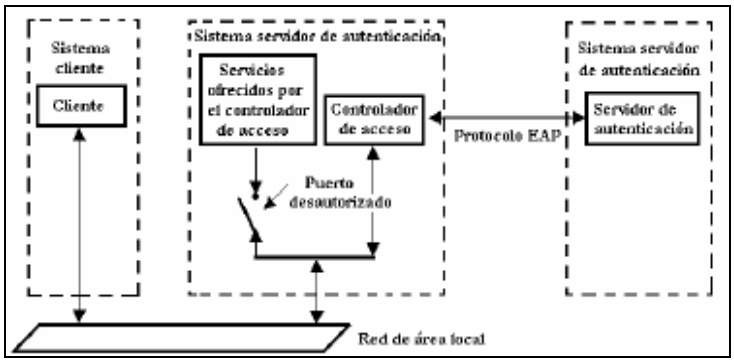


Figura 1.5 Estructura de 802.1X

En esta arquitectura, la información de autenticación se encapsula en el protocolo EAP (Extensible Authentication Protocol), un mecanismo genérico de transmisión de datos de autenticación que puede ser materializado en distintos subprotocolos entre los que, por ejemplo, se encuentra EAP-MD5, que basa la autenticación del cliente en el uso de login y password, o EAP-TLS, que se basa en el uso del protocolo TLS y permite autenticación mutua entre los dos extremos.

Finalmente, los paquetes EAP se transmiten mediante el protocolo EAPOL, el cual especifica cómo encapsular los paquetes EAP en una red de área local tanto Ethernet como 802.11.

1.4.1.1 Servidores de autenticación

Aunque en la especificación 802.1X se habla de los servidores de autenticación en términos genéricos, en la práctica se trata de elementos diseñados según los criterios del marco AAA (Authentication, Authorization and Accounting). Esta sección define los elementos básicos necesarios para autenticar usuarios, manejar peticiones de autorización y realizar la contabilidad del sistema.

Un servidor AAA debe ser capaz de recibir peticiones, examinar el contenido de dichas peticiones, determinar qué autorización se está pidiendo, recuperar las políticas que necesite de un repositorio, evaluar la petición, obtener la respuesta a la petición o bien reenviar otro servidor AAA.

RADIUS.- Es un protocolo encuadrado dentro del marco AAA y utilizado principalmente en entornos donde los clientes son elementos de acceso a la red (como los puntos de acceso). Estos elementos envían información al servidor cuando un nuevo cliente intenta conectarse, tras lo cual, el servidor realiza el proceso de autenticación del usuario y devuelve al elemento de acceso la información de configuración necesaria para que éste trate al cliente de la manera adecuada. Toda la comunicación entre el elemento de acceso y RADIUS se encuentra cifrada mediante un secreto compartido que nunca se transmite por la red.

1.4.1.2 Fase del Protocolo

Autenticación.- La Figura 1.6 indica las fases para la autenticación utilizando 802.1X. La primera fase funciona siguiendo el estándar IEEE 802.1X, es decir, cuando el cliente entra en el área de cobertura del punto de acceso, este le pide su identidad y el cliente se la proporciona.

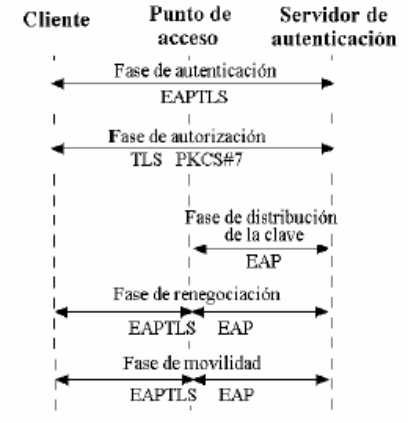


Figura 1.6 Fases de autenticación

Tras esta fase inicial se realiza el proceso de establecimiento de conexión TLS entre los extremos, donde según el estándar tanto el cliente como el servidor se autentican mutuamente mediante certificados X.509 y negocian los parámetros de configuración necesarios para establecer el canal de comunicación seguro. Una vez terminada la negociación, se establece un canal TLS entre el cliente y el servidor de autenticación basado en la posesión por ambas partes de un secreto compartido (Master Secret) que posteriormente se utilizará para derivar la clave WEP.

Fase de autorización.- En esta fase, como muestra la Figura 1.7, el cliente indica al servidor de autenticación, cual es el tipo de conexión que desea en cuanto al ancho de banda requerido y el tiempo que va a estar conectado, junto con los certificados SPKI que demuestran que el usuario está autorizado. Entonces el servidor evalúa los certificados y comprueba si todo es correcto. Si el nivel de privilegios del cliente es el necesario, continúa con el protocolo o desautorizando al cliente a acceder a la red si hay algún problema. De esta forma no es necesario acceder a ninguna base de datos de usuarios para comprobar los permisos de los mismos, sino que solo necesita confiar en las entidades emisoras de dichos certificados de autorización.

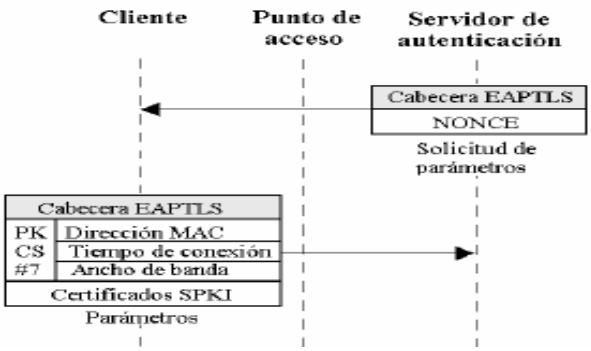


Figura 1.7 Fase de autorización

Los parámetros del cliente se mandan en una estructura firmada PKCS#7, de manera que el servidor de autenticación pueda estar seguro de que nadie ha modificado estos parámetros. Además, toda la información relativa a la autorización del cliente, parámetros y certificados, se transmiten a través del canal TLS establecido anteriormente, de manera que solo pueden haber sido enviados por parte del cliente con el que se ha iniciado el proceso de conexión. Dicha estructura PKCS#7 contiene el certificado del cliente con el que se ha realizado la firma para que el servidor pueda verificar que sea correcta. En el mensaje mediante el cual el servidor le pide al cliente sus parámetros de conexión, se incluye un identificador de 4 octetos aleatorio, que posteriormente se utilizará para derivar la clave WEP junto con la dirección MAC del punto de acceso y la clave maestra de la conexión TLS anteriormente establecida.

Fase de distribución de clave.- En esta fase del protocolo, representada en la Figura 1.8, únicamente participan el punto de acceso y el servidor de autenticación y consiste en que éste último le pase al primero un descriptor de la clave WEP que debe utilizar con el cliente, así como el tipo de servicio que el cliente espera que se le ofrezca. Esta clave WEP la habrá generado el servidor como resultado de una función de resumen digital MD5 aplicada sobre la concatenación de la clave maestra

generada por EAP-TLS, la dirección MAC del punto de acceso. El punto de acceso debe comprobar que en su situación actual puede soportar las necesidades del nuevo cliente, es decir, debe comprobar que la suma total del ancho de banda necesitado por todos los usuarios que actualmente hay conectados, junto con el requerido por el nuevo cliente, no sobrepase su capacidad, además que vaya a estar disponible el tiempo que el cliente requiere, informando al servidor de autenticación sobre la decisión que tome. Tras estas fases, el proceso de conexión ha terminado y si todo se ha realizado correctamente, el servidor de autenticación notifica al punto de acceso la autorización por su parte a que el cliente haga uso de la red. El punto de acceso traslada entonces al cliente esta decisión para que inicie la comunicación. El cliente que habrá generado la misma clave WEP que obtuvo el punto de acceso y puede comenzar a hacer uso de la red, con la garantía de que sus mensajes son solo descifrables por el punto de acceso, dado que la clave WEP generada es distinta para cada usuario.

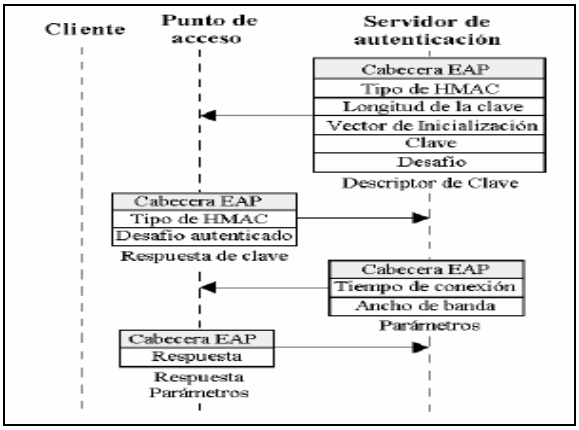


Figura 1.8 Distribución de clave

1.4.2 PORTALES CAUTIVOS

Un portal cautivo es una página Web con la cual un usuario de una red pública y/o privada debe interactuar antes de garantizar su acceso a las funciones normales de la red. Estos portales son principalmente utilizados por centros de negocios, aeropuertos, hoteles, cafeterías, cafés Internet y otros proveedores que ofrecen hot-spots de Wi-Fi para usuarios de Internet. Cuando un usuario potencial se autentifica por primera vez ante una red con un portal cautivo, una página Web se presenta, en la cual se requieren ciertas acciones antes de proceder con el acceso. Un portal cautivo sencillo obliga al visitante para que por lo menos mire y acepte las políticas de uso y luego, acepte presionando sobre un botón en la página. Supuestamente esto, puede absolver al proveedor del servicio de cualquier culpa por el uso anormal e ilegal del servicio. Se puede obligar a ingresar una identificación y/o clave asignada antes de acceder al Internet, con el objetivo de desalentar a quienes quieran usar estos servicios, para usos no autorizados. Para evitar el uso excesivo de la conexión gratuita, se puede adicionar programación que limite por ejemplo, el tamaño de los archivos a descargar o la velocidad a la cual se descargan los mismos.

1.4.2.1 Funcionamiento

Un portal cautivo fuerza a un cliente el mostrar una página determinada. Esto se realiza mediante la intercepción de trafico HTTP, independiente de la dirección seleccionada, hasta que el usuario tiene permiso de salir del portal. Este sistema se puede usar tanto en sistemas cableados como inalámbricos, en la Figura 1.9 se presenta un esquema básico de cómo se estructura un portal cautivo.

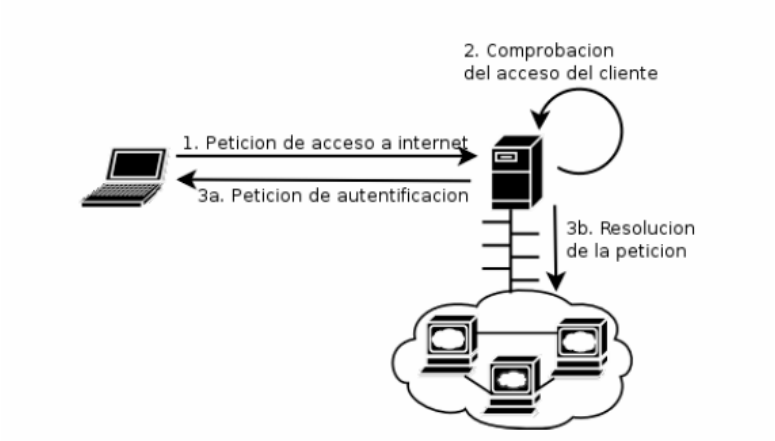


Figura 1.9 Funcionamiento de portal cautivo

La red wireless, debe estar completamente operativa ya sea en modo ah-hoc o infraestructura. Además, puede evitarse colocar métodos de autenticación tales como WEP, WPA entre otros. Esto se debe a que el portal posee funcionalidades de autenticación adicionales.

Algunas características importantes de un portal cautivo son:

• Provee de un sistema de validación de clientes para nodos wireless.

• De acuerdo al tipo de usuario, asigna ancho de banda y da acceso a servicios diferenciados.

• Se basa normalmente en “tokens” temporales gestionados por HTTPSSL (443/TCP). Esto es autenticación segura basada en SSL (navegador); además autoriza mediante usuario contraseña e informa de la entrada y salida del usuario en la red.

• Añade la implementación de QoS por usuarios y grupos.

Modos de funcionamiento.- EL portal cautivo puede funcionar como un **Passive Portal** y es usado cuando hay un Firewall entre el AP y el gateway. También se la puede utilizar como **Open Portal,** esta forma muestra una web con las condiciones de uso y no requiere credenciales.

1.4.2.2 Componentes:

Los componentes de un captive portal son: Módulo de Auth que realiza la autenticación; Módulo de Gateway que redirecciona e implementa el firewall; Módulo Database (Fichero propio -MD5, Base de Datos, Ldap, Radius, PAM, Samba, IMAP) y finalmente el Punto de Acceso que es la comunicación con el cliente.

1.4.2.3 Inconvenientes:

La comunicación no cifrada (por defecto), para la implementación de VPNs. El cliente necesita software específico, además el Spoofing y hi-jacking mientras dura el token temporal.

CAPÍTULO 2
ANÁLISIS

Este capítulo comprende dos secciones: análisis de la situación actual de la infraestructura tecnológica de la empresa y el análisis de requerimientos para el diseño de una red de acceso inalámbrico para proveer servicio de Internet al sector del Condado.

Con el análisis de la situación actual, se describirá las características físicas de los componentes de la red. Los mismos que definen las funcionalidades en base a la arquitectura propuesta por CISCO SAFE.

La sección de análisis de requerimientos, permitirá centrar el estudio del diseño de red de acceso a Internet para el sector de la urbanización “El Condado”, recopilando datos sobre redes cercanas, niveles de señal, canales usados, tipos de usuarios, capacidad de la red y tipos de protocolos.

2.1 ANÁLISIS DE SITUACIÓN ACTUAL

En esta sección se analizará la red física de Gigowireless. Efectuando comparaciones entre la arquitectura modular SAFE y la de Gigowireless, de este modo se identificará los componentes de las infraestructura tecnológica.

A continuación se describirá los módulos encontrados en la red de Gigowireless, permitiendo dar una idea general de los componentes que contiene cada módulo; además se analizará la red lógica que comprende el direccionamiento y enrutamiento. Se verificará los servicios que el ISP posee y se analizará su infraestructura.

Finalmente se determinará el sistema de administración y su funcionamiento.

2.1.1 RED FÍSICA

El análisis de esta sección se basará en la arquitectura propuesta por CISCO SAFE. Se iniciará proponiendo un diagrama modular que permitirá ir agrupando los diferentes componentes que posee el ISP. Esta propuesta se la puede apreciar en la Figura 2.1.

Para empezar el análisis se tomará en cuenta la infraestructura actual que tiene el ISP y se lo comparará con la arquitectura propuesta por CISCO SAFE. Se profundizará el análisis en el módulo de Distribución y acceso, ya que el objetivo de este proyecto, es realizar un diseño de una red inalámbrica que permita proveer de Internet al sector del Condado.

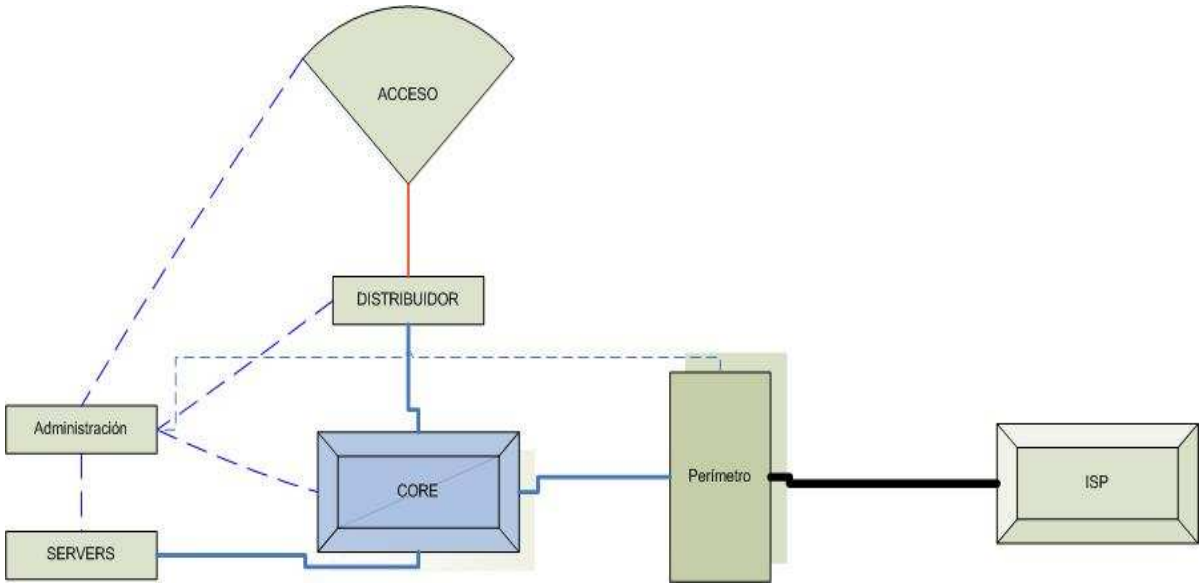


Figura 2.1 Diagrama Modular SAFE

2.1.1.1 Módulo ISP

Este módulo provee de acceso a la información pública, tanto a los clientes de la empresa, como también a los usuarios de Internet.

En este Bloque se ubicará a los carriers o proveedores de Salida internacional, tales como Andinadatos, Access Ram, Etapa. Los dispositivos a usarse pueden ser: conversores de medió, módems o ruteadores, utilizando tecnologías wan para realizar la interconexión.

En la actualidad, la Empresa cuenta con un canal de fibra óptica, el mismo que permite la interconexión con la red Metro ethernet que tiene Andinadatos a nivel de Quito. Gigowireless no tiene acceso a este módulo, debido a que los dispositivos son manejados y administrados por el carrier.

2.1.1.2 Módulo Perímetro Empresarial

Gigowireless dispone de los siguientes elementos para la interconexión hacia los proveedores de Salida internacional (acceso a Internet):

Multiplexor.- Permite separar varios canales: uno para salida Internacional (interconexión al Backbone de Internet) y otro para transmisión de datos de clientes que deseen acceder al Internet. Sus principales características son: Capacidad para manejar cuatro canales E1; 8 puertos G.703; un puerto fast ethernet y un puerto para fibra multimodo con conector ST.

Router.- Utiliza la plataforma del fabricante (CISCO) y permite la interconexión hacia el proveedor mediante una red metro usando un interfaz Fast Ethernet. Este router permite establecer el enrutamiento de la información, enviando los paquetes hacia el

proveedor de salida internacional. El ruteador es un CISCO 1841 y posee dos puertos WAN con interfaces fastethernet.

2.1.1.3 Módulo Central (Core)

El objetivo de este módulo es rutear y switchear el tráfico, lo más rápido posible, de una red hacia otra.

En el ISP se posee un switch 3com que permite manejar todos los segmentos de la red y articularlos hacia la salida internacional. Esta provisto de 24 puertos y no es administrable.

El ruteador lleva a cabo el enrutamiento y el traslado de direcciones (NAT) para la red de clientes inalámbricos de la empresa. Tiene una tarjeta WIC-FETH con cuatro puertos fasthethternet y maneja una VLAN que agrupa a las direcciones IP privadas que son asignadas a los usuarios.

2.1.1.4 Módulo de Distribución

El objetivo de este módulo es proveer servicios de distribución, ruteo, calidad de servicio y control de acceso. Permite el flujo de datos desde los switches de distribución hacia el módulo central y viceversa.

Contiene un switch 3com no administrable que interconecta los diferentes puntos de acceso Inalámbricos hacia el core de la red.

- **Enlaces Punto a punto**

Permite la extensión de la red mediante equipos que trabajan en modo Bridge.

Para este tipo de enlaces se utilizan los siguientes componentes:

Equipos

La empresa tiene equipos de diferentes fabricantes entre los cuales se destaca: Smart Bridges, que son específicos para enlaces punto a punto y Senao, que pueden ser utilizados para enlaces punto a punto o punto multipunto

Se maneja aspectos de seguridad como: encripción wep y filtrado por mac-addres. Los equipos solo se enlazan o funcionan con equipos del mismo fabricante y aceptan una sola mac-addres asociada en la interfaz inalámbrica.

Antenas

Se emplean antenas directivas con una ganancia de 22 dBi, flat panel que trabajan en la banda 5.8GHz.

En la Figura 2.2 se visualiza el diagrama de radiación de la antena y se verifica su directividad.

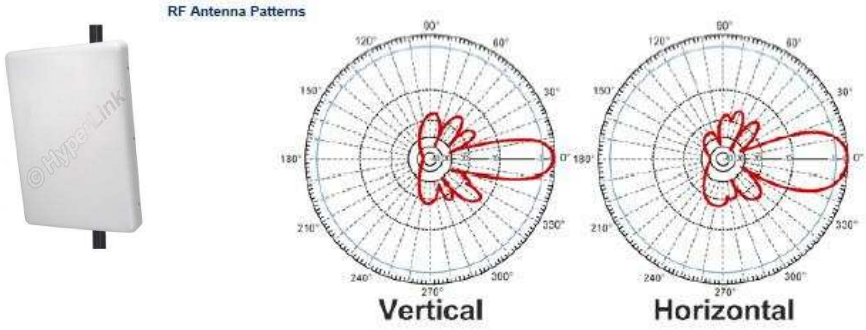


Figura 2.2 Antena directiva

2.1.1.5 Módulo de Edificios (acceso)

El objetivo principal de este módulo es proveer servicios a los usuarios.

En este módulo se ubicará el usuario final y el punto de acceso que se tiene para servir a un sector determinado.

En la actualidad se cuenta con equipos inalámbricos que trabajan en modo "Infraestructura" y como "Puntos de acceso", para proveer el servicio a diferentes sectores.

- **Puntos de Acceso**

Se emplean dispositivos del fabricante Smart Bridges que trabajan bajo el estándar 802.11b y tienen como seguridad la Encriptación WEP de 128 bits y el filtrado por mac address.

Uno de los limitantes de este dispositivo, es el manejo del número de clientes asociados, que según el fabricante se limita a 64.

En la actualidad estos dispositivos tienen asociado un máximo de 30 clientes y su potencia de transmisión se regula a través del software de administración que incluye el fabricante.

Algunos problemas encontrados en este módulo son: la falta de estudios de cobertura; niveles de señales; interferencias y canales usados. Los equipos son diseñados para ser usados en interiores y no en exteriores, lo cual limita su efectividad en la transmisión ya que su potencia está limitada a 60mw y 100 mw.

Antenas

Los nodos utilizan antenas para irradiar la señal dentro de un radio de cobertura de uno a dos kilómetros. Los diferentes tipos de antenas que se utilizan, se describen a continuación:

- **Paneles Sectoriales:**

La Figura 2.3, muestra un panel sectorial, este permite irradiar con un ángulo de apertura de 120º en el plano horizontal y 8º en el plano vertical. Tienen una ganancia de 17 dbi.

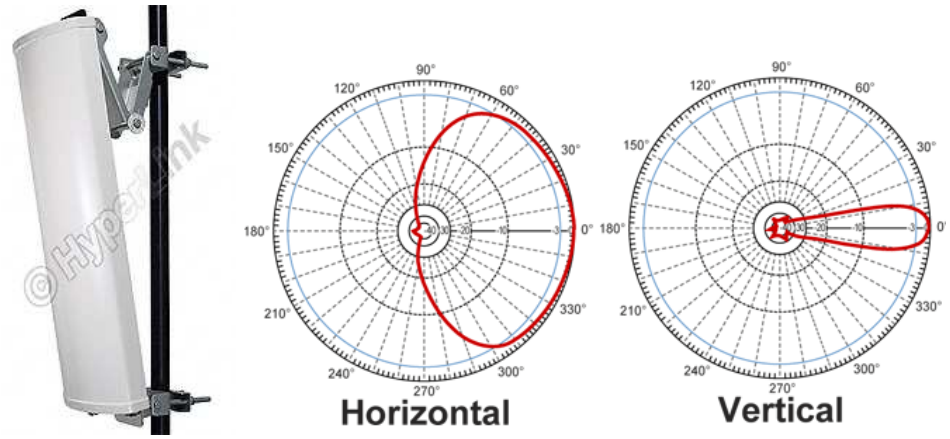


Figura 2.3 Antena Sectorial

- **Omnidireccionales**

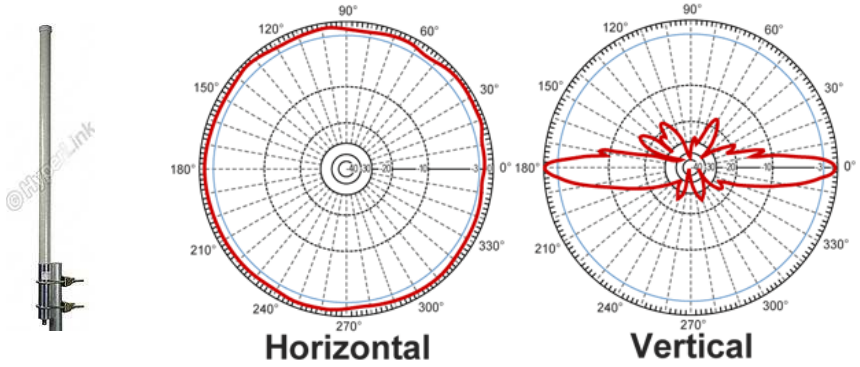


Figura 2.4 Antena ommnidireccional

Tiene un área de cobertura de 360º en el plano horizontal y 8º en el plano vertical. Con una ganancia de 15 dBi, e impedancia de 50ohm., es una antena diseñada para exteriores.

- **CPE (Customer Premises Equipment)**

El equipo receptor instalado al cliente es un punto de acceso trabajando en “modo cliente”, se usa equipos D-link con antenas externas hasta de 12dbi dependiendo de la distancia a la cual se encuentran.

Los inconvenientes de este módulo y que es de preocupación para la empresa son:

a) Inestabilidad en la conexión de los usuarios, reflejada en las continuas desconexiones, motivada por la falta de un plan adecuado de cobertura y de un análisis del entorno.

b) El excesivo tiempo que se debe emplear para la instalación de los usuarios finales, que generan la pérdida de recursos económicos.

c) La baja seguridad utilizada para el acceso, que se la hace únicamente mediante encriptación WEP y filtrado por Mac Ardes, lo que la hace muy vulnerable a los ataques exteriores.

- **Análisis de módulos de core, distribución y acceso**

A continuación se detalla el análisis de los módulos descritos en los puntos anteriores.

- El router 1800 es compartido para cumplir las funciones tanto del módulo de perímetro y de distribución. Este hecho incrementa el trabajo de procesamiento del ruteador, incumpliendo con las recomendaciones de CISCO SAFE, que sugiere “no colocar listas de acceso” en los ruteadores principales. Aparte también se le asigna el trabajo de procesar la “traducción de direcciones (NAT)” para dar acceso a Internet.

- Es necesario que la empresa adquiera un Switch administrable que permita manejar VLans y de este modo disminuir los dominios de broadcast, además este switch permitirá que se implementen las reglas de acceso para la red de distribución, lo que implica el bloqueo del protocolo netbios, que permite compartir recursos en red. En la Figura 2.5 se puede apreciar que el switch no esta bloqueado, visualizando las redes disponibles. Esta es una grave falla de vulnerabilidad, al permitir acceder a la red de un cliente, con solo utilizar el nombre de algún grupo de trabajo.

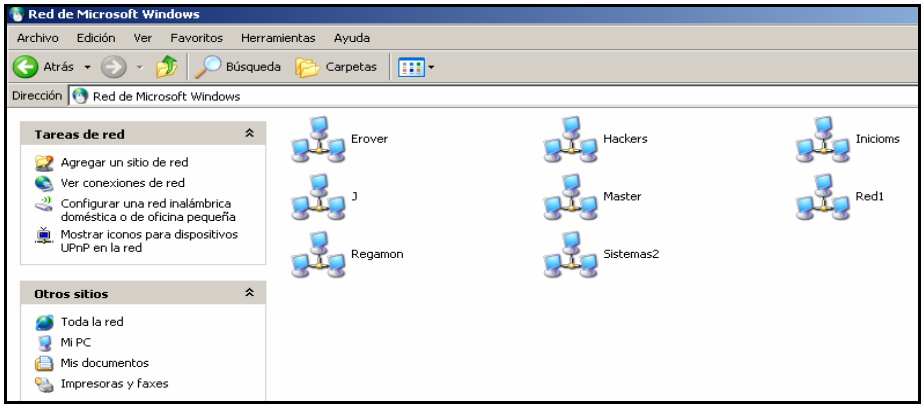


Figura 2.5 Redes

- Para el módulo de acceso se deberá elaborar diagramas de cobertura y estudios para identificar posibles interferencias e implementar mecanismos de autenticación para el acceso a la red. En este caso CISCO SAFE sugiere servidores AAA, que incrementan los niveles de seguridad para regular el acceso a la red.

2.1.1.6 Módulo de Servidores

Gigowireless cuenta con un solo servidor que provee varios servicios como: Hosting, Mail, DNS, Web. El servidor se halla conectado directamente al Core de la empresa y tiene asignado una dirección IP real. Utiliza el Sistema Operativo Linux Enterprise 4 el cual dispone un firewall como medida de protección. Posee una interfaz red Fast Ethernet 10/100 que permite establecer conexiones con el swith de CORE.

2.1.1.7 Módulo de administración

El objetivo de este módulo es facilitar la administración para todos los dispositivos y hosts de una empresa. Actualmente el ISP cuenta con un computador que monitorea

el estado de los clientes y lo equipos de la red. Éste se halla conectado al módulo de distribución mediante una interfaz *fast ethernet*.

2.1.1.8 Equipos

Para la administración de los equipos, se utiliza un software con protocolo ICMP que permite monitorear y controlar los equipos que se hallen funcionando y conectados a la red de la empresa.

Se tiene diferente niveles de poleo de los dispositivos: a los más importantes se sondea cada 20 segundos y para dispositivos de clientes, cada 5 minutos.

En este equipo se verifica el estatus de clientes, comprobando la pérdida de paquetes.

Los equipos de enlace y puntos de acceso, son administrados a través del “software propietario” utilizando el protocolo SNMP.

- SAFE propone que para realizar la administración y monitoreo de dispositivos se lo realice mediante SNMP. En la red, actualmente, existe componentes que se encuentran activados con protocolo SNMP y configurado el nombre de la comunidad como “public”. Esta será una vulnerabilidad aprovechada por cualquier persona para acceder a la configuración y administración de los equipos, poniendo en serio peligro la disponibilidad de la red.

2.1.1.9 Ancho de Banda

Para la administración de ancho de banda se utiliza un dispositivo llamado Packeteer, que permite crear clases de servicio, con diferentes clientes. Esta

característica permite identificar diferentes capacidades para distintos clientes. Por ejemplo: si se quiere crear clientes con 128Kbps, 256kbps, 512Kbps se los puede priorizar y asociar la capacidad mediante direcciones IP, de esta forma se relaciona una dirección con la capacidad de ancho de banda que un cliente requiere.

- La administración de este servicio no está correctamente implementada. Existen graves errores en la administración de las clases creadas, unas están subutilizadas y otras saturadas, generando un continuo malestar en los clientes.

2.1.2 RED LÓGICA

2.1.2.1 Esquema de direccionamiento

El direccionamiento se lo realiza mediante dos tipos de direcciones: IP públicas e IP privadas. Las direcciones IP públicas son usadas en el módulo de Core y Perímetro, mientras que las direcciones IP privadas se las utiliza en los módulos de distribución y acceso.

En el módulo de Core y Perímetro, se tiene dos tipos de subredes que se detallan en la tabla 2.1

Lugar	Segmento
Perímetro	201.219.0.228/30
Core	201.219.13.0/24

Tabla 2.1 Segmentos de red real

El segmento que se encuentra asignado para el Perímetro es usado para la interconexión con el router de Andinadatos, por esta razón la red tiene únicamente dos direcciones IP.

El segmento que corresponde a la red de Core utiliza la otra subred real 201.219.13.0/24, estas direcciones son utilizadas en una de las interfaces del router de borde, otra dirección es usada para los servidores y las restantes se asignan a clientes específicos para el funcionamiento de servidores o aplicaciones especiales.

En la red de distribución y de acceso, el direccionamiento se lo hace a nivel de “capa tres” mediante direcciones IP privadas. Se usa un conjunto de direcciones clase B, pero no se efectúa un subneteo de la misma, esto motiva una excesiva generación de broadcast en la red, ya que todos los enlaces, puntos de acceso, equipos de cliente y computadores de clientes, manejan la misma máscara por defecto de una red clase B.

Tanto a los clientes como a los equipos se les asigna direcciones IP estáticas para poder controlar el ancho de banda y el estado de los terminales.

En tabla 2.2 se presenta un resumen de los segmentos de red que tienen los diferentes puntos de acceso implementados.

Lugar	Segmento
Carapungo	172.16.100.0/16
Ponciano	172.16.188.0/16
Parkenor	172.16.2.0/16

Tabla 2.2 Segmentos de red privada

En cada sector donde la empresa tiene un punto de acceso, también tiene asignado un segmento de red, destacando que no existe un subneteo, únicamente se utiliza porciones de red para los diferentes sectores. La máscara de la subred sigue siendo la de una clase B (16bits- 255.255.0.0).

2.1.2.2 Enrutamiento.

El enrutamiento se lo hace mediante rutas estáticas. El router construye su tabla de rutas en forma automática, no se utiliza protocolos de enrutamiento tales como BGP, EIGRP o RIP y se utiliza NAT (network addres traslation) para dar acceso a Internet a los usuarios de la red.

Para el enrutamiento no se hace necesario implementar protocolos de ruteo dinámico ya que posee una sola salida internacional y por defecto, un solo camino para enviar la información.

2.1.3 SERVICIOS

En esta sección se realizará una descripción de los servicios que actualmente brinda la empresa y se finalizará con el análisis de los mismos.

2.1.3.1 Web

La empresa ofrece servicio de Hosting, que permite almacenar diferentes dominios y páginas Web de diferentes clientes. Cada cliente posee una conexión FTP para acceder a los archivos WEB. Este permiso es asignado solo al “Web master” (administrador designado por el cliente) de la empresa. En la actualidad el servicio no está siendo utilizado, solo se brinda el hosting para almacenar cuentas de correo electrónico bajo un dominio propio. Todo el soporte para usuarios tanto de dominios

propios como de dominio de la empresa, lo da el departamento técnico de Gigowirless.

2.1.3.2 Mail

Para el servicio de mail se utiliza un servidor con plataforma Linux, los clientes pueden acceder a él mediante Outlook o Webmail. En este servicio se utiliza el protocolo SMTP (Protocolo Simple de Transferencia de Mensajería) para realizar el envío de información. La recepción de correos se lo hace mediante el protocolo POP (Post Office Protocol) usando el puerto 110. Todos los correos son almacenados en el servidor hasta cuando el usuario realice una conexión al mismo y los baje a su computador.

También el usuario puede revisar su correo mediante WEBMAIL, ésta es una interfaz WEB que permite acceder directamente al servidor para poder enviar y recibir correos electrónicos. Este servicio no es muy difundido por la empresa ya que los usuarios no bajan la información del servidor, consumiendo recursos de almacenamiento del disco, recurso que suele ser muy limitado. Además la empresa posee “dominios virtuales” donde los usuarios pueden crear cuentas bajo su propio dominio, por ejemplo: mi_correo@midominio.com

Cada dominio se crea con un espacio máximo en disco, esto quiere decir que para midomio.com se le puede asignar un espacio de 60MB.

2.1.3.3 DNS

La empresa cuenta con dos servidores de DNS (Domain Name Service), el primario se halla ubicado en el módulo de Core en la empresa y tiene una dirección IP real; el

secundario se halla ubicado en el proveedor de salida internacional y dispone de una copia de la base de datos de resolución de nombres del servidor primario.

2.1.3.4 Análisis de servicios

Una vez analizada la infraestructura, continuaremos con los servicio de la empresa. Empezando por el software de los servidores, no se los actualiza periódicamente ni existe una política de respaldos de información. Un ejemplo básico es la falta de respaldos de la información de los clientes, como sus páginas, cuentas de correo o configuraciones del servidor.

El hecho de poseer todos dentro del mismo servidor generaría inconvenientes. Al colapsar el servidor, colapsaría la red y sus servicios como: el correo electrónico, la navegación y el hosting. Una práctica buena sería tener no menos de dos dispositivos, uno para correo y otro para DNS y páginas Web. De esta forma se disminuirá el riesgo de dejar a la red sin servicios básicos, ayudando al mantenimiento de los mismos, especialmente cuando existan cambios que impliquen desconexión de la red o de la energía, la afectación será puntual.

Un inconveniente en las cuentas de correo es la falta de límites en los casilleros, esto genera que un cliente abuse del espacio de disco, dejando sin funcionamiento las cuentas de su propio dominio, ya que ha consumido todo el espacio asignado y los demás usuarios no podrían recibir correos.

2.2 ANÁLISIS DE REQUERIMIENTOS

Una vez realizada la descripción de la infraestructura de Gigowireless se centrará en el análisis de requerimientos para el diseño de una red que permita brindar acceso a Internet de forma Inalámbrica para el sector del CONDADO y que cumpla con requerimientos básicos de: rendimiento, disponibilidad, seguridad.

Las redes actuales de la empresa carecen de estas propiedades, por este motivo se trata de crear una metodología para el diseño e implementación de proyectos futuros. Además de centrarse en el análisis de requerimientos para el diseño del módulo de acceso y distribución (ya que la empresa cuenta con los demás módulos implementados), se realizará el análisis del entorno, para poder determinar la cantidad de equipos y su ubicación, esto indicará cuál deberá ser la topología de la red que se ajuste a los requerimientos del usuario.

2.2.1 CLASES DE USUARIOS

2.2.1.1 Usuarios Home

Son los usuarios de casa, que tienen un uso moderado de su canal de comunicaciones.

Dentro del conjunto residencial se tiene alrededor de 1200 casas, de las cuáles, el 50% posee Internet mediante ADSL o Dial-up. Existe un sector que no posee Internet Banda Ancha por falta de infraestructura de última milla, no existe tendido de cable coaxial o líneas telefónicas (ADSL). El 60% de los usuarios potenciales de casa se hallan interesados en utilizar el servicio mediante última milla inalámbrica, cuyas capacidades está sobre los 128Kbps. El tráfico más frecuente en usuarios de casa son, Navegación y consultas mediante páginas WEB, envío y recepción de correo,

trabajo en línea mediante programas como son Messenger, consultas y transacciones Bancarias, en menor medida desean descargar música y programas, usando utilitarios como lo son Lime Wire, Kazza, Ares entre otros, este tipo de tráfico deberá controlarse para no degradar el rendimiento de la red.

2.2.1.2 Usuarios Corporativos

Los usuarios corporativos se los localiza en el área comercial, en los locales del centro comercial del conjunto (CONDADO), como también en los sitios habitacionales. Este tipo de clientes necesitan usar el servicio para realizar transacciones bancarias, envío y recepción de correos, ya sea mediante servidores públicos (Hotmail, Yahoo) o privados (dominios propios son los mas usados).

2.2.2 ANÁLISIS DE TRÁFICO

Par el análisis de tráfico se ha implementado un computador con la aplicación MRTG, que permite sondear diferentes dispositivos y verificar el tráfico que está cursando por ellos. Para tener una idea real de las capacidades requeridas se ha tomado en cuenta usuarios actuales de la red y con esto datos se verificará cual es el uso efectivo de canal que el cliente realiza.

2.2.2.1 Protocolos requeridos.

Entre los protocolos requeridos para los usuarios está el uso de casilleros de correos usando POP en el puerto 110 y SMTP en el puerto 25, además el ISP proveerá el servicio de alojamiento WEB para los usuarios y dará acceso al servidor para

actualizar sus páginas mediante FTP. El tráfico http es el más utilizado por los usuarios para navegar en la WEB.

2.2.2.2 Capacidades requeridas.

Para el análisis de capacidades se ha tomado muestras de usuarios actuales (de casas y oficinas) durante un mes, para determinar el uso del ancho de banda. Identificando claramente los diferentes planes existentes tales como son 128/64, 256/128.

Canal 128/64, (usuario de oficina) este tipo de clientes tienen un uso de ancho de banda muy alto, porque poseen programas de descarga continua que saturan su canal. Se puede apreciar en las Figura 2.6 Tráfico diario y 2.7 que el uso del canal es: 80% del canal de bajada y 50% del canal de subida

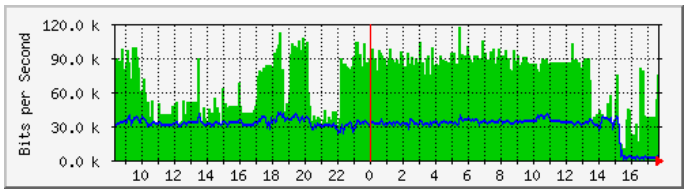


Figura 2.6 Tráfico diario

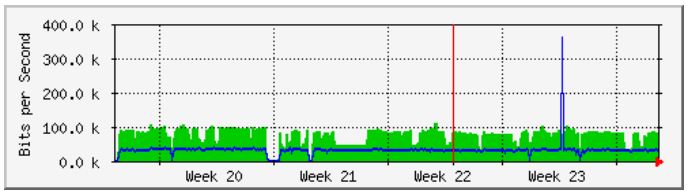


Figura 2.7 Tráfico Mensual

En las figuras 2.8 y 2.9 se puede apreciar el tráfico típico de un usuario doméstico. El uso de canal de este tipo de cliente es mediante ráfagas o por instantes, su comportamiento en el tráfico permite compartir el canal con más clientes y de este modo reutilizar los recursos de ancho de banda y contar con un negocio rentable. En las figuras 2.8 y 2.9 se puede observar que durante una semana, el pico más alto llega al 90% del canal de bajada y el canal de subida tiene un pico de 60%.

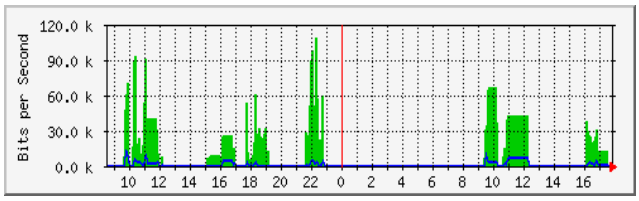


Figura 2.8 Tráfico diario

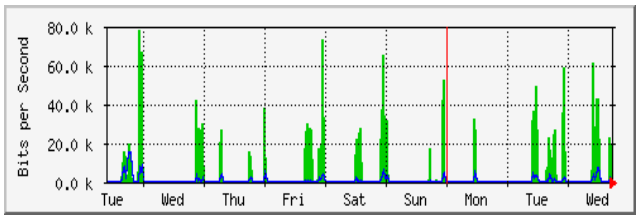


Figura 2.9 Tráfico Mensual

Plan 256/128, el cliente es una institución educativa que posee cámaras para vigilar a los niños en forma visual. Se puede observar en las figuras 2.10 y 2.11 que el uso de canal se inicia a las 9am y termina a las 14pm. Este tipo de comportamiento de tráfico no es perjudicial para el ISP ya que el canal de subida tiene un porcentaje de uso del 90%. Y el de bajada un nivel de uso del 14%.

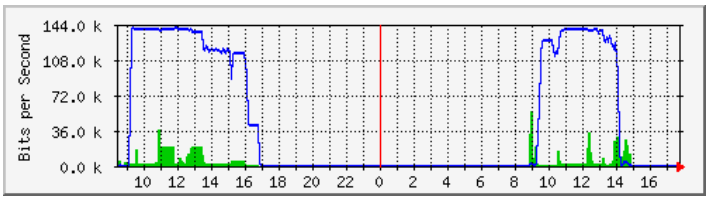


Figura 2.10 Tráfico Diario

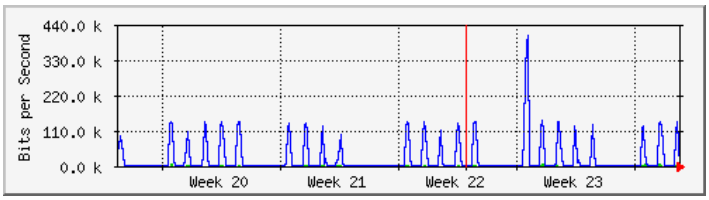


Figura 2.11 Tráfico Mensual

Usuario 256 corporativo, este cliente tiene un alto nivel de utilización, maneja 16 computadores internos, con un tráfico de correo tanto de subida y bajada, sus mensajes están compuestos por imágenes escaneadas. Se puede apreciar en la figura 2.12 que su horario de trabajo es de 8 de la mañana a 6 de la tarde. El canal de bajada tiene un uso promedio del 80% y el de subida de un 60%, con un tráfico continuo sin muchas ráfagas, este usuario consume una porción de canal constante.

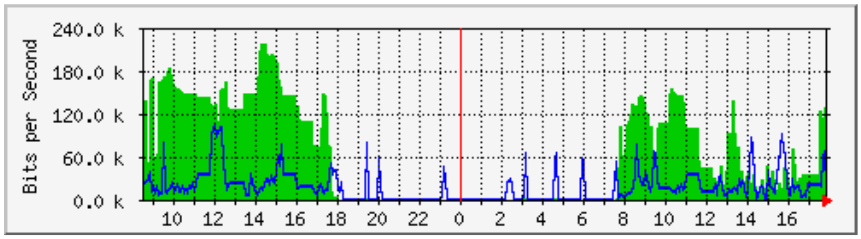


Figura 2.12 Tráfico diario

2.2.2.3 Dimensionamiento de capacidad según datos socio–económicos.

Según datos obtenidos en el Censo Poblacional realizado en el 2001, se obtiene los siguientes datos: existen 987 viviendas en la urbanización el Condado con un promedio de 4 habitantes por cada vivienda, el 89% tienen buena capacidad adquisitiva, dando como resultado un total de 878 viviendas como población objetivo. En este sector no existe niveles de pobreza extrema, todos satisfacen sus necesidades básicas, y, como dato adicional, el 90.9% de los habitantes tiene línea telefónica.

Considerando una población objetivo de 878 viviendas y utilizando el estudio de prefactibilidad realizado por la empresa, el cual determinó en un 20% la probabilidad de éxito en las ventas o requerimientos, podemos decir que nuestros futuros clientes se centran en 175 hogares.

Un requerimiento del CONATEL obliga que todo servicio de Internet para ser considerado de banda ancha deba disponer de por lo menos 256Kbps en el canal de bajada, obliga a la empresa a mantenerse pendiente en los planes de 128kps, que son mayoritarios y realizar el cálculo para las dos velocidades. En la Tabla 2.3 se puede observar un resumen de los cálculos realizados

			Compartición AB [Mbps]	
Hogares	**AB promedio[Kbps]**	**AB total [Kbps]**	**8/1**	**4/1**
175	256	44800	5,6	11,2
175	128	22400	2.8	5.6

Tabla 2.3 Cálculo de niveles de compartición

Se debe tomar en cuenta que la mayor cantidad de clientes son planes home, esto puede ayudar a identificar que el horario de uso del servicio va ha ser en la noche como hora pico y a partir de las tres de la tarde como hora inicial de carga de la salida internacional. Por las noches el canal de salida internacional se halla desocupado ya que los clientes que actualmente posee el ISP son corporativos.

Para los posteriores cálculos a realizar se tomará como capacidad mínima de los canales, 2.8Mbps y como máximo 5.6Mbps.

2.2.3 ANÁLISIS DE RENDIMIENTO Y DISPONIBILIDAD

Para el análisis de rendimiento y disponibilidad se tomará en cuenta la cantidad de usuarios potenciales que se podría tener y con esto, dimensionar el número de Access Point y su ubicación dentro del área a cubrir.

2.2.3.1 Áreas a cubrir

El área a cubrir es la urbanización “El Condado”. Para esto se realizará la verificación de usuarios potenciales. Se utilizará la herramienta Google Earth, Ozi Explorer, Radio Mobile, que permite tener fotografías satelitales de varios sectores del planeta.

Para realizar el análisis de cobertura se dividirá el área en sectores, las divisiones serán en forma horizontal, especialmente porque la urbanización se halla sobre una montaña y la topografía es irregular impidiendo que con un solo punto de acceso cubra totalmente el conjunto.

- **Sector 1**

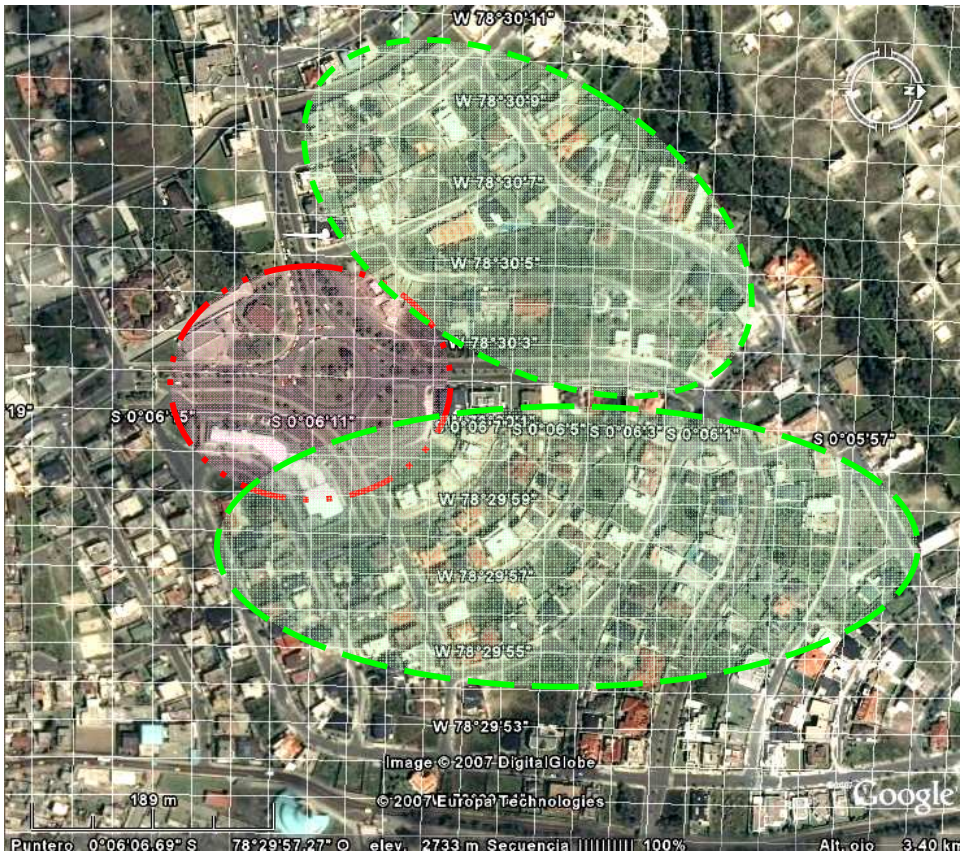


Figura 2.13 Sector 2.1

En este sector se ubica el área comercial (color rojo) y de recreación, también se encuentra usuarios residenciales (color verde), con un total aproximado de 400 casas. Este sector es el mejor abastecido de Internet por otros proveedores.

- **Sector 2**

Este sector es netamente residencial, con aproximadamente 300 casas. Los usuarios potenciales son domiciliarios.

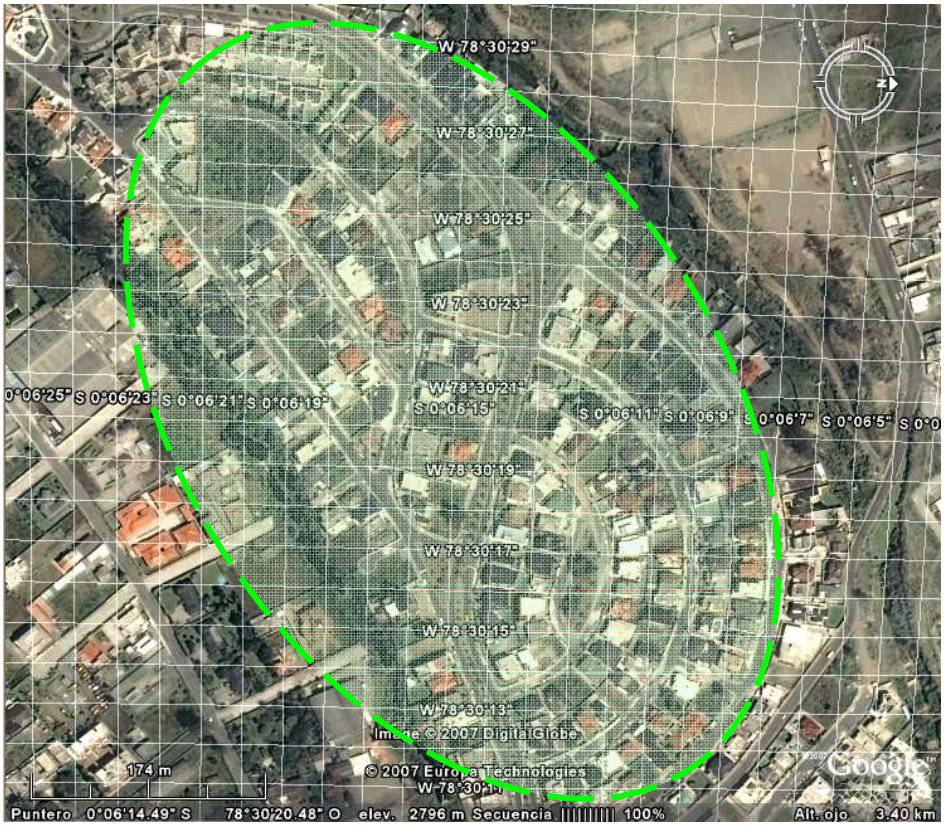


Figura 2.14 Sector 2.2

- **Sector 3**

Figura 2.15 Sector 2.3

Este segmento es de alto potencial para las ventas de nuestra empresa, no existen puertos para dar servicio ADSL y TV–Cable (empresa proveedora de internet) no dispone de infraestructura cableada para brindar sus servicios. Este sector se conecta al Internet mediante el servicio dial-up (teléfono).

2.2.3.2 Análisis del entorno

Para realizar el análisis del entorno se tomarán muestras de redes cercanas, niveles de señal y canales usados. Esto permitirá posteriormente decidir qué canales usar para implementar la red y no interferir con otras redes cercanas.

En el proceso de recolección de datos se utilizará el programa gratuito NetStumbler 4.0, que muestra las redes cercanas y sus niveles de "señal a ruido".

Para lograr este cometido se adapto a una tarjeta inalámbrica USB una antena externa que logrará captar una mayor cantidad de redes instaladas en el entorno. Para las pruebas respectivas, se acoplo una antena de 15dBi ommnidireccional a un dispositivo USB DLINK, permitiendo capturar mayor cantidad de señales.

2.2.3.2.1 Redes cercanas

Existen varias redes cercanas que se hallan con niveles de potencia bajos y que trabajan en modo infraestructura (ESS) y en modo ad-hoc (IBSS).

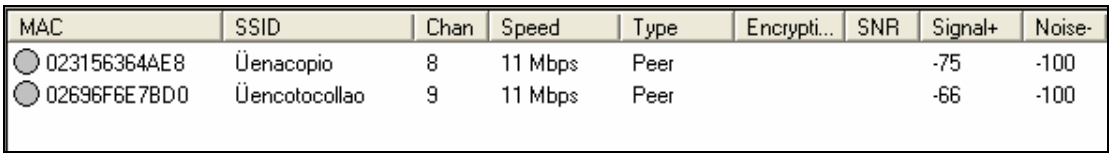
2.2.3.2.1.1 Redes en modo infraestructura (ESS)

MAC	SSID	Chan	Speed	Type	Encrypti...	SNR	Signal+	Noise-
00059E82F0D7	gig0_sena0	1	11 Mbps	AP			-78	-100
001150D4B1A2	belkin54g	3		AP	WEP		-80	-100
00059E82A4A1	Emap_t3g	11		AP	WEP		-66	-100
000D883CDD7F	Wireless	11	11 Mbps	AP	WEP		-59	-100
00179AD14F12	g1g0_c0linas	1		AP			-90	-100
0015E90CFE30	default	6		AP			-85	-100
0014BFAEE742				AP	WEP		-80	-100

Figura 2.16 Sondeo redes en modo infraestructura

En la Figura 2.16 se aprecia una lista de redes que se encuentran trabajando en modo infraestructura. Se encontró siete redes alrededor del sector a cubrir. Entre las redes encontradas en su mayoría son redes domesticas, además se pudo apreciar que la red con mayor nivel de señal es “g1g0_c0linas”, el resto contiene un nivel bajo de señal.

2.2.3.2.1.2 Redes en modo ad-hoc (IBSS)



MAC	SSID	Chan	Speed	Type	Encrypti...	SNR	Signal+	Noise-
023156364AE8	Üenacopio	8	11 Mbps	Peer			-75	-100
02696F6E7BD0	Üencotocollao	9	11 Mbps	Peer			-66	-100

Figura 2.17 Redes en modo ad-hoc

Las redes trabajando en modo ad-hoc son realmente pocas y son de la empresa Ecutel, que implementa una red de este tipo para tener una mayor cobertura y seguridad. En la Figura 2.17 se muestra la lista de redes encontradas.

2.2.3.2.2 Canales Usados

Entre los canales actualmente usados tenemos los siguientes:

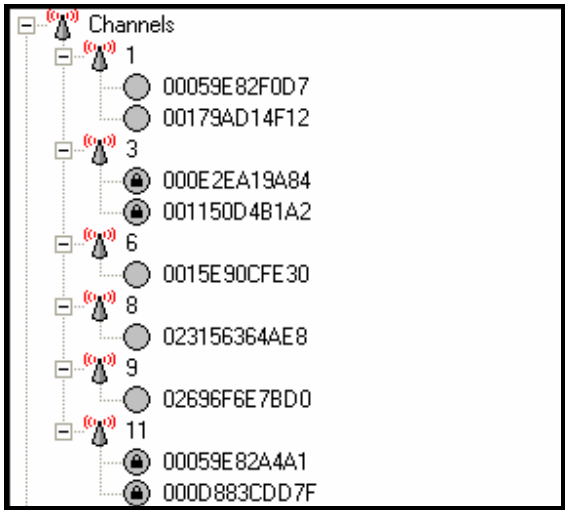


Figura 2.18 Sondeo de canales

En la Figura 2.18 se apreciar que los canales más usados son el 1, 3, 11 principalmente porque existen dos redes trabajando en las mismas. Además recordemos que para evitar la interferencia entre redes es necesario colocar en el canal 6 que se encuentra disponible.

2.2.3.2.3 Niveles de Señal

MAC	SSID	Chan	Speed	Type	Encrypti...	SNR	Signal+	Noise-
023156364AE8	Üenacopio	8	11 Mbps	Peer			-75	-100
00059E82F0D7	gig0_sena0	1	11 Mbps	AP			-78	-100
02696F6E7BD0	Üencotocollao	9	11 Mbps	Peer			-66	-100
00059E82A4A1	Emap_t3g	11		AP	WEP		-66	-100
000D883CDD7F	Wireless	11	11 Mbps	AP	WEP		-59	-100
0014BFAEE742				AP	WEP		-80	-100
00179AD14F12	g1g0_c0linas	1		AP			-90	-100
0015E90CFE30	default	6		AP			-85	-100
000E2EA19A84	Üenacopio	3	11 Mbps	Peer			-75	-100
001150D4B1A2	belkin54g	3		AP	WEP		-80	-100

Figura 2.19 Niveles de señal

Las redes encontradas en el sector del CONDADO llegan a un número de 10, con niveles de señal apreciables para la antena receptora del equipo de prueba. Entre las redes mas significativas son la red “wireless”, Uencotocollao y Emap_t3g, que tienen un nivel de señal relativamente alto, pero que no representa niveles de interferencia altos como para degradar la calidad de señal de una red que se implemente en la urbanización.

2.2.4 ANÁLISIS DE SEGURIDAD

Actualmente se tienen redes funcionado solo con WEP o WPA, sin ningún método de seguridad para facilitar el acceso al servicio. Según los resultados arrojados por el software Netstumbler se determinó que existen un notable número de redes sin ninguna seguridad.

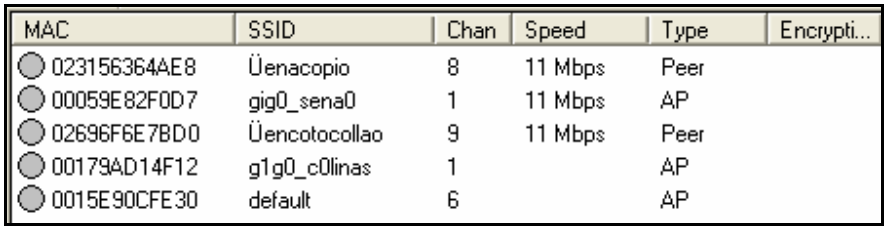
2.2.4.1 Redes con seguridad implementada

MAC	SSID	Chan	Speed	Type	Encrypti...
001150D4B1A2	belkin54g	3		AP	WEP
00059E82A4A1	Emap_t3g	11		AP	WEP
000D883CDD7F	Wireless	11	11 Mbps	AP	WEP
0014BFAEE742				AP	WEP

Figura 2.20 Sondeo de redes con seguridad

En la Figura 2.20 se puede revelar que existen redes con seguridad implementada y utilizan seguridad WEP como método de encripción.

2.2.4.2 Redes sin seguridad:



MAC	SSID	Chan	Speed	Type	Encrypti...
023156364AE8	Üenacopio	8	11 Mbps	Peer	
00059E82F0D7	gig0_sena0	1	11 Mbps	AP	
02696F6E7BD0	Üencotocollao	9	11 Mbps	Peer	
00179AD14F12	g1g0_c0linas	1		AP	
0015E90CFE30	default	6		AP	

Figura 2.21 Sondeo de redes sin seguridad

Existen varias redes sin seguridad de encripción, las redes Uenacopio y Uencotocollao se encuentran trabajando en modo ad-hoc, y se esta implementado un filtrado por MAC ya que cuando se intento realizar la asociación, no se tuvo éxito. g1g0_c0lias, es una red que tiene la empresa para enlazar al sector de Colinas del Norte y brindar acceso de Internet.

CAPÍTULO 3
DISEÑO

Se diseñará la red física y lógica la cual comprende los cálculos para los enlaces punto a punto y para la red multipunto. Se utilizará un software para medir los rangos de cobertura de los equipos. El diseño físico se basará en la arquitectura propuesta por CISCO SAFE.

En la siguiente sección se realizará el diseño de la parte de seguridad de la red tanto física como lógica y también se diseñará un sistema de autenticación. Se efectuará un análisis de los productos existentes en el mercado para finalmente llevar a cabo el análisis económico y legal del proyecto.

3.1 RED FÍSICA Y LÓGICA.

Se tomará en cuenta la arquitectura que propone CISCO SAFE. El diseño físico de la red dispondrá la distribución de los puntos de acceso, para cubrir la mayor área posible y que los niveles de señal aseguren tener una alta disponibilidad de la red.

El diseño físico usará el software EKAHAU para realizar una simulación sobre el área de cobertura que alcanza un punto de acceso, con este software se puede realizar ajustes de potencia e indicar qué tipos de antenas se debe utilizar.

3.1.1 MÓDULO DE DISTRIBUCIÓN

Este módulo comprende el enlace desde el punto central de la empresa hacia el lugar donde se desea colocar el HOT-SPOT.

Para realizar el diseño de este enlace, se tomará la localización física de los puntos en donde se encontrarán los nodos.

CONDADO

Latitud	:	0º 6’ 13.55” S
Longitud	:	78º30’ 14.13” W
Altura	:	2780 m
Altura de antena	:	35+2.50 m

El Punto Central, Gigowireless

Latitud	:	0º 6’ 0.25” S
Longitud	:	78º28’ 45.11” W
Altura	:	2838 m
Altura de antena	:	30 m + una torre auto sustentada de 12 m.

3.1.1.1 Topología

La topología a utilizar para este enlace es punto a punto, mediante esta se transportara los datos desde el Hot-spot hasta la red de salida a Internet, se debe tener confiabilidad de 99,999%.

3.1.1.2 Perfil Topográfico

El perfil topográfico permite verificar la línea de vista que se tiene entre una antena y otra. Para obtener estos datos se realizará un levantamiento topográfico, mapas con curvas de nivel o mapas digitales.

En este caso se utilizará el software “Radio Mobile” que permite obtener un perfil topográfico de los puntos a enlazar y ayuda en el cálculo de la zona de FRESNEL. La Figura 3.1 muestra el perfil que existe desde El Condado hacia Gigowireless con una distancia entre puntos de 2700 m.

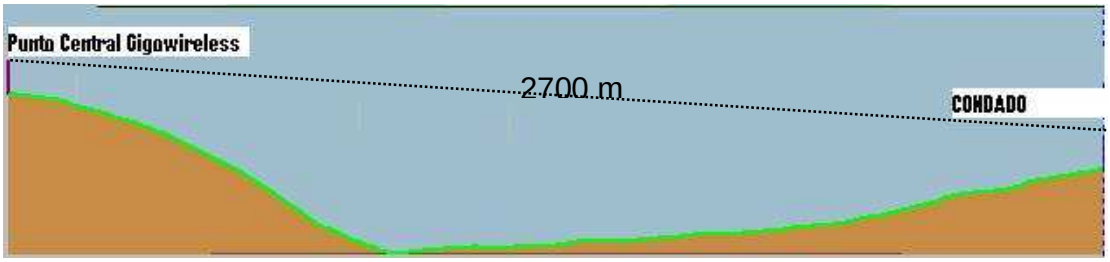


Figura 3.1 Perfil topográfico

3.1.1.3 Cálculo de primera zona de Fresnel

La primera zona de Fresnel permite establecer la condición de visibilidad entre las antenas, de forma que no existan obstáculos. Esto considera que la trayectoria no ha sido obstruida, por el contrario, de existir se tendría una pérdida en la potencia recibida. La energía debe estar concentrada cerca del rayo directo, de existir una obstrucción menor al 40% de la zona de Fresnel, se consideraría que no contribuye significativamente a la atenuación por difracción.

La forma para calcular es la siguiente:

$$R1 = \sqrt{\lambda \frac{d1 * d2}{d}}$$

$$\lambda = \frac{c}{f}$$

$$R1 = \sqrt{\frac{c * d1 * d2}{f * d}}$$

Donde:

R1 = radio de la primera zona de Fresnel (m).

d1 = distancia a un extremo del trayecto y el obstáculo (m)

d2 = distancia entre el receptor y el obstáculo. (m)

f = frecuencia (HZ).

El radio máximo se da cuando d1= d2, entonces la expresión se tiene como:

$$R1 = \frac{1}{2}\sqrt{\frac{c * d}{f}}$$

$$R1 = \frac{1}{2}\sqrt{\frac{3x10^{8}\ m/s * 2700m}{5.740GHZ}}$$

$$R1 = 5.93m$$

La zona prohibida es 0.6*5.93= 3.558 m.

3.1.1.4 Cálculo de Potencia Recibida.

Para calcular la potencia recibida se utiliza la siguiente ecuación:

$$Pr= Pt+ Gt + Gr – Lp -Lf- Lb$$

Donde:

Pt = Potencia del transmisor.
Gt = Ganancia del transmisor.
Gr = Ganancia del Receptor.
Lp = Pérdida por trayectoria en el espacio libre
Lf = Pérdida del alimentador de guías de onda
Lb = Pérdida total de acoplamiento.

Cálculo de pérdida por trayectoria en el espacio libre

$$Lp= 92.4+20 \log (f) +20 \log (d)$$

Donde:

f = frecuencia [GHZ]
d = distancia [Km.].
Lp = 92.4+20 log (5.740)+20 log (2700)
Lp = 116.21 dB

Pérdida en el alimentador de guías de onda: Es la pérdida en los cables (pigtails), según el fabricante indica que en un cable LM400 es 0.22 dB/m o si se utiliza RG-58 es 1 dB/m. En este caso se tomará el extremo que es 1 dB/m y la longitud del cable máximo 1 m.

La pérdida en los conectores y acopladores es de 0.1 a 0.5 dB, en total se tiene:

2*0.5 dB= 1 dB

Con los valores obtenidos se realiza el cálculo de la potencia en el receptor.

Pr= 15 dBm + 20 dB + 20 dB - 116.21 dB – 1 dB – 1 dB
Pr= -63.21 dBm.

Cálculo de margen de desvanecimiento

El margen de desvanecimiento permite relacionar con la confiabilidad del enlace, para obtener este dato se utiliza la fórmula de Bamett-Vigant:

$$FM = 30\log d + 10\log(6 * ABf) - 10\log(1 - R) - 70$$

Donde:

FM= Margen de desvanecimiento. [dB]
1-R=0.00001*d/400 →Objetivo de confiabilidad

d=Longitud de del trayecto [Km]

A=Factor de rugosidad:
4, si es terreno plano o agua
1, para un terreno promedio.
0.25, para un terreno rugoso.

B= Factor climático:
0.5 zonas calientes y húmedas.
0.25, zonas intermedias.
0.125, para áreas montañosas o muy secas.

f=frecuencia [HZ].

El margen de desvanecimiento es un factor de amortiguamiento en la ecuación de ganancia del sistema (Gs=Pt-Pr) que considera condiciones no ideales y que son difíciles de predecir, así como la propagación por múltiples trayectorias, sensibilidad a superficies rocosas, cambios climáticos, como son la temperatura y la humedad.

Para el cálculo se asumirá que A=0.25 y B=0.25 y se considerará un objetivo de confiabilidad del 99.999%=(1-R).

$$FM = 30\log(2.7) + 10\log 6(0.25 * 0.25 * 5.740) - 10\log\frac{0.00001 * 2.7}{400} - 70$$

FM=10.19dB.

Ahora se calculará la potencia recibida (Pr') pero se incluye el margen de confiabilidad:

Pr' = Pr-FM
Pr' = -63.21 dBm -10.19 dB.
Pr' = - 73.41 dBm.

Si se toma en cuenta que la sensibilidad promedio de un equipo está en - 80 dBm, se tiene que la potencia recibida luego de incluir el margen de desvanecimiento está dentro de los parámetros aceptables.

Restaría realizar el cálculo de la confiabilidad:

Tf = (1-0.99999)*365 días* 24 horas
Tf = 0.0876 horas/año.

Los datos obtenidos permiten definir las características de los equipos que se debe adquirir y se detalla a continuación:

Potencia del transmisor	=	15 dBm
Sensibilidad	=	-73.21 dBm.
Ganancia de las antenas	=	20 dBi
Frecuencia de trabajo	=	5.740 GHZ.

La capacidad del enlace, tomando en cuenta la sensibilidad de los equipos, indica que se encuentra en el rango de 6 Mbps a 54 Mbps cuando la sensibilidad está entre – 108 dBm y – 86 dBm respectivamente.

3.1.1.5 Simulación Mediante RADIO MOBILE.

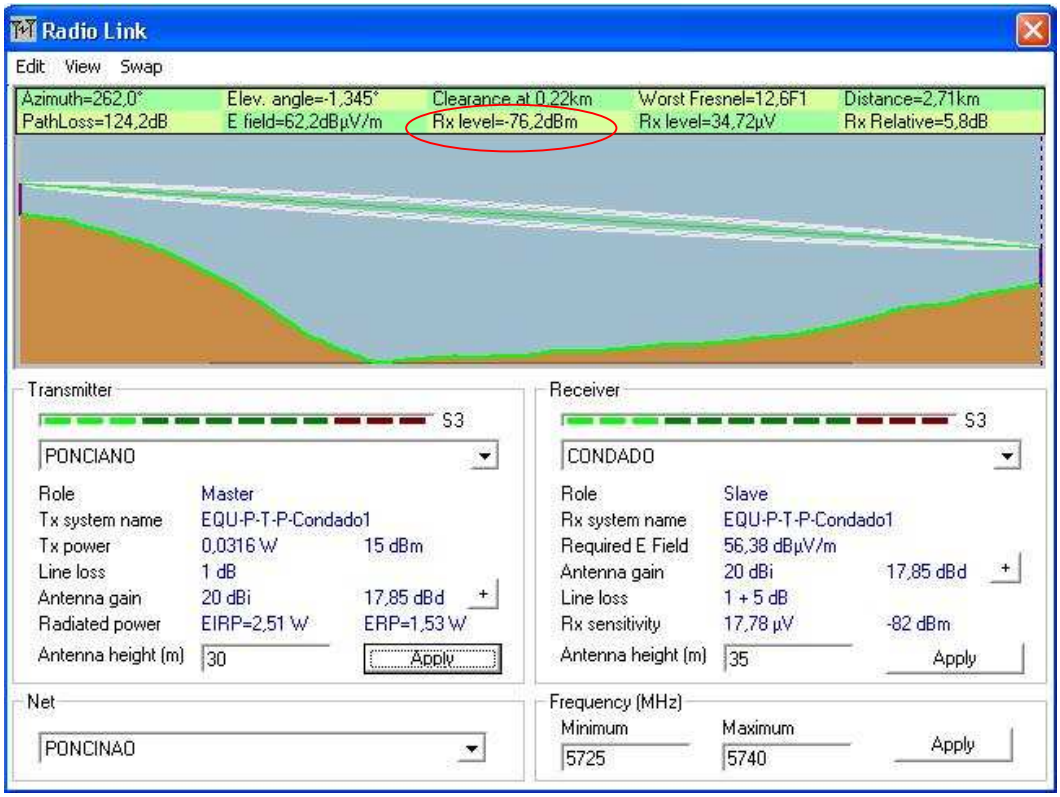


Figura 3.2 Simulación de radio enlace

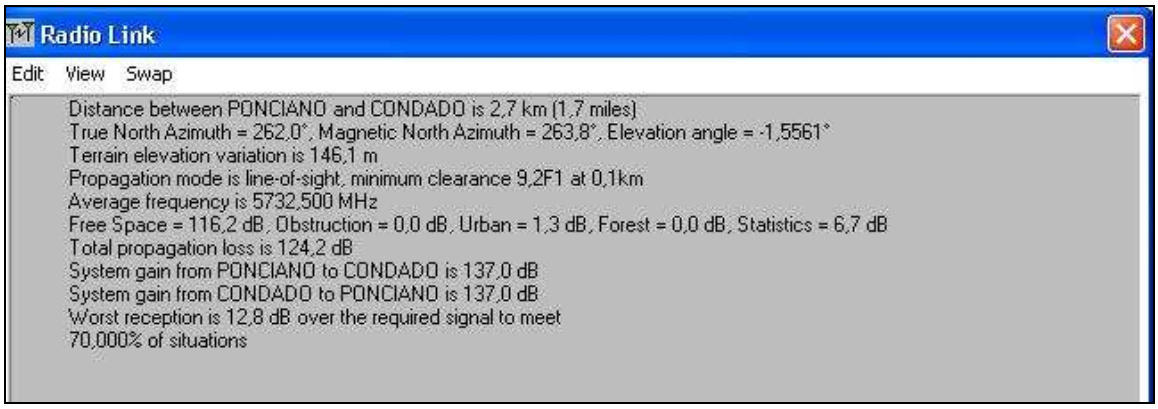


Figura 3.3 Resumen de resultados de simulación

En las Figura 3.2 y 3.3 se muestran los datos obtenidos en la simulación del radio enlace. El nivel de recepción calculado es de - 73.21 dBm y el de la simulación es - 76.2 dBm, estos datos son similares e indican que se puede confiar en la simulación realizada, la misma que advierte que el radio enlace tendrá un buen funcionamiento y cumplirá con los requerimientos de estabilidad y confiabilidad que exige el diseño.

3.1.1.6 Direccionamiento.

Se necesitan dos direcciones IP dentro de la misma red que funcione. Existen equipos a nivel de enlace que usan direcciones diferentes a las de los puertos que van hacia la red cableada. En el diagrama propuesto (punto 3.3.1) se realizará la asignación de direcciones.

3.1.1.7 Capacidad del enlace

Debe cumplir con los requerimientos que se especifican en el capítulo dos (punto 2.2.2.3), indicando el mínimo de capacidad de 2.8 Mbps y máximo 5.5 Mbps.

La capacidad del enlace tomando en cuenta la sensibilidad, podrá soportar hasta 6 Mbps. cuando la sensibilidad del equipo sea – 108 dBm y máximo 54 Mbps y pueda llegar a -86 dBm. Según los cálculos realizados la sensibilidad esta en - 65.68 dBm lo cual está dentro del parámetro de trabajo de los equipos.

3.1.1.8 Segmentación lógica

Una red WLAN genera gran cantidad de broadcast, además se verificó en el capítulo dos que la red actual no se halla subneteada, por esta razón el broadcast es alto y

contamina a los demás segmentos de red. Para disminuir los efectos de este problema, se deberá segmentar las redes, creando VLANs para cada enlace existente: Se incluirá en el módulo de distribución un switch de capa tres administrable; un puerto será designado en modo trunk para transportar la información hacia el ruteador principal y el resto se asociará una VLAN de acceso.

El principio de funcionamiento de las VLans es etiquetar las tramas, para lo cual se puede usar dos protocolos; Inter-Swuitch (ISL), que es propietario de CISCO u 802.1Q que es un estándar de IEEE.

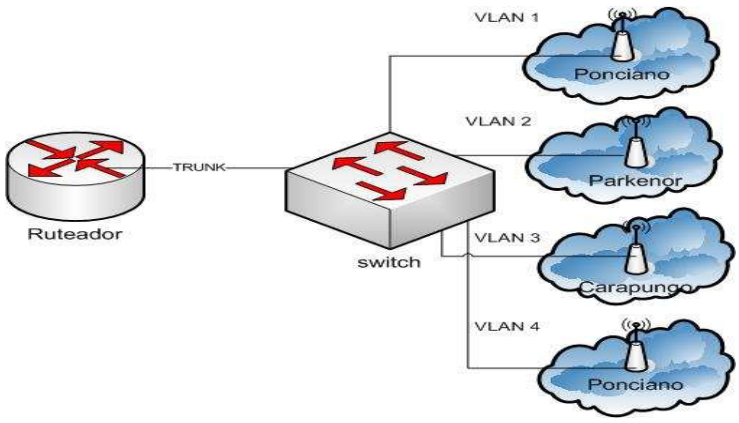


Figura 3.4 VLans

A continuación se presentan las diferentes Subredes para la empresa.

En la Tabla 3.1 se detallan la Vlan y puerta de enlace para los segmentos de red. La subred tomada para el Condado se puede verificar en el punto 3.1.3.4.

Sector	Subred	Puerta Enlace	Vlan
Condado	172.16.16.0/23	172.16.16.254	Vlan4
Carapungo	172.16.100.0/24	172.16.100.254	Vlan3
Parkenor	172.16.2.0/24	172.16.2.254	Vlan2
Ponciano	172.16.188.0/24	172.16.188.254	Vlan1

Tabla 3.1 Subredes

Se asignará a cada puerto del switch una VLAN, para aplicar listas de acceso y restricciones necesarias en la red. Una política es subnetear y de este modo activar diferentes segmentos de acuerdo a las diferentes necesidades de los clientes, evitando que un usuario coloque una dirección IP arbitraria diferente de la asignada y gane acceso a Internet.

Un problema importante a tomar en cuenta, es el bloqueo de los puertos de netbios, que permiten compartir los archivos y carpetas de los computadores del usuario, entonces se deberán bloquear los puertos 137-138-139 tanto TCP como UDP.

Otra medida de seguridad a tomar es usar filtrados MAC para un solo dispositivo se conecte en un puerto físico del switch, evitando que cualquier persona se conecte y tenga acceso a Internet.

3.1.2 MÓDULO ISP

Para el diseño de este módulo, se tomará en cuenta el ancho de banda que se requiere para dar acceso a Internet a los clientes. Se realizará el cálculo siguiendo la recomendación dictada por el CONATEL respecto a la “norma de calidad de servicio de telecomunicaciones”.

$$R \geq \frac{33kbps * n_{dial}}{20 * compartición} + \frac{\sum r_i}{\frac{noconmutadas}{compartición}} + \sum Rrt$$

Donde:

n_{dial} = número total de usuarios Dial UP.

$\sum_{noconmutadas} r_i$ = Sumatoria de de las tasas provistas a usuarios con canales compartidos

$\sum Rrt$ = Sumatoria de la capacidad de cada canal no conmutado no compartido

En este caso se tiene que:

Para servir a los usuarios de la red a implementarse en el Condado se necesitaría una capacidad total de:

Relación 8:1

Rmax > 256 * 175 / 8 Rmin > 128 * 175 / 8

Rmax > 5.6 Mbps Rmax > 2.8 Mbps

Relación es 4:1

Rmax > 256 * 175 / 4 Rmin > 128 * 175 / 4

Rmax > 11.2 Mbps Rmax > 5.6 Mbps

El ancho de bando deberá ser incrementado a medida que el número de clientes vaya creciendo.

3.1.3 MÓDULO DE ACCESO

3.1.3.1 Topología

Las topologías propuestas para este sistema son:

Red multipunto.- Mediante un equipo principal se conectarán varios clientes. El dispositivo utilizado para este propósito es un Punto de Acceso y deberá trabajar en modo infraestructura. La limitación de esta forma de trabajo es que se puede colocar máximo 3 repetidores, debido al número de canales disponibles y que no se hallan solapados. Cuantos más repetidores se coloque, el rendimiento de la red disminuirá ostensiblemente. Este sistema permite dar un nivel de redundancia promedio, que en el caso de tener dos repetidores, permite que las estaciones se conecten a otro punto de acceso cercano.

Red Mesh.- Las redes Mesh, o redes acopladas, se mezclan las dos topologías de redes inalámbricas. Básicamente trabajan con topología de infraestructura que también permiten unirse a dispositivos y, a pesar de estar fuera del rango de cobertura de los PA (personal adapters), aún se halla dentro del rango de cobertura de un TR, que directa o indirectamente, también se encuentra en el rango PA.

Las redes de malla son autoregenerables: En el caso de que algún nodo falle, el resto de nodos lo detectará, evitando el tráfico por él.

Una red mesh ofrece redundancia y fiabilidad superiores. En una topología en malla, cada equipo está conectado a todos los demás equipos. También son ventajas la

facilidad de solucionar problemas en la red y el incremento del nivel en la cobertura, por ello cobran mayor importancia el uso de Wireless.

3.1.3.2 Perfil topográfico

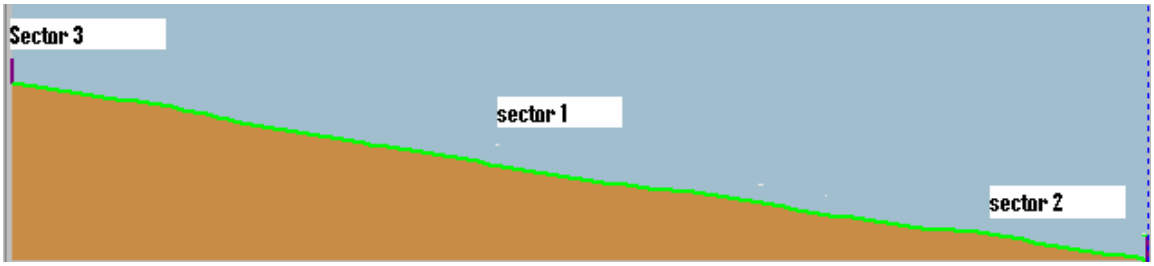


Figura 3.5 Perfil topográfico del condado

El ángulo de elevación del sector a cubrir es de 5.2º, la distancia es mas o menos 2km de la parte más alta al punto más bajo de la urbanización.

3.1.3.3 Diseño de enlace multipunto.

Para realizar el cálculo de la red multipunto (hot-spot), se recure a los modelos de propagación propuestos por “Okumura-Hata” (se expone en detalle en el Anexo B), los mismos predicen la perdida por trayectoria que una señal de RF pueda tener entre una estación base y un receptor, sea móvil o fijo. La ventaja de modelar radio canales teniendo en cuenta las características de la trayectoria entre Transmisor (Tx) y Receptor (Rx), es conocer la viabilidad de los proyectos que se deseen planear en determinados sectores, de esta manera se podrá hacer una estimación acerca de la necesidad, costos y capacidad de los equipos requeridos (especificaciones técnicas).

El desempeño de los modelos de propagación se mide por la veracidad de los resultados en comparación con medidas de campo reales. La aplicabilidad de un modelo depende de las especificaciones que este mismo requiera tal como son: el tipo de terreno (montañoso, ondulado o cuasi liso), las características del ambiente de propagación (área urbana, suburbana, abierta), características de la atmósfera (índice de refracción, intensidad de las lluvias), propiedades eléctricas del suelo (conductividad terrestre) y tipo del material de las construcciones urbanas. A continuación se detalla las expresiones usadas para realizar los cálculos para encontrar la potencia recibida en el equipo del cliente.

Para los cálculos realizados se ha tomado en cuenta las expresiones de “Okumura-Hata”, debido a que formula las perdidas por propagación de la siguiente manera:

$$\begin{aligned} L_{50}(dB)_{Hata} &= 69.12 + 26.16 \cdot log(f_c) - 13.82 \cdot log(h_{te}) + \\ &\quad - 3.2(log\,11.75h_{re})^2 + \\ &\quad + (44.9 - 6.55 \cdot log(h_{te})) \cdot log(d) - 2\left(log\left(\frac{f_c}{28}\right)\right)^2 \end{aligned}$$

Y el modelo de Okumura-Hata extendido” (cost), que se define con la siguiente expresión:

$$\begin{aligned} L_{50}(dB)_{Hata-Ext} &= 51.27 + 33.9\,log(f_c) - 13.82\,log(h_{te}) \\ &\quad - 3.2(log\,11.75h_{re})^2 + (44.9 - 6.55\,log(h_{te}))\,log(d) \end{aligned}$$

A continuación se define el coeficiente de Hata (CH) y de Hata Extendido (CHE), los mismos que ayudan a cuantificar el nivel de obstrucción del enlace.

$$\begin{aligned} CH(dB) &= L_{50}(dB)_{Hata} - PL \\ CHE(dB) &= L_{50}(dB)_{Hata-Ext} - PL \end{aligned}$$

Para el cálculo de atenuación de radio enlaces se utiliza las siguientes ecuaciones:

$$L_{TR\,Hata} = PL + (\%CH) \cdot CH\,(dB)$$

$$L_{TR\,Hata-Ext} = PL + (\%CHE) \cdot CHE$$

Los coeficientes de acuerdo al nivel de obstrucción se basan en la siguiente tabla:

MEnUF	%CO, %CH y %CHE
Obstrucción Leve (L)	10
Obstrucción Parcial (P)	30
Obstrucción Critica (C)	60
Obstrucción Grave (G)	90

Finalmente la potencia en el receptor se la obtiene mediante la siguiente ecuación.

$$Prx = Ptx + Gtx + Grx - Lp - Lf - Lb$$

Donde Lf y Lb, son pérdidas adicionales debidas a conectores y guías de onda, ponderará en 2dB.

d [Km]	fc [Hz]	htx [m]	hr [m	L50 Hata	L50HE	%ch, %ce	Gtx	Grx	λ	PL	CH	CHE	LH	LHE	PrxH [dBm]	PrxHE[dBm]	PrxSim [dBm]
0,05	2450	30	10	70,28	86	60	8	2	66,69	74,2	-3,9	12,05	72	81,39	-43,84	-53,39	-49
0,1	2450	30	10	80,89	97	60	8	2	66,69	80,2	0,7	16,63	81	90,16	-52,61	-62,16	-57
0,2	2450	30	10	91,49	107	60	8	2	66,69	86,2	5,29	21,21	89	98,93	-61,38	-70,93	-66
0,3	2450	30	10	97,69	114	60	8	2	66,69	89,7	7,97	23,89	95	104,1	-66,51	-76,06	-71
0,4	2450	30	10	102,09	118	60	8	2	66,69	92,2	9,87	25,79	98	107,7	-70,15	-79,70	-75
0,5	2450	30	10	105,51	121	60	8	2	66,69	94,2	11,3	27,27	101	110,5	-72,97	-82,52	-78
0,6	2450	30	10	108,30	124	60	8	2	66,69	95,7	12,6	28,48	103	112,8	-75,28	-84,83	-80
0,7	2450	30	10	110,66	127	60	8	2	66,69	97,1	13,6	29,50	105	114,8	-77,23	-86,78	-82
0,8	2450	30	10	112,70	129	60	8	2	66,69	98,2	14,5	30,38	107	116,5	-78,92	-88,47	-84
0,9	2450	30	10	114,50	130	60	8	2	66,69	99,3	15,2	31,16	108	118	-80,41	-89,96	-85
1	2450	30	10	116,11	132	60	8	2	66,69	100	15,9	31,85	110	119,3	-81,74	-91,30	-87
1,1	2450	30	10	117,57	133	60	8	2	66,69	101	16,6	32,48	111	120,5	-82,95	-92,50	-88
1,2	2450	30	10	118,90	135	60	8	2	66,69	102	17,1	33,06	112	121,6	-84,05	-93,60	-89
1,3	2450	30	10	120,13	136	60	8	2	66,69	102	17,7	33,59	113	122,6	-85,06	-94,62	-90
1,4	2450	30	10	121,26	137	60	8	2	66,69	103	18,2	34,08	114	123,6	-86,00	-95,55	-91
1,5	2450	30	10	122,31	138	60	8	2	66,69	104	18,6	34,53	115	124,4	-86,87	-96,43	-92
1,6	2450	30	10	123,30	139	60	8	2	66,69	104	19	34,96	116	125,2	-87,69	-97,24	-92
1,7	2450	30	10	124,23	140	60	8	2	66,69	105	19,4	35,36	116	126	-88,45	-98,01	-93
1,8	2450	30	10	125,10	141	60	8	2	66,69	105	19,8	35,74	117	126,7	-89,18	-98,73	-94
1,9	2450	30	10	125,93	142	60	8	2	66,69	106	20,2	36,10	118	127,4	-89,86	-99,42	-95
2	2450	30	10	126,72	143	60	8	2	66,69	106	20,5	36,44	119	128,1	-90,51	-100,07	-95

Tabla 3.2 Resumen de cálculos para red multipunto

En la tabal 3.2 se muestra los cálculos realizados mediante las expresiones expuestas en esta sección, también se ha creado una columna en la cual se ha tabulado los resultados que se refieren a la potencia recibida en diferentes sectores según el simulador “EKAHAU”, se realiza la comparación de los datos y se puede deducir que la simulación tiene un nivel de confiabilidad aceptable, permitiendo de este modo predecir el nivel de cobertura que la red dispondrá.

Los cálculos proporcionan información para verificar el tipo de equipos que se debe colocar como receptores a diferentes distancias. Por ejemplo se muestra que si “el punto de acceso” tiene una potencia de 100mw y se utiliza una antena de 8dBi se podría cubrir un área de 700m como máximo en teoría, considerando factores de atenuación críticos (%CH y %CHE, 60%). Esto debido a que si el receptor tiene una sensibilidad de -82dBm (tabla de referencia 3.3).

En la Tabla 3.3 se tiene una referencia de niveles de sensibilidad y la velocidad de trabajo en enlace para un equipo DLINK.

Receive Sensitivity (802.11b)
@ 8% PER (packet error rate)
- 11 Mbps: -83 dBm
- 2 Mbps: -89 dBm

Receive Sensitivity (802.11g)
Frame: 1000byte PDUs, @ 10% PER (packet error rate)
- 54 Mbps: -66 dBm
- 48 Mbps: -71 dBm
- 36 Mbps: -76 dBm
- 24 Mbps: -80 dBm
- 18 Mbps: -83 dBm
- 12 Mbps: -85 dBm
- 9 Mbps: -86 dBm
- 6 Mbps: -87 dBm

Tabla 3.3 Niveles de sensibilidad

En la Figura 3.6 Simulación de coberturase presenta la simulación realizada. Para esto se tomó en cuenta 3 puntos de acceso, ya que en el capitulo 2 se dividió el área de cobertura en tres sectores, por la irregularidad del terreno. También se considera el uso de 3 puntos de acceso por la capacidad de asociación, llegando a enlazar entre 60 y 70 clientes como máximo.

Los puntos de acceso se irán colocando según el requerimiento de clientes, el primero se colocará en el área central del condominio trabajando a modo de punto de acceso y los otros dos trabajaran a modo de repetidor. El canal de operación será el 11. Las antenas usadas son arreglos de paneles sectoriales de 8dBi con apertura de 120º y la potencia del transmisor es de 100mw.

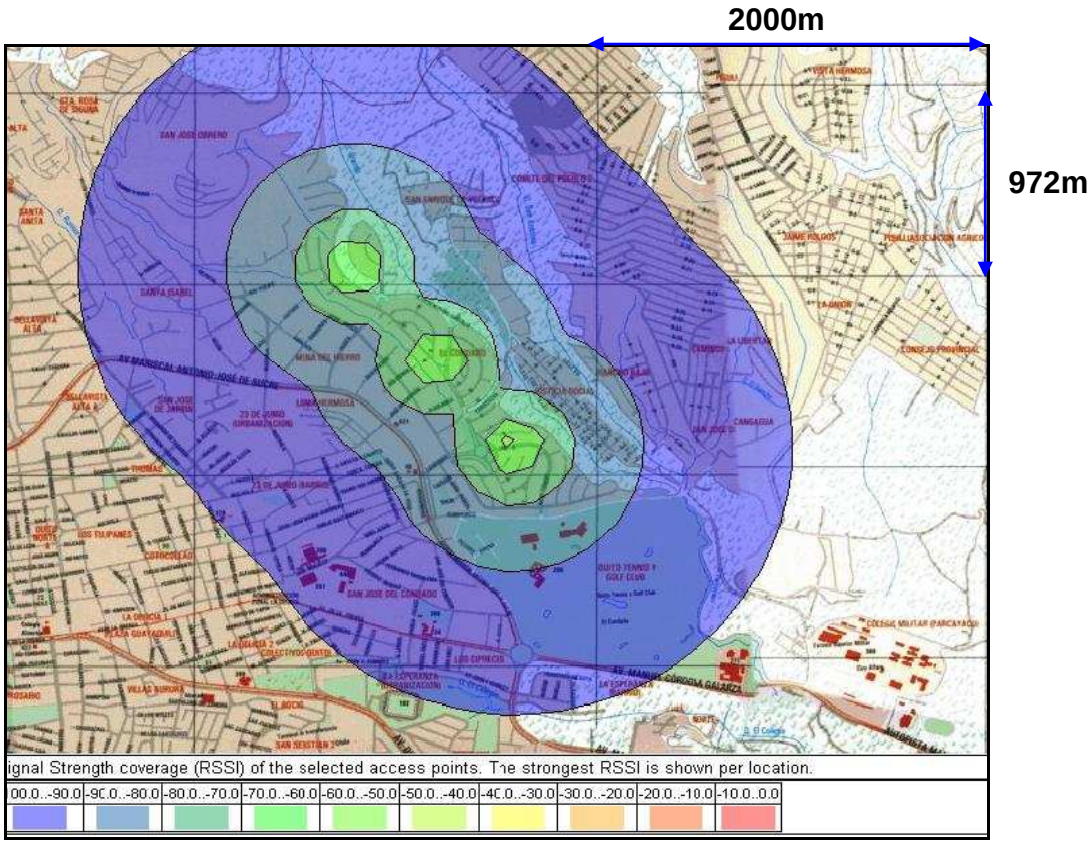


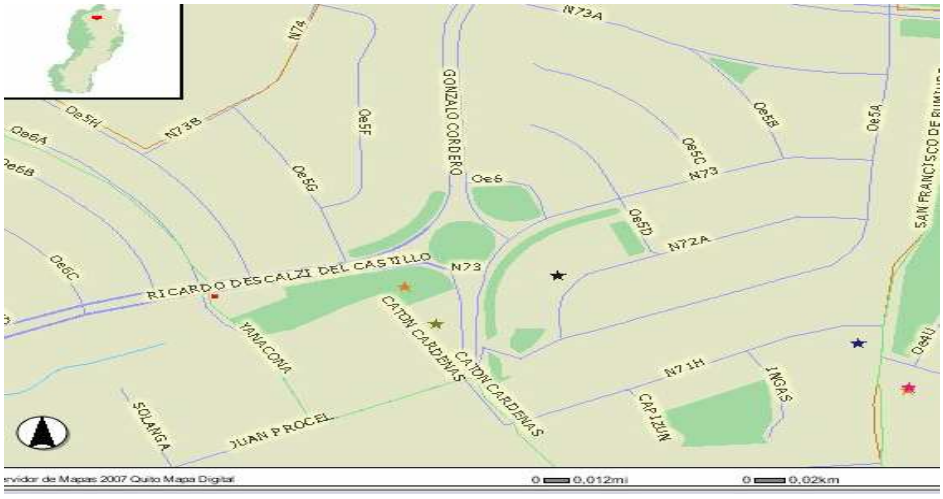
Figura 3.6 Simulación de cobertura

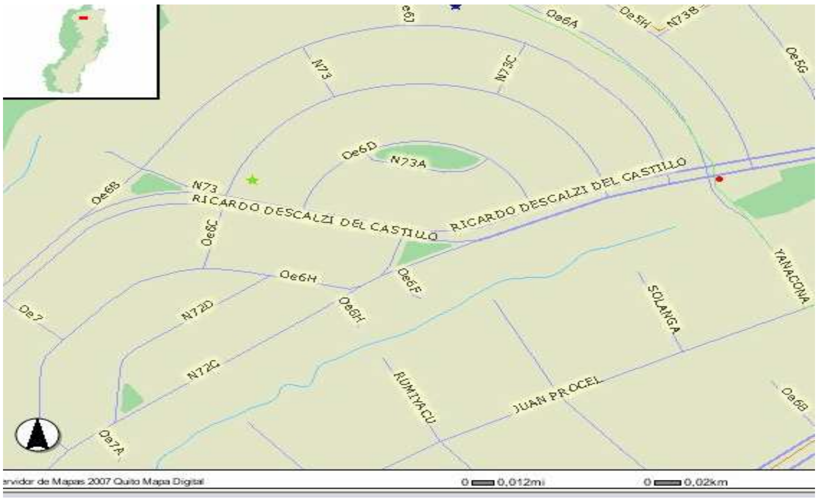
En el ANEXO C se presente el estudio completo de la red inalámbrica.

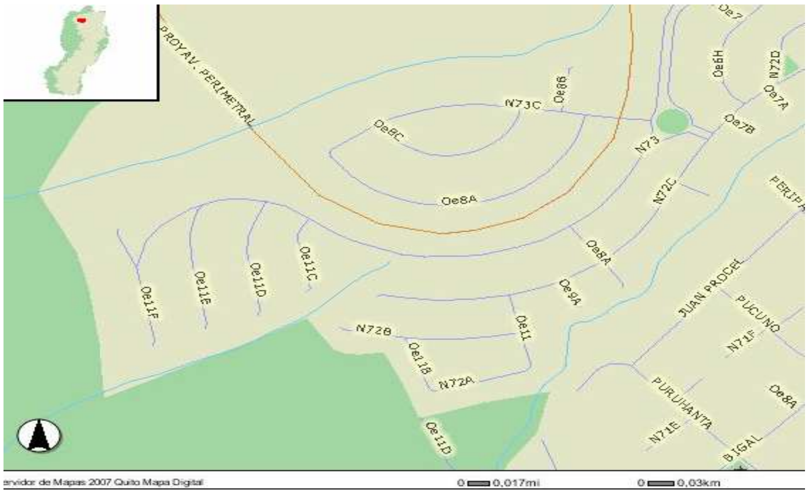
Mediante la simulación se puede planificar el área que se podrá cubrir, en la tabla se detalla el cálculo del área y se lo relaciona con la intensidad de la señal.

Sector	Ancho (Km)	Largo (km)	Área (Km^2)	Intensidad de señal (dBm)
Interno	1.728	0.585	1.01	-50 a -69
Externo	2.463	1.271	3.12	-70 a 79
Medio	3.980	2.727	10.85	-80 a -100

A continuación se presenta un mapa en el cual se visualiza las calles del sector del Condado, esto ayudará a tener una mejor visión del lugar donde se localizará el proyecto.




N73
Oe6D
N73A
N73C
Oe6A
Oe5K
N73B
Oe5G
Oe6B
RICARDO DESCALZI DEL CASTILLO
RICARDO DESCALZI DEL CASTILLO
Oe6C
Oe6H
Oe6F
Oe7
N72D
Oe6H
SOLANGA
YANACONA
N72C
RUMIYACU
JUAN PROCEL
Oe6B
Oe7A
ervidor de Mapas 2007 Quito Mapa Digital
0 0,012mi
0 0,02km


PROY.AV. PERIMETRAL
N73C
Oe8B
Oe8C
Oe8A
N73
Oe7
Oe6H
N72D
Oe7A
Oe7B
N72C
Oe11F
Oe11E
Oe11D
Oe11C
Oe8A
Oe9A
JUAN PROCEL
PUCUNO
N72B
Oe11
Oe11B
N72A
N71F
PURUHANTA
Oe8A
Oe11D
N71E
BIGAL
ervidor de Mapas 2007 Quito Mapa Digital
0 0,017mi
0 0,03km

3.1.3.4 Direccionamiento

Para realizar el direccionamiento de la red se utilizará direcciones IP privadas clase B, con una subred que abastezca el número de dispositivos.

Direcciones IP	
Detalle	Cantidad
PC Cliente	200
AP Cliente	200
Equipos de serv.	30
Total	430

Tabla 3.4 Direcciones IP

Caculo de Sub-red.

430 host +2= 432 →512 para satisfacer el requerimiento se necesita 9 bits. Para host y 23 para red.

- **La máscara a utilizar será 255.255.254.0.**

- **La subred a utilizar será 172.16.16.0 /23.**

Se toma en cuenta una dirección IP para el dispositivo inalámbrico y una para el computador del cliente con IP asociada a los recursos de ancho de banda contratado. Esto ayuda al monitoreo central y además puede dimensionar una dirección IP para cada dispositivo externo, ya que un clientes podría necesiten instalar el receptor externamente cuando se halle lejos del computador.

3.1.3.5 Clientes

Para que el cliente se conecte a la red se podrá hacer uso de tarjetas inalámbricas en los computadores o dispositivos externos como pueden ser AP en modo cliente con una antena de 2 dBi.

3.1.4 MÓDULO DE ADMINISTRACIÓN

Este módulo comprende la administración de los equipos y del ancho de banda de la red.

3.1.4.1 Monitoreo de Equipos de Red

El monitoreo de enlaces se lo hará mediante un software, que manejará el protocolo SNMP gestionando los equipos de la red y de usuarios. El software actual de la empresa es What'up (ipswitch), este permite realizar monitoreo mediante SNMP y crea una base de datos en SQL para almacenar la información obtenida.

Primeramente se creará una comunidad para el sondeo de los dispositivos, configurada al software y a los demás dispositivos a administrarse. También se configurarán los tiempos de poleo hacia los dispositivos. En la Tabla 3.5 se detalla el módulo y su tiempo de poleo.

Módulo	Tiempo
Distribución	1minuto
Core	1minuto
Acceso	10minutos
Servidores	1minuto

Tabla 3.5 Tiempos de poleo

Los tiempos a configurar están basados en el nivel de importancia de los dispositivos, por esta razón, se toma el tiempo de un minuto para el sondeo en los módulos de distribución Core y servidores, imprescindibles para el correcto funcionamiento de la red. Si uno de estos dispositivos quedara fuera de servicio, implicaría perdidas para la empresa y probables demandas legales de clientes.

3.1.4.2 Ancho de Banda

Para limitar el ancho de banda se utilizarán dispositivos especializados, considerando que Gigowireless no puede bloquear ningún tipo de tráfico. Por esta razón, no se puede realizar un bloqueo de paquetes de aplicaciones P2P, la forma de bajar el consumo de estas aplicaciones es marcar los paquetes para priorizarlos o encolarlos, de este modo se evitará el incremento de ancho de banda.

Uno de los inconvenientes que tiene el Gigowireless actualmente es que tiene demasiados planes para clientes, incumpliendo con los niveles de compartición ofrecidos. Una solución sería reagrupar a clientes de la siguiente manera:

3.1.4.2.1 Corporativos:

En estos planes se ubicará a las empresas que manejan normalmente una red interna y necesitan tener niveles de compartición menores, para este caso se tomará una compartición de 2 a 1 y 4 a 1, con mayor prioridad de salida a Internet. Los canales deberán ser simétricos ya que el tráfico que usan con frecuencia es el envío de correo electrónico

3.1.4.2.2 Home:

Son clientes domiciliarios que necesitan menor prioridad de salida, el nivel de compartición de estos clientes será de 8:1, sus canales también serán simétricos.

Requerimientos de la plataforma a usarse:

- **Ancho de banda máximo**

Es la cantidad de ancho de banda que deberá soportar el dispositivo. En la actualidad el Gigowireless tiene un ancho de banda de 3Mbps, a esta cantidad se deberá incrementar la capacidad a utilizarse en la nueva red del Condado, que según los cálculos es de 5.6Mbps (se toma la capacidad máxima para dimensionamiento).

- **Cantidad de conexiones,**

Habitualmente una plataforma puede mantener 64000 conexiones simultáneas, ya que esto tiene que ver con el número de puertos a manejarse.

- **Tipo y cantidad de interfaces**

Las interfaces que necesita el controlador de ancho de banda depende de la ubicación en la red (se puede ubicar en una red que maneje protocolos WAN). Para

las necesidades de Gigowireles se ubicará en una red que maneja interfaces fastethernet, con un mínimo de 2 interfaces de este tipo.

3.1.5 IMPLEMENTOS NECESARIOS PARA INSTALACIÓN DE NODOS INALÁMBRICOS

3.1.5.1 Sistemas de soporte

Tubos.- Si se opta por tubos, estos deben ser de perfil redondo y galvanizado. Ya que serán colocados en lugares altos, se instalarán tensores cada 3 metros, evitando su movimiento por la fuerza del viento.

Torres.- Se puede usar torres auto soportadas triangulares en tramos de 3 metros, con tensores cada dos tramos. Es preferible instalar torres auto sustentadas en lugar de tubos para facilitan el mantenimiento e instalación de nuevos.

3.1.5.2 Elementos adicionales

Figura 3.7Cajas Nema

Cajas Nema.- Este tipo de cajas protegen los equipos de los factores climáticos. Además sirven como medios de seguridad física de los equipos por la facilidad antirrobo que ofrecen.

Pigtails.- Permite el acoplamiento de la señal desde la antena hacia el equipo receptor, la distancia no debe ser mayor a un metro cuando se utilice cable LM-400 o RG-58. Los conectores más comúnmente usados son los de tipo, N y SMA

Figura 3.8 N-macho o Polaridad Reversa tipo N

En la Figura 3.8 se puede observar un conectar tipo N, este conector se puede utilizar con diferentes tipos de cable, RG8, WBC400, LMR400, Altelicon CA-400, Belden 9913, 7810

Figura 3.9 Conector SMA

El conector SMA se muestra en la figura 3.9, este conector se puede utilizar con diferentes tipos de cable, RG8, WC400, LMR400, Altelicon CA-400, Belden 9913.

Figura 3.10 Spliters

Estos dispositivos permiten realizar la división de señales para colocar múltiples antenas conectadas a un solo equipo. En estos dispositivos se toma en cuenta la frecuencia en la cual trabajan. Existen dispositivos para interiores y exteriores, en la se muestra un spliters para exteriores.

Figura 3.11 Protectores de Línea

Los protectores de línea sirven para evitar la realimentación hacia los equipos cuando existen descargas eléctricas, esto son dispositivos para exteriores. En la Figura 3.11 se puede apreciar dos tipos de conectores dependiendo de los equipos en los cuales se van ha utilizar.

3.2 SISTEMA DE SEGURIDAD.

Entre los problemas de seguridad hallados en el Capítulo 2 se encontró, que para conectarse a la red se utiliza encriptación WEP y la habilitación de direcciones IP dentro del controlador ancho de banda. Según CISCO SAFE WIRELESS indica que se debe proteger la red con la implementación de servidores AAA, sin perder de vista la seguridad física, ya que los equipos no están en lugares seguros y cualquier persona tendrá acceso a desconectarlos o robarlos.

3.2.1 SEGURIDAD FÍSICA

Una de las mejoras que se propone para el Gigowireless, es tener un cuarto de telecomunicaciones, el cual cumpla con las normas de cableado estructurado. Entre varios puntos que se debe tomar en cuenta para asegurar físicamente la infraestructura de la empresa tenemos:

- Aire Acondicionado, para mantener una temperatura de 17- a 20ºC
- Humedad, esta debe tener un rango de 40% a 60%
- Prevención, detección, suspensión y protección contra incendios.
- Alimentador de energía, generador de energía que se encienda de forma automática.
- Seguridad para acceso al cuarto de telecomunicaciones
- Seguro contra daños de equipos o robo.

- Etiquetación e inventario de infraestructura de red.

- Sistema de puesta a tierra adecuado.

- Pararrayos.

3.2.2 SEGURIDAD LÓGICA

- **Enlaces**

En los enlaces se utilizará la encripción del canal mediante WEP y además filtrado por mac-addres, Se utiliza estos métodos para enlaces punto a punto, de esta manera los equipos no permiten la conexión de más nodos al principal.

- **Puntos de Acceso**

a) En los puntos de acceso se deberá tener un sistema que permita autenticar clientes que se conecten a la red y se utilizarán listas de acceso para filtrar direcciones IP que se conectan a la red. Para la asociación de los dispositivos se utilizará WEP de 128bits.

b) Para autenticación se deberá usar un servidor central Radius que ayudará en la movilidad entre puntos de acceso o host-spots, este coordinará el acceso a la red mediante otro servidor con captive portal, el mismo que interactúa con un firewall para dar acceso y autorización a los servicios que el cliente requiere.

c) Se activará SNMP y el nombre de la comunidad con una clave de por lo menos 8 caracteres (números y letras), aplicando al SNMP solo permiso de lectura.

d) Se limitará el acceso de usuarios a la administración del equipo implementando ACL (lista de acceso), con una dirección IP de origen, permitiendo únicamente la entrada desde el módulo de administración y gestión con base a claves de usuario.

e) Habilitar el broadcast SSID. Esta opción no es recomendable en redes privadas, pero pera redes públicas es una elección acertada, ya que se puede anunciar la presencia de la red en un sector y permitir el acceso a ella.

- **Enrutadores**

a) Los enrutadores deberán tener diferentes niveles de usuarios; los que acceden al monitoreo y los que tienen acceso a modificar la configuración del equipo.

b) Se deberá realizar listas de acceso, que limitará el acceso de redes diferentes a la propia de la empresa.

c) Es necesario deshabilitar el acceso mediante http, (que facilita el ataque al equipo y su configuración) y reemplazarlo por HTTPS. Si se opta por usar acceso mediante línea de comandos (que incrementa el nivel de conocimiento del sistema, a un probable atacante) se recomienda usar SSH y no telnet, para que la información viaje encriptada, asegurando que no sea capturada en el camino.

d) Los puertos físicos no utilizados, deberán estar administrativamente deshabilitados.

e) Habilitar la encripción de todas las claves que se guardan en el router. Esta medida permitirá que al momento de mostrar la configuración, no se indique en texto claro las claves para los diferentes niveles de acceso.

- **Switches de capa 3.**

Los switches de capa 3 permitirán administrar las diferentes redes que se interconectan a la red de distribución. Además la microsegmentación de la red reduce el tamaño de los dominios de colisión y por ende las colisiones. La microsegmentación se implementa a través del uso de puentes y switches.

a) Se configurará el ancho de banda de cada puerto, dependiendo a quien este sirviendo, para el caso de servidores, se dará prioridad más alta de acceso y mejor ancho de banda.

b) Se implementarán las VLAN que combina la conmutación de Capa 2 y las tecnologías de enrutamiento de Capa 3, limitando los dominios de colisión como los dominios de broadcast. También ofrecen seguridad en la creación de grupos y permitiendo la comunicación entre ellos mediante un router. Por esta razón se realizarán Vlans para las diferentes redes que tienen el sistema.

- **Servicios:**

- Los servidores instalados responderán solo a los servicios necesarios ofrecidos a los usuarios (DNS, FTP, HTTP, POP, SMTP).

- Crear varios niveles de usuarios, para administración y monitoreo.

- Crear una DMZ (zona desmilitarizada), que permitirá separar los servidores, de los segmentos de red actuales y dar seguridad a la información que estos contienen.

- Establecer un servidor de Logs para almacenar información continua de posibles violaciones a la seguridad.

- Realizar respaldos permanentes (una vez al día), tanto de configuraciones como de información de los servidores; respaldo de correo electrónico y páginas WEB de los usuarios.

- Para los servidores de correo se deberá limitar el espacio de almacenamiento en disco hasta de 10MB para usuarios.

- Implementar un sistema anti SPAM y anti virus, que permita revisar el contenido de la información enviada y evitar el colapso de la red por inundación de “correo no deseado” o por envío de virus.

- Cada casillero de correo y acceso a la administración de los dominios deberá contener una clave y contraseña que permita acceder a los recursos asignados.

- Se deberá limitar el uso de disco de un dominio Virtual que se almacena en un servidor, se realizará una asignación de cuota en disco.

- **Clientes**

Para acceso a Internet se proveerá al cliente de un usuario y clave de acceso, esto permitirá su desplazamiento por varios nodos de la red sin necesidad de reinstalar el servicio.

3.3 SISTEMA DE AUTENTICACIÓN.

Para la autenticación de los usuarios se utilizará un servidor RADIUS, acompañado de un CAPTIVE PORTAL de creación de cuentas. A este sistema se deberán incorporar los nodos existentes de la red actual de GIGOWIRELESS.

Una ventaja del sistema abierto es el brindar servicio por horas, aprovechando el canal en momentos de bajo tráfico, por ejemplo en horario nocturno.

A continuación se muestra un esquema de infraestructura necesaria para poner en funcionamiento el sistema de autenticación.

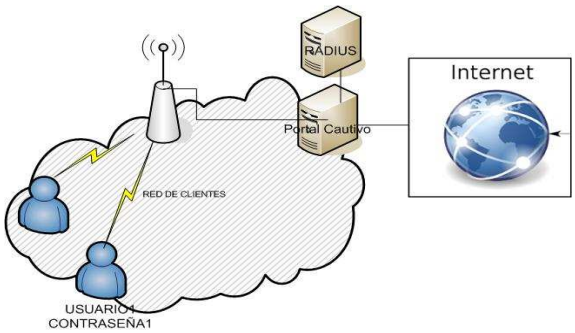


Figura 3.12 Esquema de un Portal Cautivo

Cada vez que un usuario desee acceder a la red deberá autenticarse en el sistema y se desplegará una pantalla como se muestra a continuación.

Esta pantalla se comunica con un servidor radius, el mismo que autentica al usuario, luego de lo cual intercambia información con un firewall y este habilita los servicios

requeridos por el cliente y el ancho de banda contratado.

3.3.1 ESQUEMA PROPUESTO

El esquema propuesto para el diseño se basa en la arquitectura sugerida por CISCO y que responde a los requerimientos encontrados en la fase de análisis y diseño. Se presenta una propuesta de la red íntegra de Gigowireless, agrupando los dispositivos en los diferentes módulos encontrados en el capitulo 2.

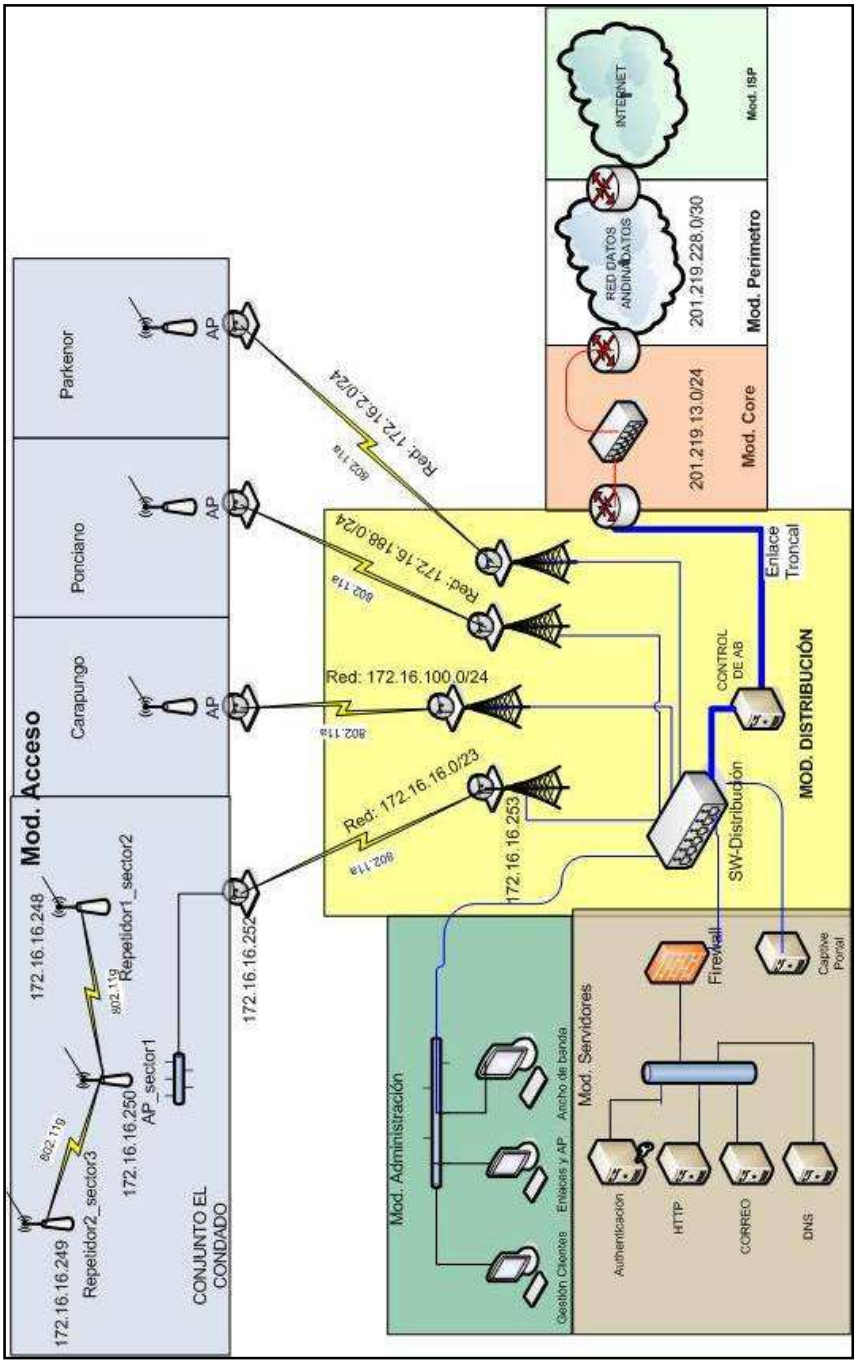


Figura 3.13 Esquema propuesto

3.4 PRODUCTOS EXISTENTES EN EL MERCADO.

Entre los Productos más usados para los enlaces tenemos los siguientes:

3.4.1 PUNTO A PUNTO

Se comparará varios parámetros de las siguientes marcas

Marca	**MTI** **BR58-11b**	**Proxim** **Tsunami 45**
Interfaces	Fasth Ethernet, 802.3u Wireless: 802.11a	
Seguridad	WEP/WPA/MAc filtering	WEP
Administración	http, Telnet, SNMP	http, Telnet, SNMP
Frecuencia de trabajo	5.15-5.85GHZ	5250-5350 MHz
Sensibilidad	-68dBm@54Mbps -76dBm@36Mbps -84dBm@18Mbps -87dBm@9Mbps -88dBm@6Mbps	-79dBm
Modo de Trabajo	Bridge	Bridge
Potencia de transmisión	17dBm@54Mbps 18dBm@48Mbps 20dBm@36Mbps~6Mbps	13dBm mínimo
Antena	Tipo panel de 23dbi, Flat Panel. Frecuencias: 5.3-5.8GHZ Angulo de apertura: 11º tanto en horizontal como vertical	
Costo	1400	2200

Tabla 3.6 Comparación de equipos punto a punto

De acuerdo a las características requeridas para el enlace, se tomará como opción los equipos MTI, debido a su bajo costo y alta confiabilidad, además este equipo puede elegir uno de los 14 canales disponibles en el equipo. Los equipos Proxim solo tienen un canal para conectarse, eso hace que tengan limitaciones para sortear interferencias.

3.4.2 RED MULTIPUNTO

La red multipunto comprende el punto de acceso principal y los equipos para el cliente.

3.4.2.1 Punto de acceso

Características	**Netkrom AIR-BR500G**	**SENAO-NOC-3220**
Potencia	AIR-BR500G: 20dBm AIR-BR500GH: 23dBm AIR-BR500AG: 20dBm	25dBm@1~24Mbps 23dBm @ 36Mbps 21dBm @ 48Mbps 20dBm @ 54Mbps
Sensibilidad	-90dB@6Mbps, -89dB@9Mbps, -87dB@12Mbps -85dB@18Mbps, -82dB@24Mbps, -79dB@36Mbps, -76dB@48Mbps, -74dB@54Mbps	-88dBm @ 6Mbps -70dBm @ 54Mbps
Velocidades	54, 48, 36, 24, 18, 12, 11, 5.5, 2, 1Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24,36, 48, 54 Mbps
Rango de cobertura	16 Km	5Km
Seguridad	WEP 64/128/152 - bit Filtrado de MAC.	IEEE802.1x WEP, WPA / Pre Share

	IEEE802.1x TLS, TTLS, PEAP WPA-PSK WPA-EAP, WPA2	KEY (PSK)/ TKIP Filtro de MAC
Frecuencia	2.400 ~ 2.497 GHz	2.400 ~ 2.497 GHz
administración	SNMP, WEB	WEB
Costo	299	202.36

Tabla 3.7 Comparación de equipos multipunto

Los equipos Netkrom son equipos para funcionar en ambientes de un ISP y recomendados para esta función. Además cumplen con los requerimientos que en el diseño fueron expuestos. Su costo es relativamente alto pero tiene mejor desempeño y garantía de parte del fabricante.

3.4.2.1.1 Antenas

Para implementar los nodos se utilizarán un arreglo de tres antenas sectoriales de la marca HYPERLYNK, los paneles podrán ser direccionables dependiendo de la topografía del terreno.

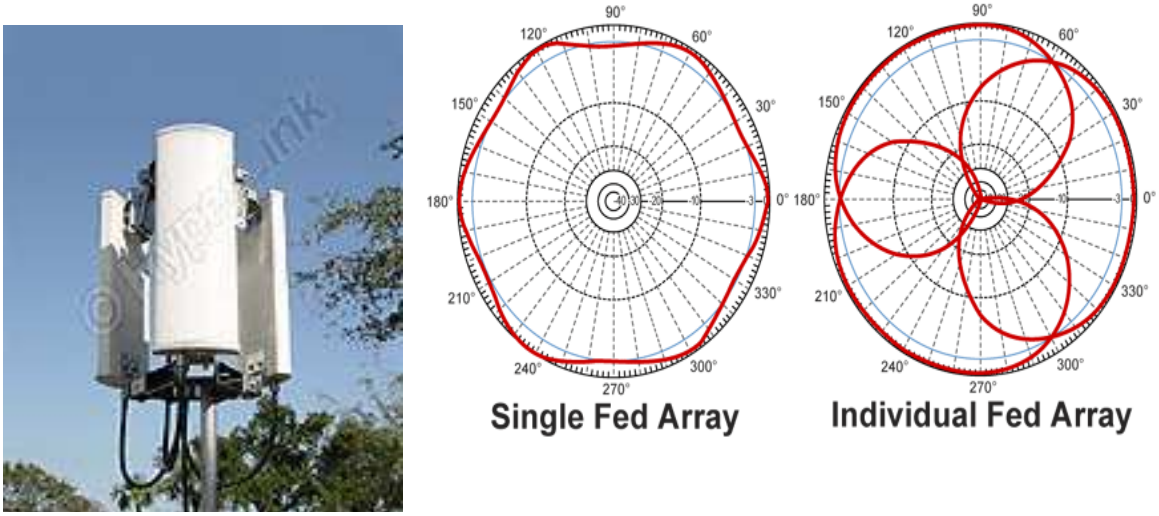


Figura 3.14 Arreglo de paneles

Características

Ganancia:	14 dBi
Frecuencia:	2400-2500MHZ
Ángulo de apertura horizontal:	120
Ángulo de apertura vertical:	15
Rango de potencia:	25 w
Montaje:	Se puede montar sobre estructuras metálicas.
COSTO=	550 dólares

3.4.2.2 Clientes

Los equipos a usar para clientes son de varios tipos, pudiendo ser tarjetas PCCARD, o USB, PCI o finalmente AP en modo cliente.

Características

	DLINK DWL-G132	**NETGEAR WG111**
Estándar	• 802.11b • 802.11g	802.11b • 802.11g
Velocidad	802.11b: 11, 5.5, 2 y 1Mbps 802.11g: 108, 54, 48, 36, 24, 18, 12, 9 y 6Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
Seguridad	WEP 64/128bit WPA-Personal WPA-Enterprise (includes 802.1x)	WEP, WPA, 802.11x
Cobertura	Indoors: 100m Outdoors:400m	Indoors: 100 Outdoors: 450m
Sensibilidad	-82dBm, 11Mbps -87dBm, 2Mbps -88dBm, 6Mbps -86dBm, 9Mbps -84dBm, 12Mbps -82dBm, 18Mbps -78dBm, 24Mbps -74dBm, 36Mbps -69dBm, 48Mbps -66dBm, 54Mbps	82dBm
Potencia de	15dBm@ 8Mbps	

transmisión	16dBm @ 36Mbps 17dBm @ 24, 18, 12, 9 y 6Mbps	
		
COSTO	55	50

Tabla 3.8 Comparación de equipos para cliente

Los clientes podrán conectarse a la red con cualquier tipo de tarjeta inalámbrica, tomando en cuenta que las Laptops ya vienen provistas de ellas, esto reducirá el costo de instalación del servicio. En el caso que un usuario necesite instalación de un equipo externo para conectarse a la red, lo hará mediante un AP en modo cliente. La diferencia con las redes que se hallan implementadas actualmente está en que se puede usar la misma antena que incluye el equipo cuya ganancia es de 2dBi.

3.4.3 CONTROLADORES DE ANCHO DE BANDA

En el Mercado existen varias soluciones para controlar el ancho de banda como el sistema operativo Linux, controladores mediante plataforma CISCO. Hardware y software especializado como PACKETEER o LINUX.

3.4.3.1 LINUX

Linux ayuda al control de ancho de banda mediante técnicas de encolamiento tales como CBQ, que presenta la capacidad de otorgar el ancho de banda requerido por cada clase en un intervalo de tiempo especificado, si hubiera demanda del mismo. Esto se logra mediante un mecanismo similar al utilizado por los “delay_pools” de Squid para limitación de ancho de banda de proxy HTTP, aplicando esperas entre las transferencias de paquetes. En segunda instancia, CBQ permite que las clases tomen prestado ancho de banda no utilizado por otras clases.

El QoS es implementado por un mecanismo de encolamiento. El encolamiento maneja la manera en que los paquetes están esperando por su turno para salir de la interfase, siempre trabaja sobre la interfase de salida, las disciplinas de encolamiento controlan el orden y velocidad de los paquetes que están saliendo a través de la interfase; adicionalmente define cuales paquetes deben esperar por su turno para ser enviados fuera y cuales deben ser descartados.

Las disciplinas de encolamiento pueden ser clasificadas dentro de 2 grupos por su influencia en el flujo de datos – schedulers y shapers

- **Tipo Scheduler**

Reordena el flujo de paquetes. Este tipo de disciplinas limita los números de paquetes sin degradar la velocidad. Se puede hacer colas tipo FIFO, RED, SFQ PFIFO y BFIFO son del tipo FIFO (First-in-First-out) colas con un buffer pequeño. La disciplina de FIFO no cambian el orden del paquete, ellos justamente acumulan los paquetes hasta que un límite definido es sobrepasado. Cuando la interfase va a mandar un paquete, el FIFO regresa el menos reciente (el que arribó primero),

PFIFO se limita por el número de paquetes mientras que colas BFIFO está limitada por conteo de bytes.

RED (Random Early Detect, también conocido como Random Early Drop), no limita la velocidad, pero cuando el canal esta lleno, lo hace indirectamente ecualizando las velocidades de los usuarios En una longitud promedio de cola “red-min-threshold” , RED empieza a “descartar” paquetes aleatoriamente con un incremento lineal de la probabilidad, hasta que el promedio de la longitud de la cola alcanza el tamaño “red-max-threshold”. Este es el promedio del tamaño de la cola, es calculado por el tamaño efectivo de la cola en un instante y es mayor que el parámetro “red-max-threshold”. Es posible especificar un límite para el tamaño de la cola con la propiedad “red-limit”.

- **Tipo Shaper**

Controlan la velocidad del flujo de datos. Adicionalmente pueden hacer un trabajo programado. La cola que se utiliza en este caso es PCQ (Per Connection Queue), la cual permite escoger clasificadores (uno o más de src-address, dst-address, src-port, dst-port), no limita el número de subflujos. Puede controlar cuantos paquetes son guardados por la cola con el parámetro “pcq-limit”, es posible limitar la máxima velocidad dada a cada uno de los subflujos actuales.

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

	Características	Costo
STICK GATE.	Control de ancho de bando por IP, o MAC. Reportes de clientes, firewall incluido. Instalación del software sobre Linux,	600
Mikrotik	Controlador de ancho de banda, router, hotspot. Control de flujo tanto inbound como outbound, clasificación por Ip, Mac o subredes. Y manejo de tráfico WAN y LAN. Manejo de redes ATM, Frame Relay.	250

Tabla 3.9 Comparación de controladores de ancho de banda

3.4.3.2 Ruteadores CISCO.

Este tipo de routers permite realizar la clasificación de ancho de banda mediante los siguientes mecanismos:

Shaping and Policing.- Este mecanismo permite tomar acciones sobre violaciones a la regla de tráfico, Si aplicamos Shaping este retarda el trafico mediante el encolamiento y polycing permite tomar acciones como el descarte de paquetes.

Traffic Policing.- Trabaja en una interfaz controlando el ancho de banda tanto de subida como de bajada usando tocken buckent, esta técnica se podría utilizar para limitar los enlaces de la red de distribución.

Traffic shaping, únicamente controla el tráfico saliente de una interfaz Los Routers CISCO que permiten tener esta funcionalidad son los de las series 7500 y actualizados el IOS del router se puede implementar las series 2500 y 3500.

ROUTER CISCO 2500	Este router cuenta con 2 interfaces seriales y 2 interfaces Fast Ethernet, incluye versión de IOS 12.3 (8r) T8, tiene la funcionalidad de controlar ancho de banda de acuerdo a los mecanismos expuestos en este item.
Costo	2400

3.4.3.3 PACKEETER

Este sistema es muy importante y se especializa en el control de ancho de banda, además permite sacar reportes, priorizar, clasificar y bloquear tráfico. Puede trabajar ya sea sobre redes 802.3 o sobre redes ATM, frame relay.

Permite realizar clasificación de tráfico mediante puertos ya sean UDP o TCP, asignar ancho de banda por IP, MAC-Addres, subred, host. Además maneja calidad de servicio para priorizar tráfico.

En la actualidad se utiliza este dispositivo para realizar el control de ancho de banda de los clientes, el problema de este dispositivo es que la capacidad de manejo de

ancho de banda esta limitada a 6Mbps, para la expansión de la capacidad es necesario adquirir una licencia cuyo costo es de USD$1000, este es un rubro muy alto para la empresa.

3.4.3.4 SELECCIÓN DE PRODUCTO

En la selección del producto se toma como opciones, Packeeter o Linux- Mikrotik, no se ha tomado routers CISCO debido a que su funcionamiento es limitado para controlar ancho de banda y además su costo es elevado respecto a las otras soluciones. Tanto Packeteer como Mikrotik cumplen las características necesarias para manejar los requerimientos de la red, pero en cuestiones económicas es más conveniente usar productos Mikrotik ya que no necesitan de un sistema operativo instalado tal como lo requiere Stickgate, además Mikrotik permite adquirir las licencias según las necesidades, controla el ancho de banda e implementa un firewall y clasificador de tráfico. Su administración es mediante herramientas gráficas que permiten visualizar tráfico por clases. Permite incorporar un hotspot que trabaja con un Portal Cautivo y un servidor Radius interno.

Existe Puntos de acceso que incorporan estas funcionalidades en su software, pero no es recomendable asignar al punto de acceso toda la responsabilidad de manejar y administrar el ancho de banda de usuarios, ya que esto incrementaría el procesamiento del dispositivo y disminuiría su rendimiento, por este motivo el punto de acceso solo permitirá la asociación a la red y, el manejo de los otros servicios, se lo hará mediante otros dispositivos.

El Anexo D, muestra información de los equipos seleccionados para el diseño.

3.5 ANÁLISIS DE COSTOS.

Para el análisis de costos se tomará en cuenta los precios actuales por el servicio de Internet, el costo de salida internacional, el costo de la implementación del hotspot y finalmente se determinará el precio del servicio de Internet con que la empresa podría salir al mercado.

Se determinará el costo total de implementación y la tasa de retorno de dicha inversión.

3.5.1 PROVEEDORES

En esta sección se presentará un conjunto de proveedores de servicio de Internet con el fin de comparar los precios que estos cobran por el servicio y por la instalación, también los beneficios que incluyen en sus planes. Entre las principales tecnologías de acceso se tienen: XDSL, cable MODEM, inalámbrico.

Proveedor	Tipo de enlace	Velocidad [Kbps]	Compartición	Tarifa	Instalación	Servicios adicionales
Interactive	Doméstico	128/64	8 a 1	39,9	90	1 Cuenta de correo, 10M
		256/128	8 a 1	59,9	90	2 Cuentas de correo, 10M
		512/128	8 a 1	89,9	90	5 Cuentas de correo, 10M
Panchonet S.A	Doméstico	128/64	8 a 1	39	80	1 cuenta de correo, 10MB
		256/128	8 a 1	65	80	3 cuentas de correo, 10MB
Satnet	Doméstico	128/128	6 a 1	39,9	100	1 Cuentas correo, 10MB 1 Pc's concurrentes
		200/150	6 a 1	49,9	100	2 Cuentas correo 10MB 2 Pc's concurrentes
		400/150	6 a 1	75	100	3 Cuentas correo, 50MB 3 Pc's concurrentes
		800/300	6 a 1	125	100	5 Cuentas correo, 50MB 5 Pc's concurrentes
Andinanet	Doméstico	128/64	8 a 1	39,9	50	1 Cuentas correo, 10MB
		246/128	8 a 1	65	50	2 Cuentas correo, 10MB
		512/256	8 a 1	79,99	50	5 Cuentas correo, 10MB
	Corporativo	128/64	8 a 1	49,9	50	3 Cuentas correo, 10MB
		246/128	8 a 1	79,9	50	5 Cuentas correo, 10MB
		512/256		99,9	50	7 Cuentas correo, 10MB
ECUTEL	Store Pack	128	8 a1	40	100	7 Cuentas correo, 4MB 1-5 Pc's concurrentes
		256	8 a 1	65	100	10 Cuentas correo, 4MB 1-10 Pc's concurrentes

Tabla 3.10 proveedores de servicio de Internet

De la Tabla 3.10 se puede concluir que la mayor cantidad de empresas usan tecnología XDSL como última milla, Satnet usa cable coaxial para la implementación de cable modems y solo Ecutel lo hace mediante medios inalámbricos. El precio del

servicio se mantiene entre los 40 y 100 dólares. Los beneficios que ofrecen la mayoría de proveedores son cuentas de correo que están entre 1 a 10 cuentas, dependiendo del plan contratado. El costo de instalación mas bajo es presentado por Andinadatos que es de 50 dólares, el resto tienen precios superiores.

3.5.2 PROVEEDORES DE ANCHO DE BANDA

En esta sección se tomará en cuenta el costo de ancho de banda para salida internacional. Gigowireless posee actualmente 3Mbps de este ancho de banda, de esta, se halla disponible en promedio 1Mbps. Para iniciar el proyecto se utilizará el ancho de banda disponible de la empresa y se ira incrementando paulatinamente, según el dimensionamiento previsto en el capítulo 2 se requería de un E1.

Se tomará como proveedor a Andinadatos, puesto que la empresa posee una conexión de fibra óptica. El costo de un E1 es de 1200 dólares mensuales.

3.5.3 COSTO DE IMPLEMENTACIÓN DEL HOT SPOT

Solo se analizarán los costos en equipos necesarios para implementar la red física

Requerimiento	Detalle	cantidad	Costo unitario	Total
Enlace Gigowireless-Condado	MTI	2	700	1400
Punto de Acceso Principal	Netkrom-AIR-BR500G	3	299	897
Arreglo de Paneles Sectoriales	Hyper link-14dBi	3	550	1650
Pigtails	LM-400	10	10	100
Estructuras de 3m	Tubo Galvanizado	4	15	60
Cajas para equipos	Cajas térmicas	3	25	75
Instalaciones eléctricas	Cable, toma corrientes.	3	15	45
Mikrotik	PC+Mikrotik	1	1000	1000
Instalación y configuración de equipos	Técnicos	3	100	300
	TOTAL			5527

Tabla 3.11 Presupuesto de implementación de hotspot

3.5.4 ANÁLISIS TARIFARÍO

Los servicios que deberá cancelar un cliente serán los siguientes:

3.5.4.1 Instalación del servicio

Este precio lo cancelarán solo aquellos clientes que no disponen de un dispositivo inalámbrico, para aquellos que si lo disponen, podrán directamente acercarse al departamento de atención al cliente.

Detalle	Costo
Instalación	20
Dispositivo Inalámbrico	55
Total	75

3.5.4.2 Precio según el plan requerido

Para establecer el precio por ancho de banda requerido se tomará como referencia las tarifas que se manejan en el mercado. Si se toma en cuenta que el precio del ancho de banda se lo debe compartir con el mayor numero de usuarios posible para poder tener una rentabilidad, entonces se tomará en cuenta que si se alquila un E1 en Andinadatos tiene un costo de 1200 dólares, si el nivel de compartición es de 8, se puede tener 128 usuarios de 128Kbps, si se toma como referencia el precio mas bajo que es 39.9 se tendrá un ingreso de US$5.107 dólares, de este monto se descontará el costo de Andinadatos e IVA y se tiene un ingreso para la empresa de 3396.48 dólares.

Con este antecedente se presenta una propuesta de las tarifas para el mercadeo de los productos.

Plan	Costo
128/128 Home	35+IVA
256/256 Home	50+IVA
512/512 Home	75+IVA
128/128 Corporativo	50+IVA
256/256 Corporativo	80+IVA
512/512 Corporativo	100+IVA

Tabla 3.12 Precios de servicio

3.5.4.3 Adicionales en cada plan

A cada usuario se le proveerá:

1-6 cuentas de correo bajo el dominio de Gigowireless.

Conexión a 1PC que para el caso de los clientes corporativos, se deberá instalar un ruteador o un servidor que permita compartir la conexión de Internet.

3.5.4.4 Crecimiento de usuarios e ingresos

Tomando como referencia el crecimiento promedio que ha tenido Gigowireless, este año se vendió 30 contratos al mes, con un crecimiento del 10% mensual. En la Tabla 3.13 se realiza la proyección de los ingresos y el tiempo de saturación de la red.

Tiempo	Usuarios	Planes requeridos	Costo	IVA	Ingresos	Ingresos-IVA
mes 1	30	128	35	39,2	1176	1050
mes 2	33	128	35	39,2	1293,6	1155
mes 3	36	128	35	39,2	1411,2	1260
mes 4	39	128	35	39,2	1528,8	1365
mes 5	42	128	35	39,2	1646,4	1470
TOTAL	180	128	35	39,2	7056	6300

Tabla 3.13 Crecimiento

3.6 ANÁLISIS LEGAL

Para este análisis se tomará en cuenta la ley reformada de telecomunicaciones, así como también varias normas.

- Reglamento para la Prestación de los Servicios de Valor Agregado, publicado en el Registro Oficial No. 545 del 1 de abril del 2002.

- Reglamento para la Homologación de Equipos Terminales de Telecomunicaciones, publicado en el Registro Oficial No. 10 del 24 de agosto de 1998, y su reforma, publicada en el Registro oficial No. 623 del 22 de julio del 2002.

- Norma para la Implementación y Operación de Sistemas de Espectro Ensanchado, publicada en el Registro Oficial No. 215 del 30 de noviembre del 2000.

- Norma de calidad del servicio de valor agregado de Internet

3.6.1 REGLAMENTO PARA LA PRESTACIÓN DE LOS SERVICIOS DE VALOR AGREGADO, PUBLICADO EN EL REGISTRO OFICIAL NO. 545 DEL 1 DE ABRIL DEL 2002.

En primera instancia se analizará si el proyecto cumple con el **"Reglamento para la prestación de servicios de Valor Agregado"**, para esto se tomarán varios aspectos del reglamento como el que dice: "*Son servicios de valor agregado aquellos que utilizan servicios finales de telecomunicaciones e incorporan aplicaciones que permiten transformar el contenido de la información trasmitida. Esta transformación puede incluir un cambio neto entre los puntos extremos de la transmisión en el*

código, protocolo o formato de la información" El proyecto cumple con este requisito de "valor agregado" y dispone el permiso necesario para brindar servicios de Internet.

El transporte de la información para la prestación de sus servicios lo podrá hacer mediante:

a) *Infraestructura propia.- Para lo cual deberá especificarlo en la solicitud adjuntando el diagrama y especificaciones técnicas y conjuntamente deberá tramitar la obtención del título "habilitante", necesario para su operación no pudiendo ser alquilada su capacidad o infraestructura a terceros y,*

b) *Contratar servicios portadores.- Para lo cual deberá señalar en la solicitud correspondiente la empresa de servicios portadores que brindará el servicio.*

El proyecto por naturaleza no cumple con esta norma referente al acceso, ya que dispone de permiso para brindar servicios de valor agregado y no para proveer accesos de última milla, que solo es permitido para empresas que poseen un título habilitante de portador.

Para subsanar este aspecto se ha realizado un acuerdo con Access Ram, misma que representará legalmente la declaración de los enlaces y clientes inalámbricos, el costo por cada enlace será de 100 dólares. Este detalle se ha consultado con la Ingeniera Mónica Riofrío, quien trabaja en el departamento legal del CONATEL, indicando que hay aceptación legal porque Access Ram tiene titulo habilitante de portador.

3.6.2 NORMA PARA LA IMPLEMENTACIÓN Y OPERACIÓN DE SISTEMAS DE MODULACIÓN DIGITAL DE BANDA ANCHA

Esta norma establece las frecuencias en las que debe trabajar un sistema de modulación de banda ancha, las frecuencias que se detallan en la norma son las siguientes:

BANDA (MHz)
902 - 928
2400 - 2483.5
5150 – 5250
5250 - 5350
5470 - 5725
5725 - 5850

En el proyecto se utiliza dos bandas descritas en la norma, estas son: el rango de 2400- 2483.5MHZ para la red de acceso (puntos de acceso) y la de 5725-5850MHZ para la red de distribución (enlaces punto a punto). Además cumple con las dos formas de configuración para sistemas de modulación de banda ancha, punto a punto y punto multipunto.

Para la legalización de los enlaces es necesario presentar el estudio técnico, el mismo que se ampara en los siguientes formularios a llenar:

Formulario RC-1B, RC-2A, RC-3A, RC-3B, RC-4A, RC-9A, RC-9B, RC-9C, RC-14A, RC-15A

En el anexo E, se detalla el significado que cada formulario.

3.6.3 REGLAMENTO PARA HOMOLOGACIÓN DE EQUIPOS DE TELECOMUNICACIONES

La norma indica que los equipos que se utilicen, deberán ser homologados en la superintendencia de telecomunicaciones. Gigowireles necesitará homologar los radios MTI.

Para la homologación será necesario presentar los siguientes documentos:

- Solicitud escrita dirigida al Superintendente de Telecomunicaciones.
- Manuales técnicos.
- Características de funcionamiento y modo de conexión a la red.
- Un certificado de características técnicas de los equipos cuya clase, marca y modelo se quiere homologar, emitido por un organismo internacional reconocido.

3.6.4 NORMA DE CALIDAD DEL SERVICIO DE VALOR AGREGADO DE INTERNET

Esta norma ayuda a regular la calidad de los servicios de telecomunicaciones y define el término de banda ancha, que dice: " *Se establece como banda ancha a todas las conexiones cuya capacidad sea desde 256kbps como velocidad de bajada y 128 como velocidad de subida, bajo estos valores se considera banda angosta*". El proyecto cumple con esta norma ya que presenta planes que están dentro de los 256Kbps tanto para subida como bajada, pero todavía se mantienen los planes cuyo

ancho de banda es 128Kbps, debido a que los costos por salida internacional son todavía altos e implicaría no ofrecer a los clientes, planes económicos.

CAPÍTULO 4

PROTOTIPO Y PRUEBAS

Este capítulo presenta el prototipo de la red inalámbrica de acceso a Internet, permitirá la simulación de un hotspot para brindar el servicio en un sector específico. En el prototipo se realizarán las pruebas que determinen la funcionalidad de la red de acceso a Internet y sus servicios. Finalmente se documentará los resultados obtenidos en las pruebas y se realizarán los ajustes correspondientes para el prototipo.

4.1 IMPLEMENTACIÓN DEL PROTOTIPO.

En esta sección se describirá las características físicas de los componentes del prototipo. Este comprenderá un enlace hacia un proveedor, el punto de acceso para los clientes, control de ancho de banda, portal cautivo y los servidores de web, DNS y correo para simular la red de servidores.

El enlace hacia el proveedor de Internet, que en este caso será un nodo acceso de la empresa que esta ubicado en el sector de San Fernando, se lo hará utilizando un Access Point SENAO y una antena flan panel de 15.5 dB. Mediante éste enlaces se representará la conexión punto a punto, que en el diseño se hace referencia. Para bajar la señal hacia el punto de acceso se utilizará una interfaz 802.3u, que se interconectará hacia un switch de distribución, se colocará un ruteador que permitirá separar la interconexión con el proveedor y la red de distribución de Internet, el ruteador utilizará la dirección IP: 172.16.188.246/24 en la interfaz WAN y en su interfaz LAN se usará la IP:192.168.1.1/24 tal como se indica en la Figura 4.1 . El prototipo se basa en el diseño propuesto en el capítulo 3.

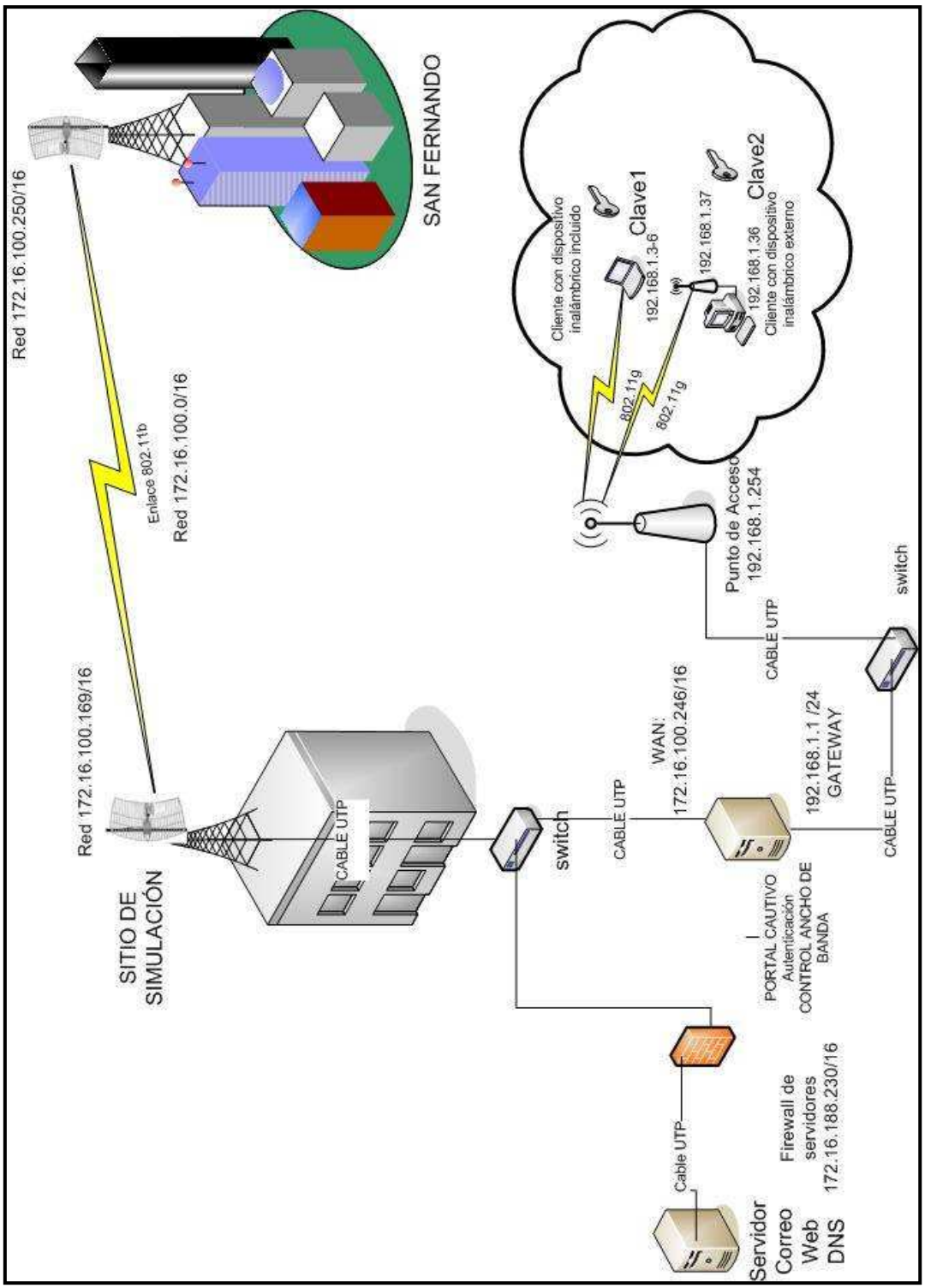


Figura 4.1 Diagrama del prototipo de pruebas.

Para la implementación de la red de acceso se utilizó un Access Point de la marca D-Link 2100, con una potencia de 63mw y un panel sectorial de 15dB. El servidor de autenticación, acceso y control de ancho de banda se halla en un mismo computador. Para la implementación de estos servicios se utiliza el software Mikrotik, que realiza también el papel de router de Acceso, tiene dos interfaces fastethernet, una con una IP 172.16.188.246 que conectará hacia la red de Gigowireless de salida Internacional y la otra interfaz con la IP 192.168.1.1 que permitirá la comunicación con la red de clientes.

Finalmente se implementa los servicios de correo y WEB, mismos que se encuentran alojados en un computador bajo el sistema operativo LINUX. Además se implementa un Firewall que proteja al servidor.

Todas las configuraciones de los equipos y servidores se documentan en el ANEXO F.

4.2 PRUEBAS DE RENDIMIENTO.

En esta prueba se verificará la estabilidad de la red desde diferentes lugares del hotspot, utilizando una laptop con una tarjeta de red que permita la conexión a la red inalámbrica

4.2.1 PRUEBA

Se verifica la estabilidad del enlace hacia el punto de acceso asignado utilizando el protocolo ICMP, se efectúa un Ping durante un tiempo de 10 minutos. Se comprueba la estabilidad del enlace a diferentes distancias y ángulos, de igual manera se realiza una tabla en la que se detalle los tiempos de respuesta hacia el punto de acceso, se obtuvieron tiempos desde 1ms y hasta 15ms como máximo, la cantidad de paquetes perdidos fue mínima, en una de las muestras tomadas se tuvo 10 paquetes perdidos en 300 paquetes, que realmente no afectan a la

calidad del servicio. A continuación se muestra la Tabla 4.1 con los resultados obtenidos.

	TIEMPOS DE RESPUESTA HACIA EL PUNTO DE ACCESO							
ANGULO[º] \ DISTANCIA[m]	**0**	**30**	**60**	**90**	**120**	**150**	**180**	**210**
0	1	2	2	2	5	7	8	15
30	1	1	3	3	4	8	10	11
60	1	2	3	5	3	9	11	14
90	1	2	4	4	5	7	10	10
120	1	1	2	4	4	8	11	15
150	1	1	3	3	5	7	9	12
180	1	2	2	3	6	9	8	13

Tabla 4.1 Tiempos de respuesta.

4.3 PRUEBAS DE DISPONIBILIDAD

En esta sección se probará los niveles de señal, la relación señal a ruido en diferentes puntos de la implementación del hotspot, para realizar las pruebas se utilizará un laptop y una tarjeta inalámbrica y mediante el software Netstumbler se realizará la detección de las señales de las redes cercanas, la prueba consiste en realizar mediciones de niveles de señal en diferentes puntos del sector de implementación del prototipo, los resultados indicarán si la cantidad de señal detectada es suficiente para que un enlace se establezca y permanezca estable.

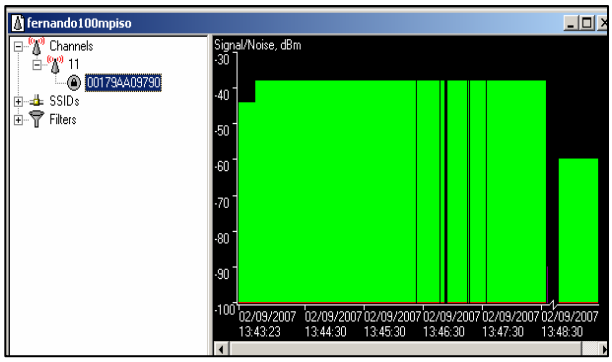
4.3.1 PRUEBA

Para realizar la prueba de disponibilidad se ha elaborado un cuadro en el cual se toma muestras de porcentajes de señal a diferentes distancias y en varios ángulos tomado como eje la antena del punto de acceso. En la Tabla 4.2 se muestra el cuadro correspondiente a estas mediciones.

	MEDIDA DE NIVEL DE PORCENTAJE DE SEÑAL							
ANGULO[°] \ DISTANCIA[m]	**0**	**30**	**60**	**90**	**120**	**150**	**180**	**210**
0	100	100	100	100	100	100	100	100
30	100	98	95	92	87	80	77	70
60	100	95	94	90	85	78	75	69
90	100	97	93	93	86	82	73	67
120	100	97	91	90	81	80	76	63
150	100	95	94	91	84	78	79	67
180	100	98	93	90	83	80	78	70

Tabla 4.2 Porcentaje de señal

Para corroborar los datos se presenta la figura 4.2, Figura 4.2 Nivel de señal a ruido e intensidad de señalen la que se puede apreciar el nivel de señal a la distancia de 210 m, además se tomó una muestra del nivel de señal a ruido que existió en esta misma posición.



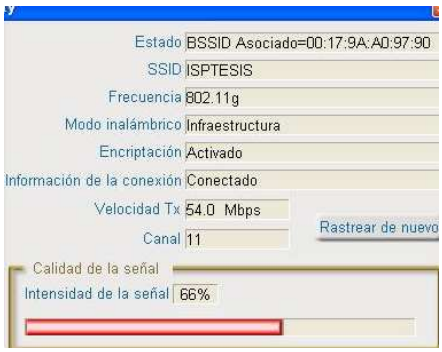


Figura 4.2 Nivel de señal a ruido e intensidad de señal

Con las pruebas y muestras tomadas, se comprobó que existe conectividad con el punto de acceso y disponibilidad de los servicios de Gigowireless, se realizó pruebas de navegación y acceso a los servicios disponibles. Se verificó que con niveles de señales menores al 50% se tiene perdidas de paquetes, esto afecta el servicio, mismo que empieza a ser inestable presentando pérdidas que oscilan entre 10% y 15%.

4.4 PRUEBAS DE SEGURIDAD.

Se verificará el funcionamiento de las claves de seguridad para los usuarios y para los servicios, se creará varias cuentas para clientes con sus respectivos dominios para pruebas, en las cuales se verificará el funcionamiento de los servicios con los respectivos niveles de señales.

4.4.1 PRUEBA

Se comprueba que si el cliente no se autentifica, no podrá enviar tráfico a ningún lado, porque el firewall implementado en el portal cautivo bloquea todo tipo de información y redirecciona hacia la página de autenticación: En la Figura 4.3 se mira que se hace un ping hacia el gateway y no se tiene respuesta, se demuestra que el usuario se encuentra asociado al punto de acceso pero a pesar de ello no puede realizar transmisiones mientras no se autentique, además, cada vez que se intente abrir una página de Internet, se desplegará la interfaz que pedirá los datos de acceso al servicio.

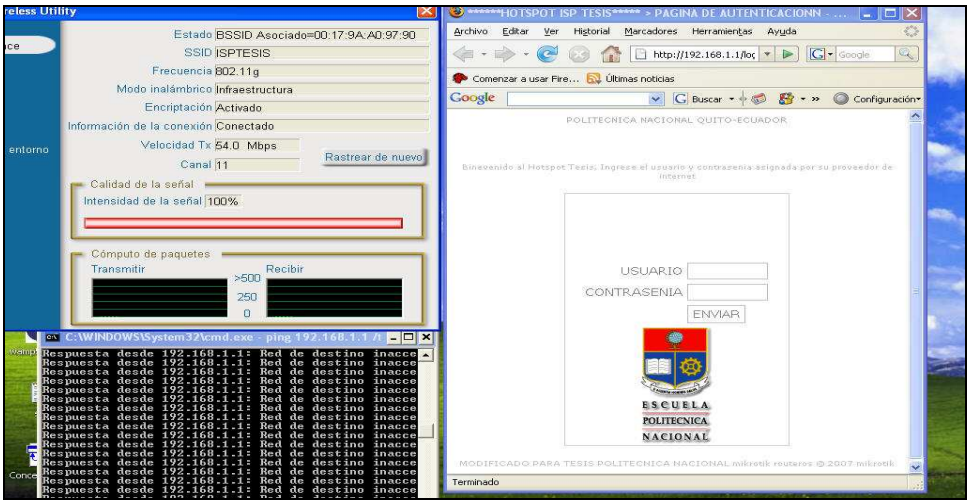


Figura 4.3 Acceso a la red

En la Figura 4.4 se demuestra que ingresando la clave asignada por el Gigowireless se puede enviar tráfico y, además, el servidor indica que ha sido autentificado, se puede verificar además que una vez realizado este procedimiento, el mensaje ICMP de host de destino inaccesible desaparece y se cambia por el mensaje de respuesta desde el servidor.

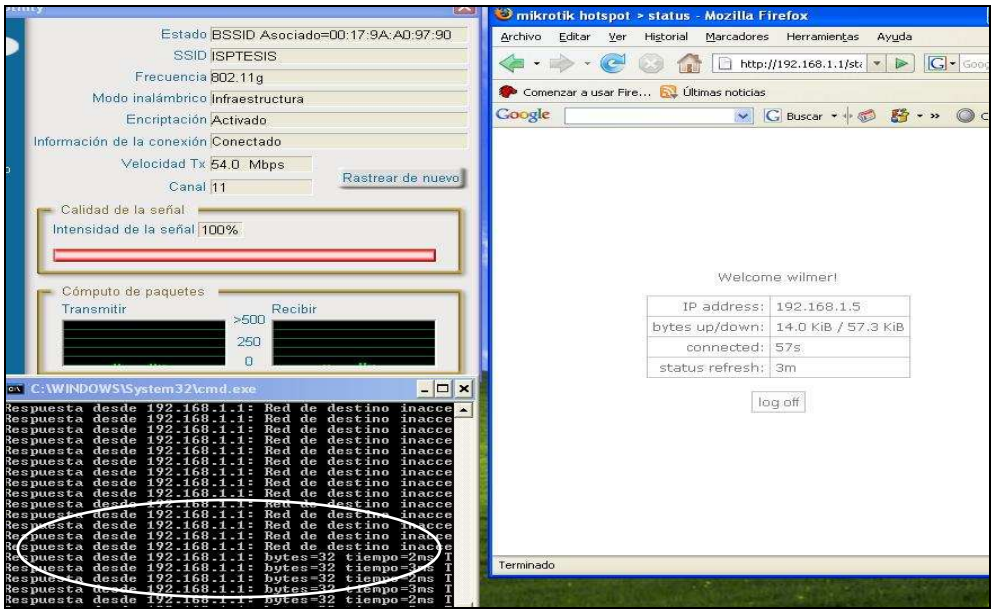


Figura 4.4 Prueba de autenticación

4.5 PRUEBAS DE FUNCIONALIDAD.

En esta sección se verificará la funcionalidad completa del prototipo la forma de configurar los dispositivos inalámbricos para conexión a la red y acceso al servicio, verificando además los diferentes tipos de planes y su funcionalidad, se utilizarán medidores públicos que permitan probar los planes y sus velocidades

4.5.1 PRUEBA 1

Para probar la funcionalidad del prototipo se verificará las características del servicio y la configuración de los dispositivos para que el cliente acceda al servicio. Primeramente el cliente deberá recibir la clave wep para asociación al access point. Se indicará la dirección IP que es asignada y que estará ligada a una capacidad de canal contratada. Entonces para la asociación a la red inalámbrica, se localiza la misma, en este caso el SSID de la red es ISPTESIS, se verifica los niveles de señal y luego se asocia. El proceso de conexión tendrá 4 fases que se detallan a continuación.

FASE1, se detecta la red a conectarse, y se comprueba el nivel de señal existente, se debe recordar que el nivel mínimo de señal debe ser el 50%, en la gráfica se muestra que el nivel es el 100%.

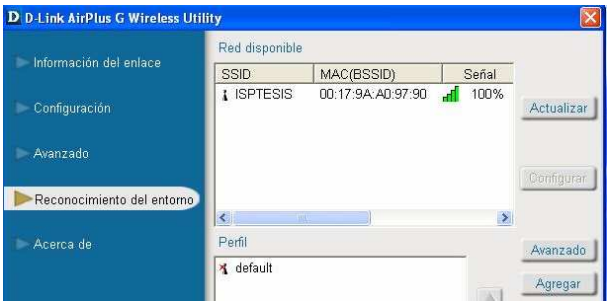


Figura 4.5 Detección de la red

FASE 2, se configura el acceso, para lo cual se elige la red “ISPTESIS “y se completa los parámetros tales como, la clave WEP, y la dirección IP asignada.

Figura 4.6 Configuración de parámetros de red

FASE 3, una vez configurado los parámetros, se presiona el botón “conectar” y se verifica que se halla asociado al punto de acceso. En la Figura 4.7 se aprecia que el usuario se halla conectado a la red y pero que no se puede enviar datos hacia el exterior. Esta es una característica importante del hotspot, que incrementa la seguridad del sistema, inclusive podrá colocar una red abierta sin ninguna clave WEP, debido a que el usuario no podrá enviar tráfico mientras no sea autentificado en el servidor.

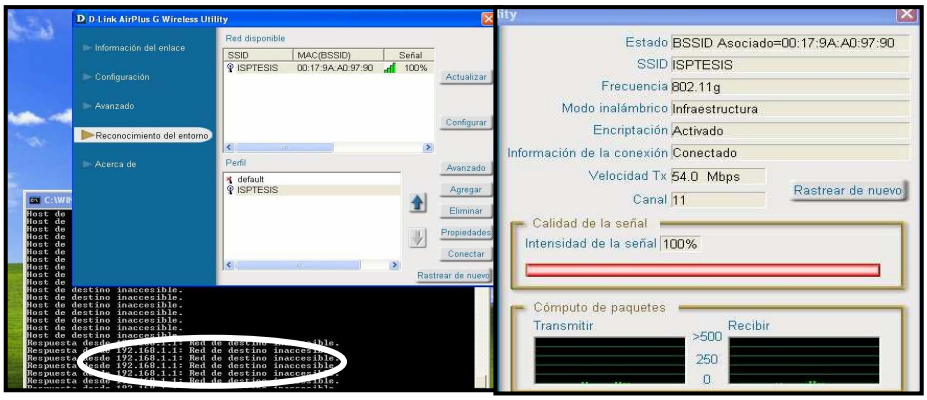


Figura 4.7 Asociación a la red

FASE 4, se debe ingresar la clave de usuario, esta clave dará los permisos para el uso de los recursos. Una vez ingresado saldrá una pantalla de bienvenida e indica que se encuentra autentificado para usar el servicio. En esta fase ya se puede navegar a Internet y enviar tráfico a cualquier lugar.

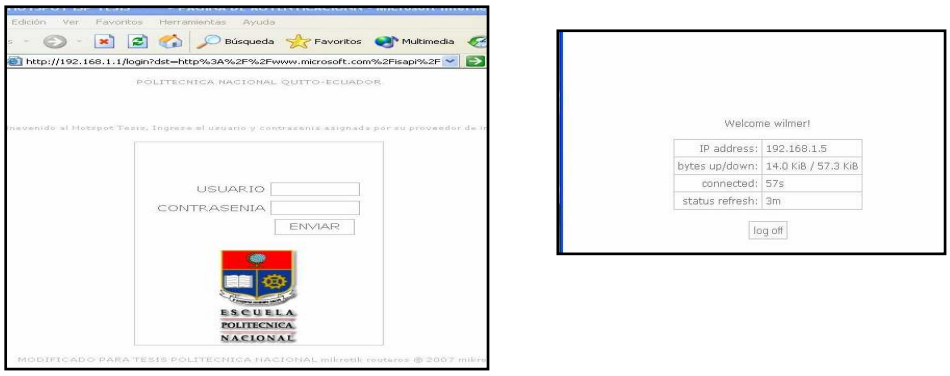


Figura 4.8 Autenticación y bienvenida a la red

4.5.2 PRUEBA 2

En esta prueba se verificará la validez de uno de los planes para clientes creados. Se tomará como ejemplo un plan 128 Kbps /128 Kbps, para esto se utilizó el medidor público de un proveedor y se verificó que el ancho de banda del cliente fue 125 Kbps. Esta prueba se realizó durante 5 ocasiones y siempre se tuvo un resultado similar, la medida mas baja que se tuvo fue 100 Kbps y la máxima 125 Kbps.

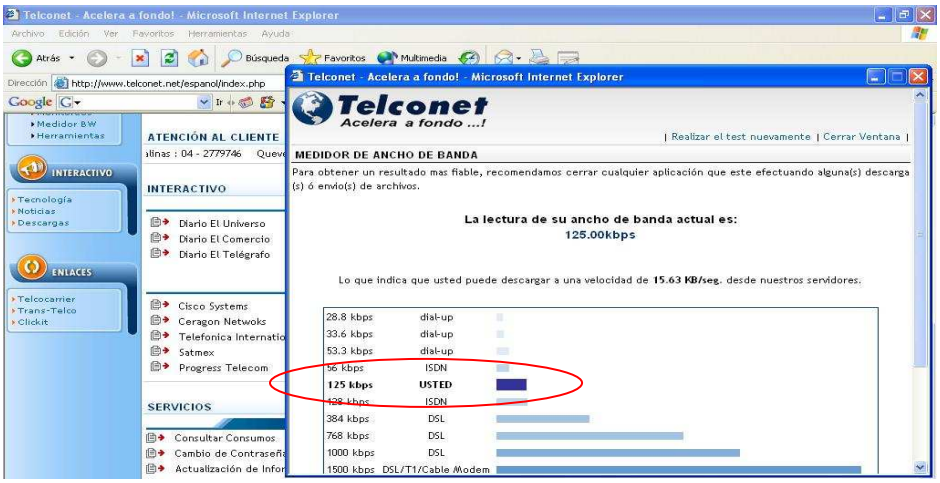


Figura 4.9 Medición de ancho de banda

Se realizó otra medición de la tasa de transferencia realizando una descarga de un programa, apreciando una tasa de transferencia de 14.2KB/seg., misma que se encuentra en bytes por segundo, aunque normalmente el ancho de banda se lo hace en bits por segundo, por esta razón es necesario multiplicar por un factor 8 para obtener el valor en bits. 14.2KBps*8= 113.6Kbps.

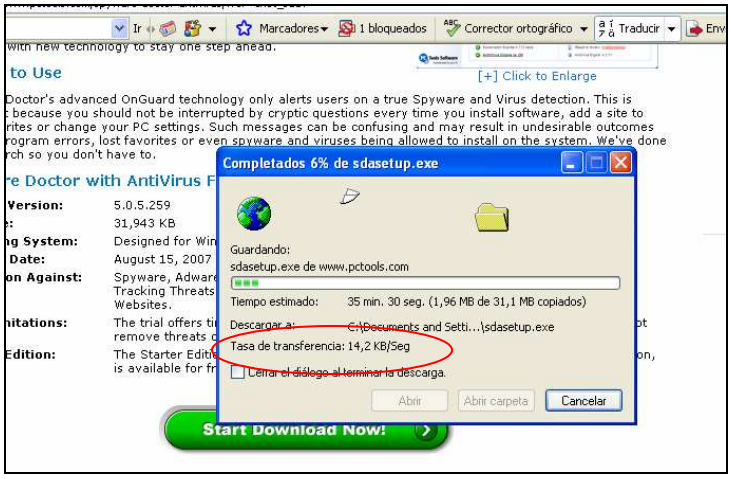


Figura 4.10 Descarga de archivo y tasa de transferencia

4.5.3 PRUEBA 3

Esta prueba tiene como objetivo verificar la funcionalidad de los servidores de correo, web, DNS. Para esto se ha creado varios dominios virtuales sobre el servidor que permiten crear cuentas de correo y la administración de la página WEB. Se comprobará la conexión hacia el servidor y hacia el dominio. En primer lugar se efectuará la conexión hacia el dominio de Gigowireless que se denominó, www.isptesis.com y mostrará la página que se aprecia en la Figura 4.11.

Figura 4.11 Página de Hotspot.

En Figura 4.12 se detalla los servidores virtuales creados, cada servidor virtual es un dominio y en este caso se tienen tres dominios con sus correspondientes casilleros de correo

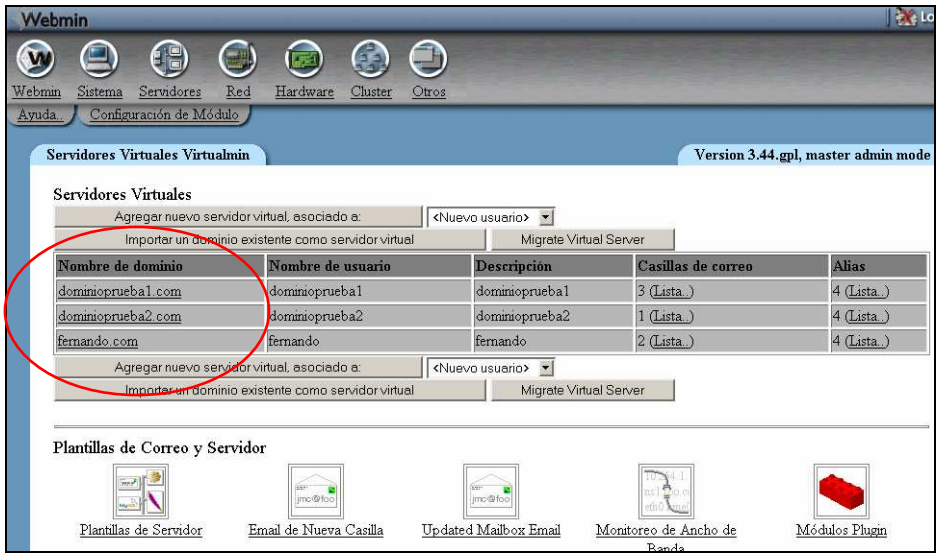


Figura 4.12 Dominios

- **Prueba del DNS.**

Para la prueba del servicio de DNS se hará un ping hacia un dominio que se halla configurado en el servidor, en las figuras siguientes se observa primero que la tarjeta de red se halle con la dirección IP del DNS, en este caso es 172.16.188.230, en la Figura 4.13 se verifica que cuando hacemos un ping hacia isptesis.com, se tiene una respuesta del servidor donde se encuentra alojado el dominio. Con esto se prueba que se esta asociando un dominio con una dirección IP y se esta realizando la trasformación correspondiente.

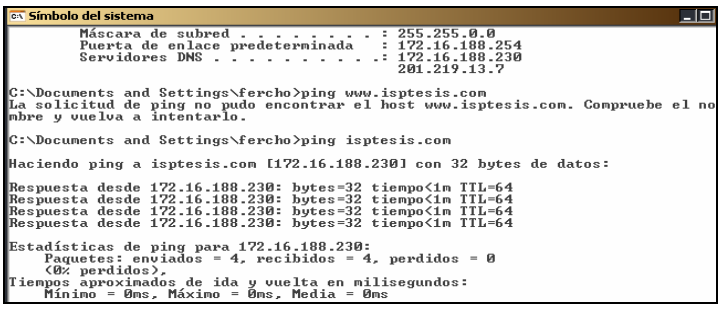


Figura 4.13 pruebas de DNS

- **Prueba de correo**

Para la prueba de correo, se configurará una cuenta utilizando Outlook y se verificará su funcionamiento, en la Figura 4.14 se puede identificar los parámetros a completar, siempre el pop y smtp será el mail.nombre_dedominio.com, el nombre del usuario irá sin el dominio y la clave que fue asignada en el servidor, además se debe tomar la opción de “mi servidor requiere autenticación”, este detalle es importante porque si no se elige esta opción, será imposibilitado de enviar correo mediante el servidor de la empresa.

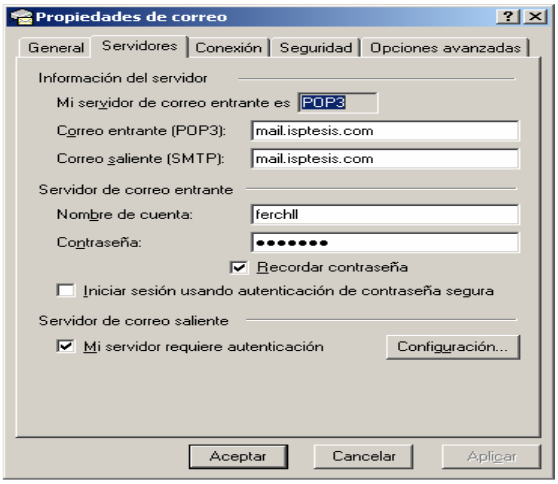


Figura 4.14 Configuración de cuenta e Outlook.

En la Figura 4.15 se muestra los correos recibidos como prueba, se puede apreciar además que también llegó la información de otro dominio así como el que fue reenviado desde la misma cuenta.

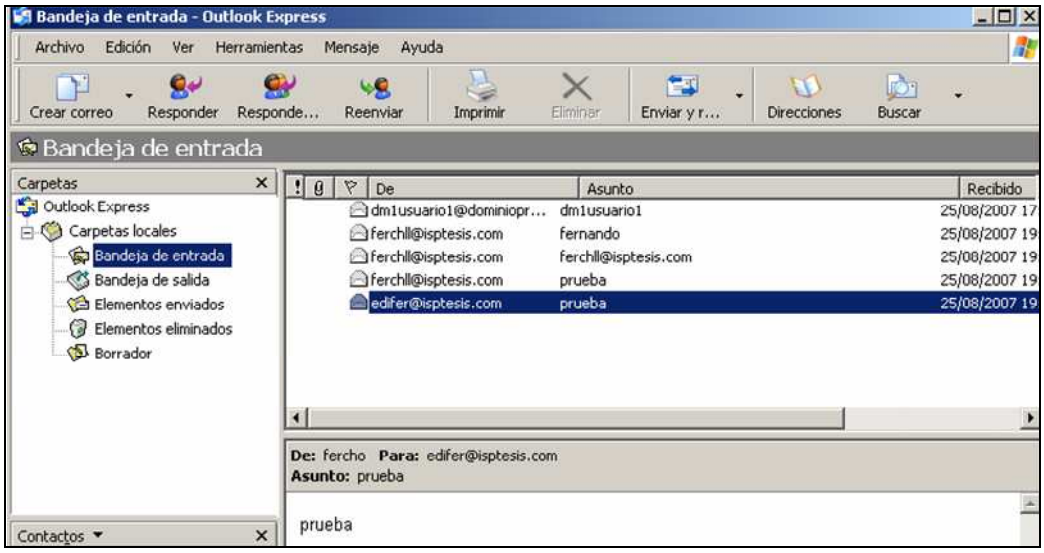


Figura 4.15 Correos en la bandeja de entrada de Outlook

4.6 AJUSTE DEL DISEÑO

En esta sección se analizará los resultados encontrados en la etapa de pruebas y con los resultados obtenidos se realizará ajustes al diseño en cualquiera de los componentes que este comprenda.

4.6.1 AUTENTICACIÓN.

El problema encontrado en este módulo fue que una vez ingresado el usuario y clave, no se volvía a pedir nunca más autenticación. El ajuste del diseño que se hace necesario en este módulo es limitar el tiempo de autenticación cada vez que usuario apague la máquina y también en el momento que vuelva a ingresar al servicio tenga que autentificarse nuevamente. Para lograr este cometido se debe reducir el tiempo de “keepalive timeout” ya que por defecto viene configurado para tres días y bajarlo a 3 minutos, esta acción permitirá borrar el cookie y al apagar la máquina vuelva a pedir la autenticación.

Figura 4.16 Configuración de "profile"

4.6.2 MÓDULO DE ACCESO

El inconveniente hallado en este punto fue con la cobertura que brinda la antena con la cual trabaja el punto de acceso, ya que en el momento de llevar a cabo la instalación se colocó sin inclinación. Cuando se efectuaron las pruebas se comprobó la existencia de pérdidas de paquetes porque los niveles de señal fueron menores al 40%, había una conexión a la red pero con pérdida de paquetes del 35% y continuas desconexiones.

El ajuste consistió en la inclinación de la antena un ángulo de 10º, esto mejoró la cobertura en los lugares bajos y se logro tener conexiones estables sin pérdidas de paquetes.

4.6.3 SERVIDORES

Una dificultad que se detecto en el servidor de correo, web y DNS, fue que la interfaz gráfica consumía muchos recursos, esto ocasionó al cliente una lentitud en el acceso al servicio.

Para eliminar el inconveniente, fue deshabilitada el interfaz gráfico y configurado el servidor para que inicie en modo 3, el cual elimina el modo gráfico.

Se tomo medidas de protección adicionales para el acceso al servidor, limitando el número de intentos de autenticación errados, con el fin de evitar intrusiones usando métodos de “fuerza bruta”. También se bloquea el acceso desde cualquier dirección IP y solo se permite acceder desde las direcciones IP propias de la red.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

Esta sección presentará las conclusiones y recomendaciones surgidas durante la elaboración de este proyecto. Se presentará las conclusiones generales y luego las conclusiones referentes a cada una de las fases de la metodología. Posteriormente se presentarán todas las recomendaciones aplicables al proyecto.

5.1 CONCLUSIONES.

- La arquitectura SAFE ayudó a realizar el análisis actual de Gigowireless. Los componentes de Gigowireless fueron agrupados según su funcionalidad en cada módulo de la arquitectura SAFE, llegando a tener una organización física según esta recomendación. Una vez agrupados los dispositivos se procedió al análisis de cada módulo y a identificar potenciales inconvenientes. Esta agrupación además sirvió para realizar el diseño de la red específica que se pondrá en funcionamiento en el sector de El Condado.

- Para conseguir los datos requeridos para el diseño de la red se utilizó software gratuito como “Netstumbler” y “Google Earth”. El primero permitió realizar un "site survey " del sector a cubrir, con el mismo se descubrió qué redes se hallan presentes y sus niveles de señal, además se verificó la seguridad implementada en cada una de ellas así como también su modo de trabajo. Google Earth permitió tomar “fotografías satelitales” del sector a cubrir y recabar información geográfica como: coordenadas y alturas de los sitios donde posiblemente se podría instalar los puntos de acceso, también dividir el área a cubrir en diferentes sectores.

- Para el proceso de diseño de la red de acceso inalámbrico (multipunto). Se realizó cálculos matemáticos, en base a los modelos de propagación propuestos por “Okumura-Hata” y fueron comparados con datos obtenidos mediante el simulador EKAHAU, de este modo se obtuvo que el área a cubrir era alrededor de 3.2Km^2, utilizando tres puntos de acceso, entre la información relevante conseguida esta: en nivel de señal a diferentes distancias, velocidad e interferencias.

- Para simular el enlace punto a punto se utilizó el software RADIO MOBILE, mismo que indica la libertad de zona de fresnel y niveles de potencia recibidas.

- Se realizó un análisis de diferentes tipos de equipos existentes en el mercado, se comparó las características técnicas y se procedió a la elección de una de ellas, tomando en cuenta aspectos técnicos y económicos. Se realizó un análisis de los precios del mercado actual y el costo que presenta el proyecto. Se hace una proyección de crecimiento de la red debido a la incorporación de clientes, basado en las ventas actuales que tiene el ISP, esta proyección indica en que tiempo se tendría ocupada al 100% la red.

- En el análisis legal se tomó en cuenta los requisitos que implica la implementación de una red inalámbrica pública, recurriendo a normas y reglamentos expuestos por el CONATEL. Se buscó una solución para la implementación de la red y no infligir el “*Reglamento para la prestación de servicios de valor agregado*”, que permite solo a dar acceso de última milla a los Portadores, firmando un convenio con la empresa “Access Ram “ (tiene título habilitante de portador) que auspiciará y declarará los enlaces que la empresa posee.

- Para probar la funcionalidad del diseño se implemento un prototipo, en el que se realizaron varias pruebas. Una de ellas permitió determinar cuál es el nivel mínimo de señal para poder conectarse a la red. Los resultados obtenidos arrojan un nivel de señal del 50%, suficiente para asociar a la red y obtener estabilidad en el envío de datos, esto implica que no exista perdida de paquetes.

- El control de ancho de banda se hizo mediante el establecimiento de prioridades de las colas de datos, que van de uno a ocho, donde uno es la prioridad más alta y 8 es la más baja.

- El uso de un “portal cautivo” hace que la red se vuelva funcional y dinámica. Al usar un servidor Radius externo se puede centralizar la base de datos para autenticar a los clientes y así poder realizar un rommíng adecuado entre diferentes redes de la empresa. El uso de claves para los usuarios incrementa la seguridad para el acceso a la red; si un usuario ha logrado asociarse a los dispositivos inalámbricos pero no posee una cuenta creada en el servidor de autenticación, no podrá ingresar a ningún recurso, ni enviar tráfico a la red.

5.2 RECOMENDACIONES.

- Se recomienda a Gigowirleess, regularizar los enlaces inalámbricos y puntos de acceso implementados, para lo cual se debe llenar los formularios pertinentes para declaración de enlaces, tanto punto a punto como multipunto, mimos que deberán ser avalados por un portador y firmados por un Ingeniero en Electrónica, para posteriormente ser entregados en la Superintendencia de Telecomunicaciones (SUPTEL).

- Se recomienda tomar como referencia para el análisis de redes, la arquitectura SAFE de CISCO, la que permite efectuar un análisis ordenado y modular de la infraestructura. Además es adaptable a cualquier tipo de red, sea esta de una empresa pequeña o de una corporación con grandes recursos e infraestructura tecnológica, En cada módulo se agrupó componentes dando una idea organizada de la red implementada.

- En este proyecto se utilizó la topología punto – multipunto. Se recomienda investigar sobre la implementación de redes de acceso a Internet usando topología ad_hoc para el funcionamiento de redes MESH, que se caracteriza por formar un manto sobre un área y facilita el incremento de cobertura. El inconveniente a resolver sería el de definir los protocolos de enrutamiento a utilizarse para la comunicación entre los nodos y el direccionamiento de tráfico.

- Se recomienda el uso de portales cautivos que permitan el acceso a una red, sea esta cableada o inalámbrica, permitiendo ofrecer diferentes tipos de servicios “limitados por un tiempo”. Este esquema podría ser aplicable en Aeropuertos, Centro Comerciales, Ferias o Conjuntos Residenciales, para vender paquetes de servicios prepago.

ANEXOS

CONTENIDO

ANEXO A

ARQUITECTURA SAFE

ANEXO B

MODELOS DE PROPAGACIÓN

ANEXO C

SIMULACIÓN EKAHAU

ANEXO D

MANUALES DE EQUIPOS

ANEXO E

DETALLE DE FORMULARIOS PARA DECLARACIÓN DE ENLACES

ANEXO F

CONFIGURACIÓN DE EQUIPOS

Bibliografía

- DEVIN Akin, CWNP certified Wireless Network Administrador, Mc Graw Hill, California 2006.

- UNGER Jack, Deploying License-Free wireless Wide-Area Networks, CISCO Press 2003.

- KAEO, Merike; Diseño de Seguridades en Redes. Primera edición. PEARSON EDUCATION, S.A. Madrid. 2003.

- **Documentos CISCO SAFE**

- Best practices for securing routing protocols

- CONVERY Sean, MILLER Darrin, Wireless Lan security in depth

- TRUDEL Bernie, COVERY Sean, A security blueprint for enterprise networks

- HALPERN Jason, Vpn ipsec virtual private networks in depth.

- CORREA Cristian, Evaluación de enlaces de acceso inalámbricos usando protocolo IEEE 802.1, Junio 2005, Universidad de Tarapacá.

DIRECCIONES ELECTRÓNICAS

- VILLALÓN Huerta Antonio **Seguridad en Unix y Redes. Versión 2.1**, Julio 2002,

http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node1.html

- **Cálculo de margen de desvanecimiento,**

http://www.frsf.utn.edu.ar/catedras/sistemas/comunicaciones/herramientas/desvanecimiento.html**.**

- **Cálculo de Radio Enlaces,**

http://www.e-advento.com/tecnologia/calculos.php

http://www.fi.uba.ar/materias/6637/calculoweb.html

- **Tipos de equipos Homologados por SUPTEL,**

http://www.supertel.gov.ec/homologaciones/equipos/modulacion%20digital.htm

- **Normas y Reglamentos para declaración de enlaces de telecomunicaciones.**

http://www.conatel.gov.ec/website/servicios/serv_varios/banda_ancha.php?cod_cont=42

- **Censo de vivienda**

http://www4.quito.gov.ec/mapas/indicadores/Vivienda%20barrios.htm

http://www4.quito.gov.ec/mapas/indicadores/Pobreza_barrios.htm

GLOSARIO

I

IEEE.- Instituto de Ingenieros Eléctricos y Electrónicos, una asociación estadounidense sin fines de lucro, dedicada a la estandarización, se halla formada por profesionales de las nuevas tecnologías, como ingenieros de telecomunicaciones, ingenieros electrónicos e Ingenieros en informática.

EIRP (Equivalent Isotropically Radiated Power). - Es la potencia radiada por la antena, es importante por que es regulado por la FCC y se usa para el cálculo de enlaces.

ISP.- Proveedor de servicio de Internet, que revende el ancho de banda que provee un portador.

H

Hacker.- Es aquella persona con muy buenos conocimientos en informática y telecomunicaciones, que los utiliza dichos conocimientos en forma positiva o negativa, siempre al margen de la ley o sin autorización del Administrador de la red.

Hijacking.- En seguridad informática, significa secuestro del navegador, es la captura del navegador del sistema por parte de un malware (software maligno). El objetivo es mostrar publicidad mientras se navega y, en otros casos, capturar datos importantes sobre el usuario.

L

LLC.- Logical link control es un subcapa definida por la IEEE y es responsable del control de enlace lógico, maneja el control de errores, control del flujo, entramado y direccionamiento de la subcapa MAC.

M

MD5.- (acrónimo de *Message-Digest Algorithm 5)*. Algoritmo de Resumen del Mensaje 5. Es uno de los algoritmos de reducción criptográficos, la codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimal.

P

PKCS #7.- Es un conjunto de normas para firmar y encriptar documentos normalmente usado en el mail para la autenticidad y privacidad de los datos contenidos en ellos.

R

Radiador Intencional.- Es definido por la FCC como el dispositivo que radia señales de radio frecuencia, incluye conectores y cables pero no antena.

S

SPKI.- (Simple Public Key Infrastructure) Se caracteriza por definir tres tipos de certificados diferentes, los cuales contienen al menos un emisor y una entidad receptora (subject), pueden especificar períodos de validez, información de autorización e información de delegación.

Spoofing.- En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de

investigación. Existen diferentes tipos de spoofing; IP spoofing, ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

T

TLS.- Seguridad de la capa de transporte. Se halla definido en RFC 2246, es un protocolo para establecer una conexión segura entre un cliente y un servidor.

W

WLAN.- Son las siglas en inglés de Wireless Local Area Network. Es un sistema de comunicación de datos flexible muy utilizado como alternativa a la LAN cableada o como una extensión de ésta. Utiliza tecnología de radio frecuencia que permite mayor movilidad a los usuarios al minimizarse las conexiones cableadas.