UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

ESTUDIO, DISEÑO E IMPLEMENTACIÓN DE UN ENLACE INALÁMBRICO DE LARGO ALCANCE CON ANTENAS DIRECCIONALES DE LA EMPRESA COMPUFÁCIL

Estudiante

Robinson Carlos Barbecho Barbecho

Tutor

Ing. Diego Fajardo.

Cuenca Ecuador

Noviembre 2011

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE INGENIERÍA DE SISTEMAS

CERTIFICADO DE RESPONSABILIDAD

Yo, Ing. Diego Fajardo N., certifico que el señor Robinson Carlos Barbecho Barbecho con C.C, Nº. 0103654018 realizó la presente tesis con el título **"ESTUDIO, DISEÑO E IMPLEMENTACIÓN DE UN ENLACE INALÁMBRICO DE LARGO ALCANCE CON ANTENAS DIRECCIONALES DE LA EMPRESA COMPUFÁCIL"**, y que es autor intelectual del mismo, que es origina, auténtico y personal.

_____

Ing. Diego Fajardo

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE INGENIERÍA DE SISTEMAS

CERTIFICADO DE AUDITORÍA

El documento de tesina con título **"ESTUDIO, DISEÑO E IMPLEMENTACIÓN DE UN ENLACE INALÁMBRICO DE LARGO ALCANCE CON ANTENAS DIRECCIONALES DE LA EMPRESA COMPUFÁCIL"**, ha sido desarrollado por Robinson Carlos Barbecho Barbecho con C.C. Nº. 0103654018 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

_____

Robinson Barbecho

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE INGENIERÍA DE SISTEMAS

ACTA DE CESIÓN DE DERECHOS

Yo, Robinson Carlos Barbecho Barbecho, con C.C. Nº. 0103654018, estudiante de la carrera Ingeniería de Sistemas, declaro conocer y aceptar las disposiciones del Programa de Pregrado, que en lo pertinente dice: “Es patrimonio de la Universidad Tecnológica Israel, todos los resultados provenientes de trabajos investigativos, científicos o técnicos o tecnológicos, o productos tangibles y de tesis o trabajos de grado que se realicen a través o con el apoyo de cualquier tipo de la Universidad de Tecnológica Israel, esto significa la cesión de los derechos de propiedad intelectual a la Universidad Tecnológica Israel”.

_____

Robinson Barbecho

DEDICATORIA

Dedico a mi familia de manera muy especial a mi madre la cual en base a su esfuerzo se ha convertido en mi soporte en los momentos difíciles y en la luz que me ha iluminado durante este tiempo.

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a la Universidad Tecnológica Israel a sus profesores y en especial a mi tutor el Ing. Diego Fajardo por el apoyo brindado durante la realización de este documento.

RESUMEN

Actualmente las comunicaciones inalámbricas se han convertido un punto clave de toda empresa, ya que estas contribuyen en un mejor funcionamiento, logrando que varios departamentos tanto locales (dentro de un mismo edificio) como remotos (diferentes puntos de la ciudad) puedan trabajar simultáneamente de una manera mucho más dúctil en sus conexiones sin la utilización de cableado y con amplios beneficios.

El presente trabajo está orientado a proporcionar conocimientos y poner a consideración un análisis de las ventajas y beneficios que podemos obtener al utilizar un sistema de comunicación WMAN, además de diseñar el diagrama de la red inalámbrica y unir todos estos conceptos en un documento que sea de utilidad para el Administrador de Red basado en el estudio de la Ingeniería de Sistemas y en su rama que son las Redes de Computación.

SUMMARY

Currently, wireless communications have become key points of each company, because these contribute to improved performance, making several local departments (within the same building) and remote departaments (different parts of the city) can work simultaneously in a ductile way in their connections without the use of wired and with extensive benefits

The present work is aimed at providing knowledge and put to considerate an analysis of the advantages and benefits we can get by using a WMAN communication system, in addition to designing the wireless network diagram and unite all of these concepts in a document that is useful to the study of the Network Administrator, based on Systems Engineering and its branch is Computer Networks.

TABLA DE CONTENIDOS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

LISTA DE ANEXOS

CAPÍTULO I

INTRODUCCIÓN

La presente investigación se realizó con la recolección de información y su procesamiento para evaluar los sistemas de enlaces inalámbricos WMAN, mediante el análisis de coordenadas y capacidades de dispositivos y de esta forma determinar la factibilidad de su implementación.

El rendimiento y eficiencia al momento de utilizar estos enlaces para la empresa es de vital importancia. Para lo cual el administrador de la red debe identificar los mecanismos y herramientas que le permitan sacar el mayor provecho a los recursos de la red.

En la actualidad con el avance tecnológico y el uso de equipos que están en constate evolución, pone a disposición una variedad de estándares para redes inalámbricas, los cuales son de múltiple interés ya que se debe elegir el que mayor prestaciones de acuerdo a nuestras necesidades nos pueda dar para garantizar un funcionamiento óptimo para nuestra red.

En el presente trabajo se pondrá a consideración el uso de varias herramientas entre las cuales tenemos RADIO MOBILE entre otras.

1.1. PLANTEAMIENTO DEL PROBLEMA

¿Permitirá la implementación de enlaces de comunicación Wireless a las diferentes agencias agilitar la velocidad de atención a los clientes, mejorar la administración de la seguridad y la administración de los recursos de la empresa de mejor manera?

1.2. ANTECEDENTES

En las últimas décadas las telecomunicaciones han evolucionado considerablemente dando a lugar a nuevas exigencias y expectativas en cuanto al envió de la información y la velocidad a grandes distancias, convirtiéndose así en uno de los puntos más importantes para el éxito de las empresas en la actualidad. COMPUFACIL es una empresa fundada en 1999 la consta de una matriz ubicada la calle Remigio Crespo y dos agencias ubicadas en el centro Histórico y Totoracocha respectivamente esta empresa se dedica a prestar servicios como venta, arriendo y manteniendo de equipos a más de soluciones informáticas como implementación de servidores, dominios, redes de datos y digitalización siendo esta una de sus ramas más fuertes con marcas como Epson y Xerox a más administradores de contenido como

SharePoint y Docushare ya que es una de las pocas empresas que se dedica a este ámbito en la ciudad de Cuenca .

Al momento la empresa cuenta con algunos problemas en sus agencias debido a la lentitud en la conexión con los sistemas de la empresa lo cual dificulta la atención a sus clientes ya que la generación de facturas es exageradamente demorada, la empresa busca reducir los costos que se generan al tener una conexión de INTERNET para cada agencia y mejorar la seguridad de los datos que genera está a más de controlar lo que los usuarios pueden tener como aplicativos en sus equipos, por lo que la empresa tiene la necesidad de implementar una tecnología que permita compartir estos recursos reduciendo costos de operación

Debido a esta de problemática la implementación de un enlace inalámbrico solventaría las necesidades de comunicación y seguridad

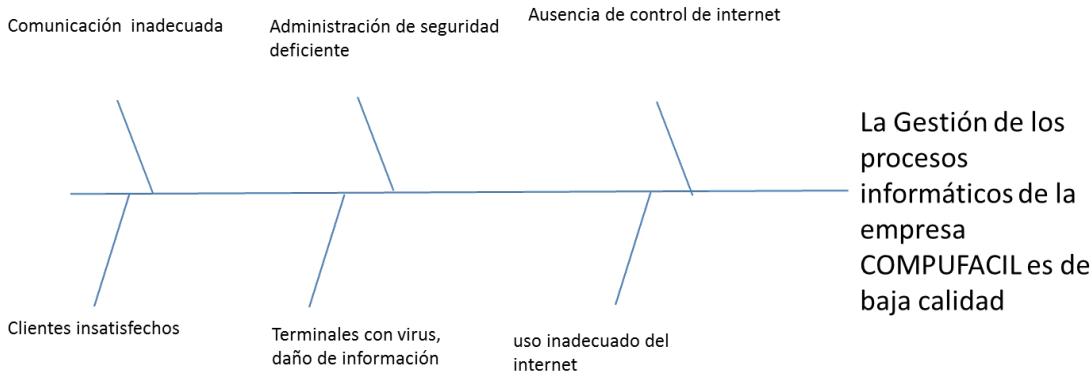
1.3. DIAGNÓSTICO

La empresa COMPUFACIL requiere el diseño y la implementación de un sistema de comunicación el cual sea confiable, veloz y seguro el cual permita comunicar sus dos agencias a la matriz y poder administrar la seguridad, sistemas, uso del INTERNET, control de impresión por usuario y demás

recursos que la empresa pudiese implementar a más de reducir costos por comunicación y mejorar la atención al cliente en cada una de las agencias.

Al momento los usuarios no tienen ningún control sobre el uso del INTERNET, programas instalados ni administración de aplicaciones que en la matriz se tienen centralizados tales como el estado de su antivirus, lo cual genera problemas de virus constantemente, la saturación del ancho de banda con el que cuenta cada agencia con programas p2p los cuales no están autorizados y por la no aplicación de las políticas de seguridad los usuarios lo pueden instalar libremente causando los problemas ya mencionados.

Causa - efectos



Pronóstico y control del pronóstico

La no implementación de estos enlaces provocarían a la empresa gastos exagerados en mantenimiento ya que se tendría gastar tiempo y dinero en dar

mantenimiento a estos equipos a más de que se deterioraría las relaciones con los clientes ya que periódicamente una terminal de facturación se encontraría sin poder atender a clientes afectando a la calidad de atención a mas poner en riego información de la empresa por virus existentes en los equipos y el uso indebido del INTERNET por parte de los usuarios.

Se pretende implementar en la empresa una comunicación fluida y confiable la cual disminuiría considerablemente los costos de operación y los tiempos que se dedica a la administración y mantenimiento de las agencias.

1.4. FORMULACIÓN DE LA PROBLEMÁTICA ESPECÍFICA

La deficiencia en la calidad en las telecomunicaciones de la empresa

Problema principal

Deficiente manejo de los recursos con los que cuenta la empresa tales como antivirus centralizado, impresoras compartidas, sistemas como SysAid, Ajesoft, RCMS.

Problemas secundarios:

- Baja calidad de comunicaciones existentes
- Inexistencia de aplicación de normas de seguridad a nivel de agencias
- Hardware inadecuado que no cubre las necesidades de la empresa
- Configuración inadecuada de elementos existes

1.5. OBJETIVOS

Objetivo general

Diseñar un enlace inalámbrico que permita agilitar la atención al cliente, compartir los recursos de la empresa, contar con una administración centralizada y disminuir costos de una forma confiable y segura en las agencias de COMPUFACIL.

Objetivos específicos

- Realizar un análisis técnico que garantice la calidad de la comunicación en los enlaces WMAN, lo que obliga a tomar en consideración los distintos tipos de tecnología que existe al momento.

- Analizar las diferentes medidas de seguridad existentes en el medio, tales como tipos de cifrado, filtros de direcciones MAC, y su posterior implementación.

- Adquirir hardware de calidad acorde a los requerimientos de la empresa y al factor económico

- Configurar e implementar el hardware acorde a las necesidades de la empresa

1.6. JUSTIFICACIÓN

Justificación teórica

La razón principal de esta investigación es la necesidad de la empresa por mejorar la gestión de recursos a través de sus comunicaciones, la cual no sólo se podría implementar en COMPUFACIL sino en otras empresas que lo requieran debido a la gran demanda de estos servicios en el AUSTRO.

Los enlaces inalámbricos son una tecnología que pueden ayudar a conectar distintos puntos de una empresa que se encuentren a distancias considerables. No se necesita una licencia para poder utilizar estos medios ya

que utilizan ondas de radiofrecuencia de baja potencia y una banda especifica que se puede usar libremente para comunicar dispositivos, lo cual propicia que tenga un crecimiento considerable en los últimos años, convirtiéndolo en uno de los más usados en la transmisión de datos por sus múltiples ventajas. Las mismas nos permitirían tener una mejor administración y reducir costos considerablemente en las comunicaciones, por lo que hemos decidido implementar esta tecnología en la empresa COMPUFACIL.

Justificación Metodológica

El enlace contará con una antena en cada agencia las cuales se conectarán a otras que se implementarán en una torre que está ubicada en el sector de ICTOCRUZ que adquirió la empresa para este fin, con lo que los equipos se podrán comunicar si problema alguno con una buena calidad de la señal.

Justificación Práctica

El resultado de este proyecto tiene una aplicación práctica, ya que nos permitirá mejorar las comunicaciones y sistemas mediante un análisis de las tecnologías que se pudiesen implementar en esta y en otras empresas al querer implementar este tipo de comunicaciones, influyendo principalmente en

el control que se puede tener de los recursos utilizados por los usuarios pudiéndose administrar que y cuando lo utilizan mediante las políticas del dominio de la empresa, a más de agilitar la atención al cliente mediante la fluidez de los datos en los diferentes procesos.

CAPÍTULO II

MARCO DE REFERENCIA

2.1. MARCO TEÓRICO

HISTORIA WIRELESS:

"Nokia y Symbol Technologies crearon en 1999 una asociación conocida como WECA (Wireless Ethernet Compatibility Alliance, Alianza de Compatibilidad Ethernet Inalámbrica). Esta asociación pasó a denominarse Wi-Fi Alliance en 2003. El objetivo de la misma fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos.

De esta forma, en abril de 2000 WECA certifica la interoperabilidad de equipos según la norma IEEE 802.11b, bajo la marca Wi-Fi. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos. Se puede obtener un listado completo de equipos que tienen la certificación Wi-Fi en Alliance - Certified Products.

En el año 2002 la asociación WECA estaba formada ya por casi 150 miembros en su totalidad.

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red Wi-Fi de una red Ethernet es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (Ethernet).”[1]

LA COMUNICACIÓN INALÁMBRICA

“Se entiende por comunicación inalámbrica a todo aquel sistema que nos permite comunicarnos por medio de ondas electromagnéticas, permitiéndonos así evitar el uso de algún tipo de cableado.

La tecnología WLAN se utiliza ondas electromagnéticas para transportar información de un punto a otro, para este objetivo se hace uso de ondas portadoras. Estas ondas son de una frecuencia mucho más alta que la onda moduladora (la señal que contiene la información a transmitir). La onda moduladora se acopla con la portadora, a esto se llama modulación, surgiendo

[1] Recuperado de: HTTP://ES.WIKIPEDIA.ORG/WIKI/WI-FI

una señal de radio que ocupa más de una frecuencia (un ancho de banda) debido a que la frecuencia de la primera se acopla a la de la segunda. Gracias a esto pueden existir varias portadoras simultáneamente en el mismo espacio sin interferirse, siempre y cuando se transmitan en diferentes frecuencias. Otra ventaja de la modulación mediante ondas portadoras es la mayor facilidad en la transmisión de la información. Resulta más barato transmitir una señal de frecuencia alta (como es la modulada) y el alcance es mayor. El receptor se sintoniza para seleccionar una frecuencia de radio y rechazar las demás, tras esto demodulará la señal para obtener los datos originales, es decir, la onda moduladora. Como curiosidad, el dispositivo electrónico encargado de esta tarea se llama módem debido a que MOdula y DEModula."[2]

TIPOS DE REDES INALÁMBRICAS

Los tipos de redes inalámbricas dependen de su alcance por lo que se ha clasificado en: WPAN, WLAN y WMAN.

PROTOCOLOS DE COMUNICACIÓN INALÁMBRICO

Para que una red del tipo que fuese funcione correctamente, se requiere de varios protocolos de comunicación, siendo el IEEE 802.x un conjunto de

[2] RECUPERADO DE http://histinf.blogs.upv.es/2010/12/02/historia-de-las-redes-inalambricas/#more-1150

estándares para las tecnologías de área local inalámbrica (WLAN), siendo uno de los más utilizados el IEEE 802.11b al cual se lo denomina Wi-Fi.

El alcance depende esencialmente de la potencia del equipo emisor dato que nos suele suministrar el fabricante.

En la actualidad existen varios métodos de transmisión como son: 802.11 legacy, 802.11a, 802.11b, 802.11g, 802.11 Súper G, 802.11n, 802.11e.

TOPOLOGÍAS

Existen 2 topologías básicas que pueden implementarse en el protocolo 802.11: Redes sin infraestructura o Ad-hoc (IBSS) y Redes con Infraestructura (BSS).

Redes ad-hoc sin infraestructura (IBSS, *Independent Basic Service Set*)

El IEEE 802.11 es un estándar que describe los protocolos y las técnicas de transmisión de datos correspondientes a los dos modos principales de construir y utilizar una LAN inalámbrica RF.

El estándar contempla una parte la comunicación en redes "ad-hoc" simples. Estas redes están compuestas por varias estaciones de trabajo con un alcance de transmisión limitado e interconectadas entre sí. No obstante, estas topologías no necesitan ningún sistema de control ni de transmisión central.

Redes con infraestructura (BSS, *Basic Service Set*)

Otra aplicación importante que se describe en el estándar IEEE 802.11 utiliza "puntos de acceso". Los puntos de acceso son componentes de red que controlan y gestionan toda la comunicación que se produce dentro de una célula LAN inalámbrica, entre células LAN inalámbricas y, finalmente, entre células LAN inalámbricas y otras tecnologías LAN. Los puntos de acceso garantizan un empleo óptimo del tiempo de transmisión disponible en la red inalámbrica.

MEDIO AMBIENTE

El espacio libre (aire), es el medio utilizado para la transmisión de datos convirtiéndose este en un aspecto importante al momento de ingresar los parámetros en Radio Mobile, por lo que es de gran importancia analizar las características del medio de transmisión para tener en cuenta que fenómenos atmosféricos pueden afectar la calidad de transmisión.

Radio Mobile utiliza el modelo Longley-Rice, este modelo requiere de algunos parámetros:

Polarización: debe especificarse si se trabaja con polarización horizontal o vertical. El modelo de Longley-Rice asume que ambas antenas tienen la misma polarización, vertical y horizontal.

Refractividad: la refractividad de la atmósfera determina la cantidad de "bending" o curvatura que sufrirán las ondas radio. En otros modelos, el parámetro de refractividad puede introducirse como la curvatura efectiva de la tierra, típicamente 4/3 (1.333). Para el modelo Longley-Rice, hay tres formas de especificar la refractividad. Se puede introducir el valor de refractividad de superficie directamente, típicamente en el rango de 250 a 400 Unidades de n (correspondiente a valores de curvatura de la tierra de 1.232 a 1.767). Una curvatura efectiva de la tierra de 4/3 (=1.333) corresponde a una refracrtividad de superficie de valor aproximadamente 301 Unidades de n. Longley y Rice recomiendan este último valor para condiciones atmosféricas promedio. La relación entre los parámetros "k" y "n", viene dada por la siguiente expresión:

$$N_s = 179.3 \cdot Ln\left[\frac{1}{0.046665}\left(1 - \frac{1}{K}\right)\right]$$

Permitividad: la permitividad relativa o constante dieléctrica del medio (ε), tiene unos valores típicos tabulados.

Clima: Hay 7 modelos de clima caracterizados en el modelo: Equatorial (Congo); Continental Subtropical (Sudan); Maritime Subtropical (West coast of Africa); Desert (Sahara); Continental Temperate; Maritime Temperate, over land (United Kingdom and continental west coasts); Maritime Temperate, over sea.

De acuerdo con el modelo, el clima continental templado es común a la mayor parte de grandes superficies en la zona templada. Se caracteriza por extremos en la temperatura y cambios diurnos y de estaciones pronunciadas en la propagación. En latitudes medias en zonas costeras, donde los vientos predominantes llevan el aire húmedo marítimo hacia el interior, prevalece un clima marítimo templado. Esta situación es típica del Reino Unido y de las costas occidentales de los Estados Unidos y Europa. El resto de los climas pueden asociarse de la misma forma a otras regiones del mundo.

Variabilidad: el modelo de Longley-Rice define cuatro modos de variabilidad. El modo seleccionado determina el significado de la fiabilidad de los valores usados en el modelo. El modo de variabilidad puede ser considerado como la especificación para determinar la fiabilidad de los cálculos. Los modelos de variabilidad definidos son: *Single message mode, Individual mode, Mobile mode, and Broadcast mode.*

El modo individual (“Accidental”), para calcular el campo en posiciones individuales se trazaban múltiples puntos a lo largo de varias radiales desde la ubicación del transmisor. Como estamos definiendo exactamente la localización del receptor para cada cálculo, el programa no tiene en cuenta la variabilidad por “localizaciones” o posición.

Los tipos de variabilidad descritos en el modelo Longley-Rice son el tiempo, la posición, y la variabilidad de situación. Estas tres dimensiones de variabilidad, fueron desarrolladas para considerar y clasificar variaciones en los niveles de señal medidos (mediana) La variabilidad de corto plazo del tipo asociado con la propagación de multitrayecto no es cubierta por el modelo.

Variabilidad de tiempo: los parámetros a tener en cuenta para considerar las variaciones de los valores medianos tomados por horas de atenuación, son por ejemplo, cambios de la refracción atmosférica o de la intensidad de turbulencia atmosférica. El campo actual en la posición de receptor se espera que esté por encima de ese valor, durante media de cada hora, y por debajo de ese valor la otra media. La variabilidad de tiempo describe los efectos de estos cambios de tiempo, expresado como un porcentaje entre 0.1 % y el 99.9 %. Este valor da la fracción de tiempo durante la cual el campo de fuerzas recibido, se espera que sea igual o superior que el valor mediano de campo por hora calculado por el programa. Esta variabilidad permite especificar cómo se desea tratar con la variabilidad de tiempo de los cambios atmosféricos y otros efectos. Tomar un

porcentaje mayor en este valor, reduce la variabilidad resultante de estos factores. El resultado calculado por el programa será menor, con lo que se asegura que el valor real medido será igual o superior en un porcentaje más elevado de tiempo.

Variabilidad por localización: Lo que hay que tener en cuenta en los estadísticos de largo plazo entre dos trayectos distintos debido, a por ejemplo, diferencias en los perfiles del terreno o diferencias ambientales entre ellos. La variabilidad por localización para los cálculos, se expresa como un porcentaje de 0.1% a 99.9%. Sucede lo mismo en los resultados que para el caso de la variabilidad de tiempo, pero con la fracción de localizaciones donde el campo recibido se espera que sea igual o superior.

Variabilidad por situación: esta variabilidad tiene en cuenta otro tipo de variables que pueden denominarse “hidden variables”. Este tipo de variables representan efectos que no pueden explicarse o que simplemente se ha decidido no controlar. Sirven para diferenciar casos con iguales equipos y condiciones de entorno similares. Estos cambios se reflejarán en los estadísticos. Y como en casos anteriores puede ser expresado como un porcentaje entre 0.1 % y el 99.9 % para controlar lo mucho o poco que se quiere que afecten.

SEGURIDAD

La seguridad en el campo inalámbrico es un aspecto muy importante ya que en una red inalámbrica una tercera persona podría entrar a nuestra red si siquiera estar en las dependencias de nuestra empresa ya que bastaría con estar en un lugar en el cual llegue la señal para realizar un ataque el cual no dejaría siquiera huellas en el caso de ser uno pasivo.

Métodos de aseguramiento una WMAN

Para poder asegurar una red WMAN contamos con métodos como: Filtrado de Direcciones MAC, Cifrado WEP, Cifrado WPA, cifrado WPA2, Clave compartida (WPA y WPA2) y 802.1x, encriptación y consideraciones que se deben tomar al momento de elegir una clave de seguridad.

TIPOS DE ANTENAS WIFI

“Existen 2 tipos de antenas según como se quiera amplificar esa distancia:

Antenas Direccionales:

Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance, actúa de forma parecida a un foco de luz que emite un haz concreto y estrecho pero de forma intensa (más alcance).

El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del Access Point emisor y la sensibilidad de recepción del Access Point receptor.

Antenas Omnidireccionales:

Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones con menor alcance.

Las antenas Omnidireccionales “envían” la información teóricamente a los 360 grados por lo que es posible establecer comunicación

independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

CAPÍTULO III

METODOLOGÍA

3.1. MARCO TEÓRICO REFERENCIAL

La metodología es el estudio sistemático y operacional de los métodos utilizados en la investigación científica, en sus diferentes áreas del saber humano y lograr perfeccionar la inteligencia creadora.

La metodología de la investigación nos permite engrandecer nuestros conocimientos de la naturaleza, de la sociedad y del hombre utilizando los métodos adecuados en la investigación.

3.1.1. Método Deductivo

La deducción es un proceso discursivo y descendente, pasa de lo generala lo particular, esta se la puede considerar, como una demostración lógica donde necesariamente se la puede relacionar como una inferencia mediata o silogismo.

3.1.2. Método Analítico

El método analítico consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular. Es necesario conocer la naturaleza del fenómeno y objeto que se estudia para comprender su esencia. Este método nos permite conocer más del objeto de estudio, con lo cual se puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías.

3.1.3. Técnicas.

Encuesta.- La encuesta es una técnica destinada a obtener datos de varias personas cuyas opiniones impersonales interesan al investigador. Para ello, a diferencia de la entrevista, se utiliza un listado de preguntas escritas que se entregan a los sujetos, a fin de que las contesten igualmente por escrito. Ese listado se denomina cuestionario.

Es impersonal porque el cuestionario no lleve el nombre ni otra identificación de la persona que lo responde, ya que no interesan esos datos.

3.2. METODOLOGÍA APLICADA

Debido al crecimiento de la empresa y la demanda de los clientes por un buen servicio hizo necesaria la implementación de esta red inalámbrica como una solución de movilidad, flexibilidad y productividad.

Para esta conexión se utiliza el estándar IEEE 802.11n que establece especificaciones para los dispositivos y las comunicaciones en redes inalámbricas además especifica también mecanismos de encriptación para realizar la protección de los datos trasmitidos.

Análisis del problema

Para una correcta implementación es necesario realizar el análisis adecuado del problema, por lo que se creyó conveniente realizar una breve pero precisa encuesta que nos ayude a aclarar los inconvenientes presentados.

Formulario de encuesta (ver a anexo I)

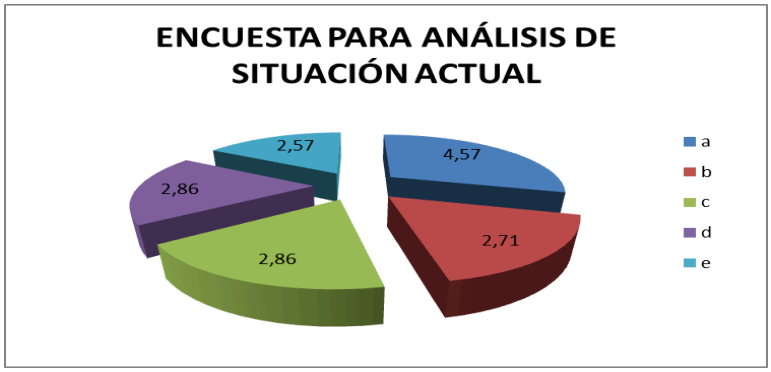


Gráfico 2 Encuesta para análisis de situación actual.

Análisis de requerimientos

Una vez definido el estándar a utilizar definiremos los requerimientos de funcionalidad que se deben cumplir así como los técnicos que implica la implementación de la solución.

Requerimientos funcionales

Al realizar la implementación de la red inalámbrica para la empresa es necesario considerar los siguientes requerimientos funcionales:

- Ofrecer acceso a los servicios y sistemas que tiene la empresa en todas sus localidades.
- Habilitar el acceso a los recursos informáticos para todos los locales.

Requerimientos técnicos

Consideraremos:

- Homogeneidad de dispositivos para conexión punto a punto
- Cobertura mínima de 3 a 4 kilómetros.
- Velocidad de transmisión de 70 Mb/s
- Soporte para tecnología MIMO
- Compatibilidad con estándares 802.11n

3.3. ANALISIS FINANCIERO

La administración financiera de negocios busca identificar los cursos de acción que tienen el mayor efecto positivo en el valor de la empresa para sus propietarios. Para esto es necesario establecer cuál es el valor de la empresa en el momento de la decisión y a través de qué caminos puede aumentarse este valor (actuando sobre los recursos que se emplean y los medios de financiamiento que se utilizan). El análisis financiero proporciona a los directivos y propietarios una medida del efecto esperado que tienen las decisiones estratégicas y de gestión en el valor de la empresa.

Un parámetro importante para la ejecución de proyectos es realizar un análisis financiero para poder establecer la cantidad y valor de recursos que se necesitarán para su aplicación, ya que la implementación de un sistema de

comunicación contrae un costo beneficio a través del tiempo, brindando a la empresa canales de comunicación eficientes y eficaces.

Costo Actual del Mantenimiento

La empresa CompuFácil Cía. Ltda., ha generado los siguientes gastos mensuales en mantener la comunicación entre sus edificios, a continuación se detallan los egresos generados:

Tabla 1 Costos mensuales de mantenimiento

Varios	Costo mensual
Servicio de internet	320
Mantenimiento	80
Eventualidades	30
Dispositivos	20
Transporte	28
TOTAL	478

Este cuadro detalla los gastos de operación que ocasionan mensualmente el mantenimiento de la red como se encuentra en la actualidad.

El costo mensual de mantenimiento es de $ 478 lo que al año nos genera un costo de $5736.

Costo de la aplicación de una red wireless

El costo del proyecto está referido a varios costos que corresponden a estudios de campo, personal involucrado en el proyecto, equipos necesarios, recursos materiales y económicos.

Proyecto de Inversión (conceptualización)

El costo de un bien constituye el conjunto de esfuerzos y recursos que han sido invertidos con el fin de producirlo, en este caso la inversión se está realizando a un servicio de transferencia de información.

Tiene como objetivos aprovechar los recursos para mejorar las condiciones de vida de una comunidad, pudiendo ser a corto, mediano o a

largo plazo. Comprende desde la intención o pensamiento de ejecutar algo hasta el término o puesta en operación normal.

Responde a una decisión sobre uso de recursos con algún o algunos de los objetivos, de incrementar, mantener o mejorar la producción de bienes o la prestación de servicios.

Costo de Elaboración y realización del Proyecto

El costo de elaboración del presente proyecto, está referido a factores como lo son: tiempo de investigación, realización y documentación; valores presentados y detallados a continuación:

COMPUFACIL CIA LTDA			
DISEÑO DE RED WIRELESS			
DESCRIPCION DE LA ACTIVIDAD	**CANTIDAD**	**VALOR/U.**	**SUBTOTAL**
Recopilación de Información	30 horas	$ 3,00	$ 90,00
Investigación de Campo	10 horas	$ 3,00	$ 30,00
Realización del diagnóstico de dispositivos actuales	4 horas	$ 3,00	$ 12,00
Propuesta de aplicación de enlaces inalámbricos	10 horas	$ 3,00	$ 30,00
Investigación de metodología, normas y estándares	20 horas	$ 3,00	$ 60,00

Aplicación de la metodología para la red	5 horas	$ 3,00	$ 15,00
Implementación de la red	40 horas	$ 3,00	$ 120,00
Pruebas de funcionamiento	5 horas	$ 3,00	$ 15,00
Manual de la Enlaces Inalámbricos (usuario y configuraciones)	15 horas	$ 3,00	$ 45,00
Varios (Movilización, esferos copias)	1	50	$ 50,00
	TOTAL		**$ 467,00**

Tabla 2 Costo de Elaboración del Proyecto

Costo de Implementación del Proyecto

Los dispositivos que se necesitan para la implementación de la nueva red, son lo que se detallan a continuación:

Tabla 3 Costo de implementación del Proyecto

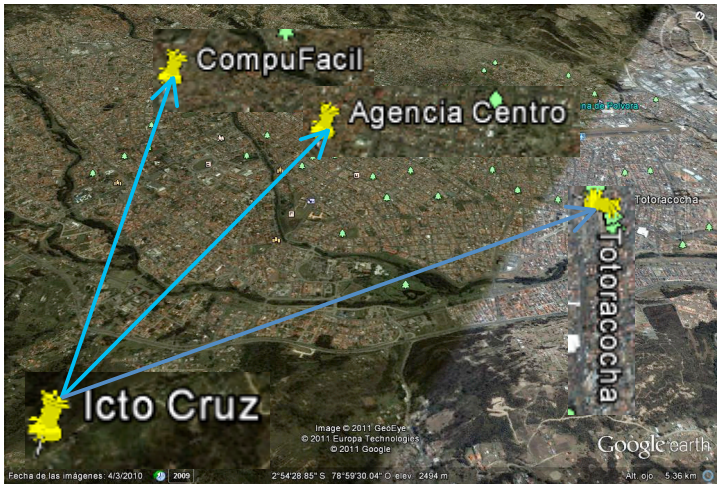
Dispositivo	Marca	Valor	Cantidad	Subtotal
Antena Powerbridge M5	Ubiquiti	450	6	2700
Swicht DES-1008D	D-link	16	1	16
Cable de Red	Nexx	0,60	58	34,80
Conectores RJ45	Nexx	0.30	21	6,30
Tubo Conduit		0.15	20	3
Amarras plásticas		0,03	40	1,20
TOTAL				**2761,00**

Para la implementación de este proyecto se han escogido estos dispositivos pretendiendo que los mismos cumplan normas y especificaciones aplicadas por la IEEE, para asegurar que este proyecto tendrá al menos diez años de vida útil y podrá soportar tecnologías futuras.

El costo total del este proyecto es de $ 3228,00 lo que al año nos significaría un ahorro de 2.508,00.

3.4. ANÁLISIS DE LA IMPLEMENTACIÓN

Una vez establecidos los requerimientos funcionales y técnicos se procede a la revisión de la ***línea de vista***[3], entre las localidades (Matriz, Centro y Totoracocha) con el sector de Icto Cruz en el cual se encuentra la torre que realiza la interconexión entre cada uno de los puntos.



[3] Línea de vista: es el espacio libre que existe entre dos puntos.

Gráfico 3 Línea de Vista de Agencias

Realizada la correspondiente verificación de espacio físico y de una adecuada línea de vista directa entre cada una de las agencias y la torre. Posteriormente se procede a ubicar cada una con sus respectivas coordenadas.

Ubicación de coordenadas

Para la ubicación de coordenadas dentro del mapa se utiliza Google Earth[4], esta herramienta nos permite ubicar las agencias en el mapa y obtener las coordenadas necesarias, esta información se vuelve de vital importancia ya que sumada a la información técnica de los dispositivos escogidos podremos obtener el cálculo de la factibilidad técnica.

Factibilidad técnica

Ya con las coordenadas de las agencias donde se va a implementar podremos realizar el cálculo de factibilidad técnica de estos mediante Radio

[4] Google Eart.- programa informático similar a un Sistema de Información Geográfica (SIG), creado por la empresa Keyhole Inc., que permite visualizar imágenes en 3D del planeta, combinando imágenes de satélite, mapas

Mobile[5], confirmando la factibilidad de poder implementar cada uno de los enlaces requeridos. Con estos datos confirmados se procede ya a la configuración de los equipos tanto en su parte de comunicación como de seguridad.

3.5. ANÁLISIS DE RESULTADOS

Para un correcto análisis posterior a la implementación se creyó conveniente aplicar la misma encuesta, ya que nos ayudara a verificar la solución o no del problema planteado.

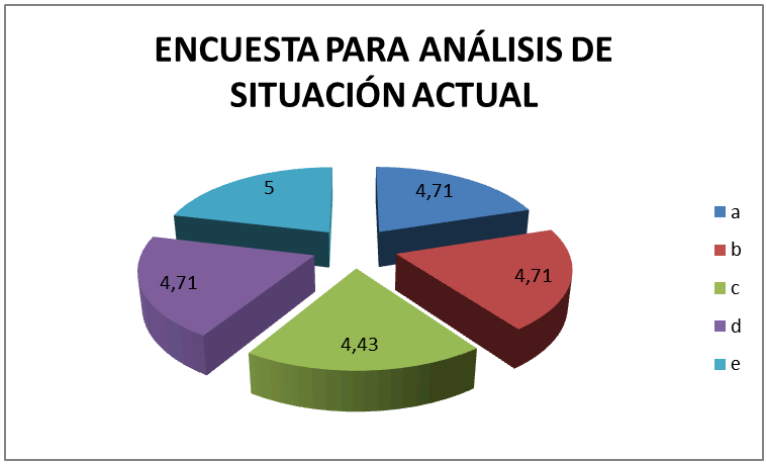


Gráfico 4 Análisis de Resultados

[5] Radio Mobile.- Software de libre distribución para el cálculo de radio enlaces de larga distancia en terreno irregular. (Funcionamiento detallado. Capitulo IV)

CAPÍTULO IV

DESARROLLO

4.1. TIPOS DE REDES INALÁMBRICAS

Los tipos de redes inalámbricas dependen en gran medida de su alcance y del tipo de onda electromagnética que utilicen, por lo que según su tamaño se ha encontrado las siguientes redes que las clasificaremos de menor a mayor.

4.1.1. WPAN

Con este tipo de redes se utiliza tecnologías como **HomeRF, Bluetooth, ZigBee y RFID. Estas son redes personales de poco alcance**

Las redes inalámbricas de área personal (**WPAN**) incluyen redes de corto alcance que engloban un área de varias decenas de metros. Este tipo de red se usa generalmente para conectar periféricos (como por ejemplo, teléfonos móviles, impresoras, electrodomésticos) como también pudiese ser

un asistente personal digital (PDA) a un computador sin conexión por cables. Podemos además conectar de forma inalámbrica dos ordenadores que se encuentren a corta distancia. Utilizamos varios tipos de tecnología para las WPAN:

Bluetooth

Es la tecnología WPAN principal, Ericsson lanzo está en 1994. Ofreciendo una velocidad máxima de 1 Mbps con treinta metros como su alcance máximo. A la tecnología Bluetooth, también se le conoce como IEEE 802.15.1, que tiene como ventaja el tener un bajo consumo de energía, lo que resulta ideal para usarla con periféricos pequeños.

La HomeRF (Home Radio Frequency)

Lanzada en 1998 por HomeRF Working Group que incluía a los fabricantes Intel, HP, Compaq, Microsoft y Motorola, entre otros ofreciendo una velocidad máxima de 10 Mbps con un alcance de 50 a 100 metros sin amplificador. Muy a pesar de contar con el respaldo de Intel, el estándar HomeRF se abandonó en enero de 2003, debido a que en su gran mayoría los fabricantes de procesadores tomaron para su uso la tecnología Wi-Fi (mediante

la tecnología Centrino, que incluía un microprocesador y un adaptador Wi-Fi en un solo componente).

Zigbee

Es una tecnología (también conocida como IEEE 802.15.4) con la cual también se puede conectar dispositivos en forma inalámbrica a un coste muy bajo y con bajo consumo de energía. Resultando particularmente adecuada ya que se integra directamente en aparatos electrónicos como, electrodomésticos, sistemas estéreos y juguetes. Esta funciona en la banda de frecuencia de 2,4 GHz y en 16 canales, y puede alcanzar una velocidad máxima de transferencia de hasta 250 Kbps con un alcance límite de unos 100 metros.

Los infrarrojos

Son conexiones que se pueden utilizar para crear enlaces inalámbricos en un radio de unos pocos metros, cuyas velocidades pueden alcanzar unos pocos megabits por segundo. Esta tecnología se usa ampliamente en aparatos electrónicos del hogar (como los controles remotos), pero puede sufrir interferencias debidas a las ondas de luz.

4.1.2. WLAN:(Wireless Local Area Network)

En las redes de área local se puede encontrar tecnologías inalámbricas basadas en HiperLAN (High Performance Radio LAN), o tecnologías basadas en Wi-Fi (Wireless-Fidelity).

Una red de área local inalámbrica (WLAN) es una red de área local (LAN) que no depende de la conexión por cable Ethernet. Una WLAN puede ser una extensión de una red con cable de corriente o una alternativa a ella.

Las WLAN tienen velocidades de transferencia de datos que van de 1 a 54 Mbps, con algunos fabricantes que ofrecen soluciones de 108Mbps de propiedad. El estándar 802.11n puede llegar a 300 o 600 Mbps.

Una señal de WLAN se puede emitir para cubrir un área que van desde una pequeña oficina a un campus de gran tamaño. Por lo general, un Access Point WLAN proporciona acceso en un radio de 65 a 300 pies.

WLAN Tipos

Casa privada o pequeño negocio WLAN

Por lo general, una WLAN de casa o negocio emplea a uno o dos puntos de acceso para transmitir una señal entre 100 a 200 metros de cobertura. Estos quipos se puede encontrar para instalar una WLAN doméstica en muchas tiendas al por menor.

Con pocas excepciones, el hardware de esta categoría se suscribe a la 802.11a, b, g o normas (también conocido como Wi-Fi), y algunos casos las WLAN de oficina ahora se adhieren al nuevo estándar 802.11n. Además, por motivos de seguridad, muchos hogares y oficinas WLAN se adhieren al estándar Wi-Fi Protected Access 2 (WPA2).

WLAN de clase Enterprise

Una empresa de clase WLAN emplea un gran número de puntos de acceso individuales para transmitir la señal a una amplia zona. Los puntos de acceso tienen más características que el equipo de casa o pequeña oficina

WLAN, tales como una mayor seguridad, autenticación, administración remota y herramientas para ayudar a la integración con las redes existentes. Estos puntos de acceso tienen una mayor área de cobertura que los de casa o de una oficina pequeña, y están diseñados para trabajar juntos para cubrir un área mucho más grande. Estos equipos pueden trabajar con el estándar 802.11a, b, g, o con las normas de seguridad de refinación, tales como 802.1X y WPA2.

4.1.3. WMAN

Las Wireless MAN satisfacen las necesidades de redes en áreas metropolitanas, como las ciudades y zonas rurales específicas. Por lo general, proporcionan las interconexiones entre usuarios fijos. En la mayoría de los casos, estas redes ofrecen conexiones fijas al aire libre.

Wireless MAN ofrecen un alto retorno sobre la inversión porque las empresas pueden evitar el arrendamiento o la instalación de circuitos caros de cobre o de enlaces de fibra óptica. De hecho, a veces es imposible la instalación de una red de cable entre dos puntos cuando el derecho de vía de las restricciones de prohibir la instalación de cables. Por ejemplo, una empresa puede utilizar los componentes de una Wireless MAN para comunicaciones de datos entre la sede central y un centro de distribución cercano.

En muchos casos, las empresas pueden ahorrar lo suficiente con una

conexión inalámbrica con lo cual pagaría por el equipo en uno o dos años. Esto sin duda le da incentivo para cualquier empresa que necesite para establecer comunicaciones entre edificios repartidos a lo largo de un área metropolitana.

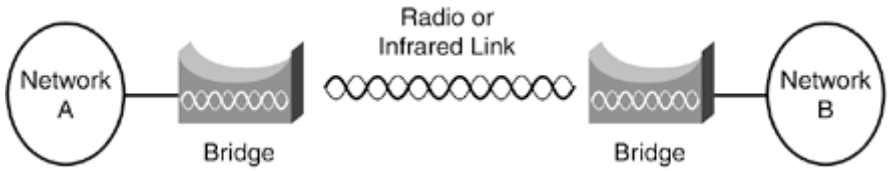
Componentes de redes inalámbricas MAN

Componentes de un MAN inalámbricas en general, vienen en pares, ya que soportan conectividad inalámbrica fija de un punto a otro. Revisaremos a los principales componentes de un MAN inalámbrica.

Bridges

Un bridge es un dispositivo que se utiliza para conectar dos o más redes del mismo tipo, como si fuesen una sola. Estos transmiten los paquetes de datos de una dirección a otra independientemente del protocolo de transmisión utilizado.

Gráfico 5 Bridges que permiten la conexión de dos redes



Un bridge inalámbrico se encuentra por lo general en cada extremo del enlace punto a punto, como los que interconectan dos edificios. Un Bridge tiene un puerto de conexión de cable que se conecta a la red y un puerto inalámbrico

que se conecta con un transmisor-receptor. Este recibe paquetes en un puerto y lo retransmite a otro puerto. Un Bridge no se iniciará la retransmisión hasta que se recibe un paquete completo. Debido a esto, las estaciones de ambos lados pueden transmitir paquetes simultáneamente sin colisiones.

Los Bridge de red son transparentes para los usuarios. Los paquetes se envían de forma automática atreves de este. De hecho, los usuarios no tienen idea de que sus paquetes están atravesando un enlace que conduce a una ubicación diferente.

Bridges de grupos de trabajo

Bridges para grupos de trabajo son la respuesta para la conexión de redes inalámbricas de mayor tamaño a redes Ethernet cableadas. Un bridge de grupo de trabajo actúa como un cliente inalámbrico en la red inalámbrica, y luego en las interfaces de una red cableada. La parte cableada se conecta a un switch Ethernet que conecta varios dispositivos.

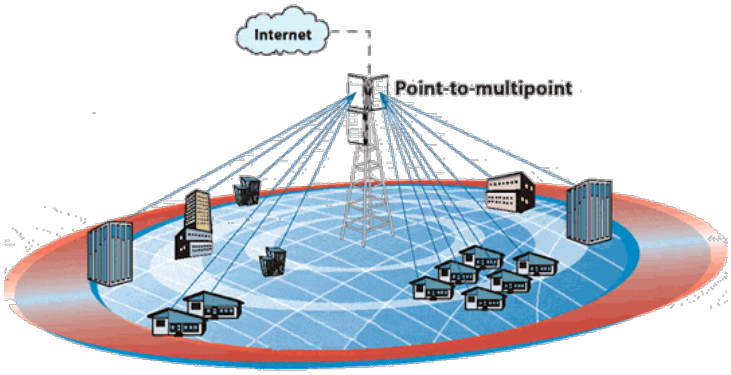
4.2. TIPOS DE ANTENAS

En la conexión Wireless utilizamos diferentes tipos de antenas las cuales se clasifican en omnidireccionales y Direccionales

4.2.1. Antenas Omnidireccional

Emiten en todas direcciones la señal con un amplio haz pero de corto alcance, una antena omnidireccional se asemejaría a una bombilla que emite luz en todas direcciones afectando esto a su alcance ya que es de menor distancia que las antenas direccionales.

Las antenas Omnidireccionales transmiten la información a 360 grados por lo que es posible comunicarse con esta red sin importar el punto en el que se encuentre ubicado alrededor de la antena.

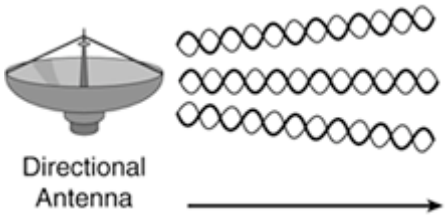


4.2.2. Antena direccional

La antena es un elemento importante de una Wireless MAN. A diferencia de otros tipos de redes inalámbricas, la mayoría de las antenas de Wireless MAN utilizan antenas direccionales, principalmente debido a que operan en

zonas más amplias. La imagen ilustra la propagación de las ondas de radio de una antena direccional. Esto contrasta con una antena omnidireccional, que transmite ondas de radio en todas las direcciones.

Imagen. Antena direccional maximiza la intensidad de las ondas de radio en una dirección



4.3. ESTÁNDARES WIFI

Al hablar de WiFi una gran mayoría sabe que estamos hablando de conexión inalámbrica pero no sabemos los diferentes tipos de estándares que existen por lo que a continuación describimos algunos de los más importantes.

802.11a

Fue creado en 1999, este estándar funciona con la frecuencia de los 5 GHz buscando tener menor interferencia con dispositivos como teléfonos inalámbricos que usan la frecuencia de 2.4 GHz cuya máxima velocidad de conexión es de 54 megabits por segundo. Siendo su alcance muy limitado ya que si encuentran objetos a su paso estos bloquean fácilmente la frecuencia de los 5 GHz.

802.11b

Se creó en 1999 usando la frecuencia de 2,4 GHz, y tiene una velocidad máxima de transmisión de 11 Mbit. Debido al espacio ocupado por la codificación del protocolo CSMA/CA (Carrier Sense Multiple Acces/Collision Avoidance), la velocidad máxima de transmisión en la práctica con este estándar es aproximadamente 5.9 Mbit/s.

802.11g

Creado en el 2003, Utiliza la banda de 2.4 Ghz opera a una velocidad máxima de 54 Mbit/s, o de 24.7 Mbit/s de velocidad real de transferencia, muy semejante al del estándar 802.11a. Este estándar es compatible con el b y utiliza la frecuencia 2.4GHz.

Este estándar lo adoptaron significativamente y sigue siendo uno de los más utilizados hasta la fecha ya que su velocidad es adecuada para una gran mayoría de aplicaciones.

802.11n

El este estándar lanzado en el 2009 trabaja en las dos frecuencias 2.4 y 5 GHz con velocidades máximas de 600 Mbit/segundo. El alcance de operación de este estándar es mucho mayor gracias a la tecnología MIMO (Multiple Input – Multiple Output), tecnología que permite utilizar varios canales de entrada como de salida para la transmisión de datos gracias a la incorporación de varias antenas.

MIMO usa múltiples antenas transmisoras y receptoras para mejorar el desempeño del sistema. Esta tecnología usa múltiples antenas para manejar más información (cuidando la coherencia) que cuando se usa una sola antena.

Esta tecnología depende de las señales multiruta. Estas señales multiruta son las reflejadas que llegan al receptor un tiempo después de que la señal de línea de vista (line of sight, LOS) ha sido recibida. En una red sin MIMO, como las redes 802.11a/b/g, las señales multiruta las reciben como interferencia que disminuyen la posibilidad del receptor de recobrar el mensaje

en la señal. MIMO utiliza las señales multirutas para poder capturar la mayor cantidad de mensajes de la señal.

4.4. SEGURIDAD

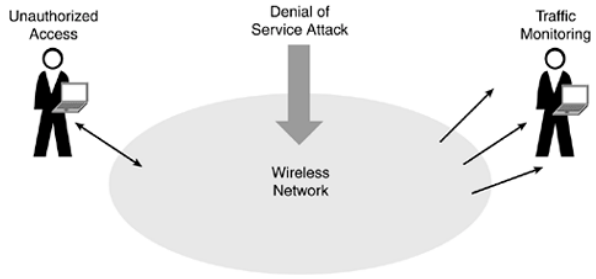
La seguridad en el campo inalámbrico es un aspecto muy importante ya que en una red inalámbrica una tercera persona podría entrar a nuestra red sin siquiera estar en las dependencias de nuestra empresa ya que bastaría con estar en un lugar en el cual llegue la señal para realizar un ataque el cual no dejaría siquiera huellas en el caso de ser uno pasivo.

El cifrado básico y tecnologías de autenticación y las normas

La seguridad es de vital importancia para las redes inalámbricas, principalmente porque las señales de comunicación están a disposición a medida que se propagan por el aire. Empresas y personas que utilizan las redes inalámbricas deben ser conscientes de los problemas potenciales y las contramedidas aplicables. Este capítulo trata de las amenazas de seguridad y las maneras de reforzar la seguridad de una red inalámbrica mediante el uso de encriptación y autenticación.

Hay varias formas de amenazas a la seguridad de las redes inalámbricas. Por ejemplo, los hackers pueden robar información de una empresa, obtener acceso no autorizado a las aplicaciones, e incluso interrumpir el funcionamiento de la red.

Amenazas a la seguridad de red inalámbrica incluyen el monitoreo pasivo, acceso no autorizado y denegación de servicio (DoS)



Monitoreo de Tráfico

Un hacker experimentado, o incluso un fisgón casual, puede controlar fácilmente los paquetes de datos WiFi sin protección con herramientas como AirMagnet y AiroPeek, que revelen completamente el contenido de los paquetes de datos inalámbricos. Por ejemplo, los fisgones pueden monitorear todas las transacciones que ocurren en la parte inalámbrica de la red de varios cientos de metros de distancia del edificio que tiene la red LAN inalámbrica. Por supuesto, la cuestión es que cualquier persona puede identificar los nombres de usuario, contraseñas, números de tarjetas de crédito, y así sucesivamente.

La solución a este problema es, como mínimo, usar cifrado entre el dispositivo cliente inalámbrico y la estación base. El cifrado altera los bits de datos utilizando una clave secreta. Dado que la clave es secreta, un hacker no es capaz de descifrar los datos. Como resultado, el uso de mecanismos de cifrado eficaz mantiene la privacidad de los datos.

Acceso no autorizado

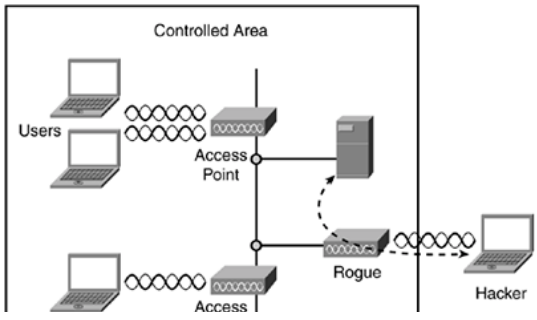
Similar a la supervisión de una aplicación inalámbrica, alguien fácilmente puede acceder a una red inalámbrica de la empresa desde fuera de las instalaciones si las precauciones no se toman. Alguien puede, por ejemplo, sentarse en un coche aparcado y se asocian con una de las estaciones bases inalámbricas ubicadas en un edificio. Sin la seguridad adecuada, esta persona puede acceder a servidores y aplicaciones que residen en la red corporativa. Esto es similar a que un extraño dentro de su hogar u oficina.

Desafortunadamente, muchas compañías despliegan sus redes inalámbricas utilizando el valor por defecto, sin garantía configuraciones de estación base, por lo que es posible para cualquier persona interactuar con los servidores de su aplicación. De hecho, usted puede ir conduciendo y descubre que el 30 por ciento de los puntos de acceso LAN inalámbrica en una ciudad media no desplegar ningún tipo de seguridad. Esto permite que cualquiera

pueda acceder a unidades de disco duro y utilizar los recursos, tales como las conexiones a Internet.

Los sistemas operativos actuales hacen que sea fácil de interactuar con las redes inalámbricas, especialmente en redes LAN inalámbricas públicas. Cuando se asocia una computadora portátil con la red LAN inalámbrica, el usuario puede desplazarse a cualquier otro ordenador portátil asociada a la misma LAN inalámbrica. Sin la protección de firewall personal, una persona puede navegar a través de su disco duro. Se trata de un riesgo de seguridad enorme.

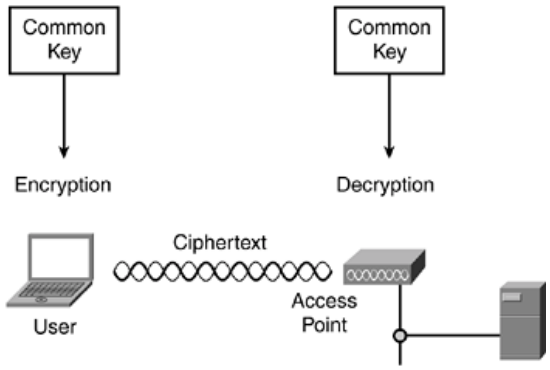
Incluso si se implementan todos los controles de seguridad en los puntos de acceso, la posible conexión de un Access Point pirata es una amenaza significativa. Un Access Point no autorizado es un Access Point no autorizado en la red. Un empleado puede comprar uno e instalarlo en su oficina sin conocer las implicaciones de seguridad. Un hacker podría plantar un acces point no autorizado dentro de un local a propósito de la conexión de un Access Point sin protección a la red corporativa.



Encriptación

La encriptación altera los bits de cada paquete de datos para ocultarla de los fisgones de decodificación de datos, como números de tarjetas de crédito. Antes de la encriptación de los datos se denomina texto plano, lo cual es fácil de descifrar mediante el uso de herramientas de rastreo. El cifrado convierte el texto plano en texto cifrado, lo que alguien pueda descifrar sólo a través de la utilización de una clave secreta correcta.

Muchos métodos de encriptación, como el 802.11 Wired Equivalent Privacy (WEP), son simétricas Es decir, la misma clave que hace que el cifrado es también la que realiza el descifrado. La figura ilustra este proceso.



Por ejemplo, la NIC radio utiliza xyz clave para cifrar un paquete de datos, y un Access Point utiliza xyz clave para realizar el descifrado. Esto requiere que tanto el envío y recepción de emisoras a confiar unos en otros, como es el caso de una aplicación de redes inalámbricas privadas, como una LAN inalámbrica empresarial.

Para el cifrado simétrico para ser eficaz, la función debe minimizar la reutilización de claves de cifrado, cambiando con frecuencia, posiblemente cada transmisión de la trama. Esto reduce el tiempo disponible para un hacker para irrumpir en la red y hace que sea difícil, Si no imposible. Para no comprometer la seguridad de la red. Como resultado, los mecanismos de cifrado simétrico deben tener métodos eficaces de distribución de claves.

WEP

WEP es el cifrado 802,11 opcional y estándar de autenticación implementado en la capa MAC que la mayoría de los NIC de radio y el apoyo de puntos de acceso los vendedores. Al implementar una red inalámbrica, es necesario para comprender plenamente la capacidad de mejorar la seguridad WEP.

WEP Operación

Si un usuario activa WEP, la tarjeta de red cifra la carga (el cuerpo marco y comprobación de redundancia cíclica [CRC]) de cada trama 802.11 antes de la transmisión con un cifrado de flujo RC4 proporcionado por RSA Security. La estación de recepción, como un Access Point u otra tarjeta de red de radio, realizan el descifrado de la imagen llegada. Como resultado, 802.11 WEP cifra los datos entre las estaciones de 802,11. Una vez que entra en el marco de la parte cableada de la red, por ejemplo, entre los puntos de acceso, WEP ya no se aplica.

Como parte del proceso de cifrado, WEP prepara un programa clave (semilla) mediante la vinculación de la clave secreta compartida suministrados por el usuario de la estación emisora con un vector de inicialización generado de forma aleatoria de 24 bits (IV). El IV se alarga la vida de la clave secreta ya que la estación puede cambiar el IV en cada transmisión de la trama. WEP entradas de la semilla resultante en un generador de números pseudo-aleatorios que produce un flujo de clave igual a la longitud de carga útil del marco además de un valor de integridad de 32 bits de verificación (ICV).

El ICV es una suma de comprobación de que la estación receptora

vuelve a calcular y se compara con el enviado de la estación emisora. Determina si los datos transmitidos se sometieron a ningún tipo de manipulación durante el transporte. Si la estación receptora calcula el ICV que no coincide con la que se encuentra en el marco, la estación receptora puede rechazar el marco o la bandera del usuario.

WEP especifica una clave secreta compartida para cifrar y descifrar los datos. Con WEP, la estación receptora debe utilizar la misma clave de descifrado que cada tarjeta de red de radio y Access Point, por lo tanto, se debe configurar manualmente con la misma clave.

Antes de la transmisión que se lleva a cabo, WEP combina el flujo de claves con la carga ICV a través de un proceso a nivel de bits XOR, que produce un texto cifrado (datos cifrados). WEP incluye el IV en el claro (sin cifrar) en los primeros bytes del cuerpo del marco. La estación receptora utiliza este IV junto con la clave secreta compartida suministrados por el usuario de la estación receptora para desencriptar la parte de carga del cuerpo marco.

En la mayoría de los casos, la estación emisora se utiliza un IV diferente para cada fotograma (esto no es requerido por el estándar 802.11). Cuando la transmisión de mensajes tiene un principio común, como la dirección del remitente de un correo electrónico, al inicio de cada carga útil encriptada será

equivalente cuando se utiliza la misma clave. Una vez cifrados los datos, los inicios de estos marcos sería el mismo, ofreciendo un modelo que puede ayudar a los piratas informáticos descifrar el algoritmo de cifrado. Dado que el IV es diferente para la mayoría de los marcos, WEP protege contra este tipo de ataque. El cambio frecuente de IVs también mejora la capacidad de WEP para proteger en contra de alguien comprometer los datos.

WEP Problemas

WEP es vulnerable debido a vectores de inicialización relativamente corta y las claves que permanecen estáticos. Los problemas con WEP en realidad no tienen mucho que ver con el algoritmo de cifrado RC4. Con sólo 24 bits, WEP finalmente utiliza el mismo IV para los paquetes de datos. Para una red grande, ocupado, esta repetición de IVs puede ocurrir dentro de una hora o así.

Esto se traduce en la transmisión de tramas con secuencias de claves que son muy similares. Si un hacker se acumula suficientes cuadros basados en la misma IV, el individuo puede determinar los valores compartidos entre ellos-es decir, el flujo de claves o la clave secreta compartida. Esto, por supuesto, lleva al hacker descifrar alguna de las tramas 802.11.

La naturaleza estática de las claves del secreto compartido hace hincapié en este problema. 802.11 no proporciona funciones que permiten el intercambio de claves entre las estaciones. Como resultado, los administradores de sistemas y usuarios en general, utilizar las mismas claves durante semanas, meses e incluso años. Esto le da a los culpables travieso mucho tiempo para controlar y cortar en redes con WEP.

Cuándo usar WEP

A pesar de sus defectos, debe activar la WEP como un nivel mínimo de seguridad. Muchas personas han descubierto las redes inalámbricas que utilizan los analizadores de protocolo, como AiroPeek y AirMagnet. La mayoría de estas personas son capaces de detectar las redes inalámbricas que WEP no está en uso y luego usar una computadora portátil para tener acceso a recursos ubicados en la red de asociados.

Temporal Key Integrity Protocol

El estándar 802.11i incluye mejoras en la seguridad LAN inalámbrica.

Una de las mejoras es el Protocolo de Integridad de Clave Temporal (TKIP), inicialmente conocido como WEP2. TKIP es una solución provisional que fija problema reutilización clave WEP. De hecho, muchos productos de LAN inalámbrica ya tienen TKIP como una opción.

El proceso de TKIP comienza con una clave temporal de 128 bits compartida entre clientes y puntos de acceso. TKIP combina la clave temporal con la dirección MAC del cliente y luego agrega una cantidad relativamente grande de 16-byte IV para generar la clave que cifra los datos. Este procedimiento asegura que cada estación utilice secuencias de claves distintas para cifrar los datos.

TKIP utiliza RC4 para realizar el cifrado, que es lo mismo que WEP. Una gran diferencia de WEP, sin embargo, es que TKIP cambia las claves temporales cada 10.000 paquetes. Esto proporciona un método de distribución dinámico que mejora significativamente la seguridad de la red.

Una ventaja de usar TKIP es que las empresas existentes con WEP basada en puntos de acceso y tarjetas de red de radio se pueden actualizar a través de parches de firmware TKIP relativamente simple. Además, WEP, sólo el equipo todavía va a funcionar con TKIP dispositivos habilitados para el uso de WEP

WPA

El Wi-Fi Access Protocol (WPA) estándar proporcionado por la Alianza Wi-Fi ofrece una actualización de WEP que ofrece cifrado de clave dinámico y autenticación mutua. La mayoría de los proveedores inalámbricos son ahora compatibles con WPA. Clientes WPA utilizan claves de cifrado diferentes que cambian periódicamente. Esto hace que sea más difícil de descifrar la encriptación.

WPA 1.0 es en realidad una instantánea de la versión actual de 802.11i, que incluye los mecanismos TKIP y 802.1x. La combinación de estos dos mecanismos proporciona un cifrado de clave dinámico y autenticación mutua, algo necesario en las redes LAN inalámbricas. WPA 2.0 ofrece compatibilidad total con el estándar 802.11i.

WPA 2

WPA2 (Wi-Fi Protected Access 2) proporciona a los administradores de red con un alto nivel de seguridad en el que sólo los usuarios autorizados

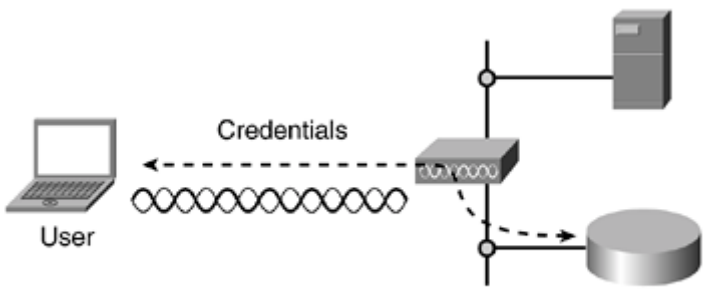
pueden acceder a la red. Basado en el estándar IEEE 802.11i ratificado, WPA2 proporciona una seguridad de nivel gubernamental al implementar el Instituto Nacional de Estándares y Tecnología (NIST) FIPS 140-2 compatible con algoritmo de encriptación AES. WPA2 se puede activar en dos versiones - WPA2 - Personal y WPA2 - Enterprise. WPA2 - Personal protege el acceso no autorizado de la red mediante la utilización de una contraseña de configuración. WPA2 - Empresa verifica los usuarios de la red a través de un servidor. WPA2 es compatible con WPA.

AUTENTICACIÓN

El uso de la autenticación mutua es importante en una red inalámbrica. Esto evita muchos problemas de seguridad, tales como el hombre en el medio de ataque. Con la autenticación mutua, el cliente inalámbrico y la red inalámbrica deben acreditar su identidad el uno al otro. Este proceso utiliza un servidor de autenticación, tales como Remote Authentication Dial-In User Service (RADIUS), para realizar la autenticación.

La figura ilustra el proceso de autenticación

La autenticación verifica la identidad de los usuarios y de dispositivos del cliente a través de credenciales, como contraseñas y certificados digitales



Filtros MAC

Algunas estaciones de bases inalámbricas ofrecen un control de acceso MAC al medio de filtrado. En la aplicación de filtrado de direcciones MAC, el Access Point examina la dirección MAC de origen de cada trama entrante. El Access Point al negar marcos sin una dirección MAC que coincida con una lista específica programada por el administrador. Como resultado de ello, el filtrado MAC ofrece una forma primitiva de autenticación.

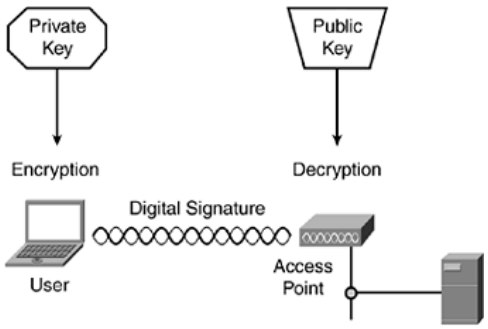
Filtrado de direcciones MAC, sin embargo, tiene algunas debilidades. Por ejemplo, el cifrado WEP no cifra el campo de la dirección MAC de la trama. Esto permite a un hacker para percibir fácilmente la transmisión de tramas y descubrir direcciones MAC válidas. Y, un hacker puede utilizar el software de libre disposición para cambiar la dirección MAC de NIC de radio para que coincida con una dirección MAC válida. Esto permite a los hackers hacerse pasar por un usuario real y engañar al Access Point cuando el usuario legítimo no se encuentra en la red.

Autenticación utilizando la criptografía de clave pública

Además de proteger la información de hackers, las emisoras pueden utilizar la criptografía de clave pública para autenticarse a otras estaciones o

Access Point. Esto puede ser necesario antes de un acces point o el controlador permite una estación en particular para interactuar con una parte protegida de la red. Del mismo modo, el cliente puede autenticar el Access Point de una manera similar.

Una estación se autentica mediante el cifrado de una cadena de texto dentro de un paquete con su clave privada. La estación receptora descifra el texto con la clave pública de la estación emisora. Si el texto descifrado coincide con un texto predeterminado, como el nombre de la estación, la estación receptora sabe que la estación emisora es válida. El cifrado de una cadena particular de texto, en este caso actúa como una firma digital. La figura ilustra el concepto de usar el cifrado de clave pública para la autenticación.



802.1x

El uso de IEEE 802.1x ofrece un marco eficaz para la autenticación de forma automática y el control de tráfico de usuarios a una red protegida, así

como de forma dinámica diferentes claves de cifrado. Lazos 802.1x un protocolo llamado Protocolo de Autenticación Extensible (EAP) a los dos los medios de comunicación de red cableada e inalámbrica y soporta múltiples métodos de autenticación, como tarjetas de identificación, Kerberos, las contraseñas de una sola vez, los certificados y autenticación de clave pública.

Operación 802.1x

Comunicación 802.1x inicial comienza con un solicitante no autenticados (dispositivo de cliente inalámbrico) de intentar conectar con un autenticador (estación base inalámbrica). La estación base responde al permitir que un puerto para pasar sólo los paquetes EAP entre el cliente y un servidor de autenticación se encuentra en la parte cableada de la estación base. La estación base se bloquea todo el tráfico, tales como HTTP, DHCP, y paquetes de POP3, hasta la estación base se puede verificar la identidad del cliente mediante un servidor de autenticación, como RADIUS. Una vez autenticado, la estación base se abre el puerto del cliente para otros tipos de tráfico basado en los derechos de acceso que realiza el servidor de autenticación.

4.5. HARDWARE PARA WMAN

Para realizar un enlace inalámbrico de largo alcance se requiere de Hardware apropiado el cual nos permitirá realizar la conexión de los diferentes puntos requeridos con la agencia principal de la empresa.

Este tipo de Hardware se puede encontrar en proveedores especializados en diferentes marcas y modelos los cuales diferenciándose por el protocolo IEEE bajo el cual están establecidos.

Solución Ubiquiti: En el caso de Ubiquiti, el modelo elegido es el PowerBridge M5 diseñado especialmente para exteriores. Dicho modelo muestra que es compatible con los estándares IEEE 802.11 a/n añadiendo la tecnología MIMO que en este tipo de antenas permite transportar de mejor manera los datos y mejora las prestación de dichos estándares a más de una función propietaria como lo es AirMax TDMA (Time Division Multiple Access), de Ubiquiti, que redefine los estándares de escalabilidad en enlaces punto a punto. Además, con la aplicación AirControl se pueden gestionar de forma centralizada hasta 100 de estos equipos. Esta nos permite alcanzar enlaces punto a punto de mayores a 20 Km usando su antena de doble polaridad de 25 dBi de ganancia en ambos equipos. El PowerBridge M5 tiene 1 interfaz radio de 5.8 GHz (5470MHz-5825MHz) lo que nos permitiría disponer de un enlace independiente en la red. Su máxima sensibilidad en esa banda es de -96 dBm, tiene una potencia máxima de transmisión 27 dBm, tiene un puerto Ethernet 10/100 WEP, WPA y WPA2, tiene un consumo energético max de 8 W, este

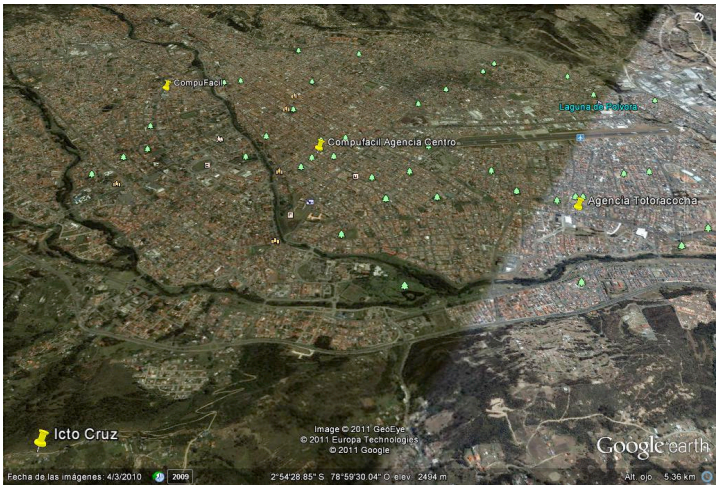
equipo nos puedes dar una ancho de banda en el exterior de 150 Mbp/s en enlaces de hasta 20 KM.

Para el desarrollo de este proyecto se deben seguir las siguientes etapas:

- Inspección del área donde se implementará la WMAN
- Diseño de plano, distancias y ubicación de antenas
- Implementación WMAN
- Configuración de la seguridad en el enlace WMAN

4.6. ANÁLISIS DEL ÁREA

La empresa CompuFácil está ubicada en las calles Remigio Crespo y Guayas, contando además con dos agencias una ubicada en el centro histórico de la cuidad y su segunda agencia en Totoracocha por lo que se decidió unir a estas a fin de poder compartir los recursos de la empresa y tener un mejor control sobre sus recursos. El siguiente Gráfico nos permite observar una panorámica de ubicación de las agencias las cuales se procederán a enlazar.



Realizando la inspección de las áreas en donde se colocaran los enlaces se puede constatar que estos tienen una línea de vista directa sin obstáculos que puedan deteriorar la calidad del enlace de datos, pudiéndose además verificar que se cuenta con el espacio físico necesario para poder realizar la instalación de las antenas en cada una de la agencias como podemos ver a continuación en las siguientes imágenes. La imagen nos permite apreciar el Sector de Icto Cruz desde la Matriz de la empresa CompuFácil.

En el sector llamado Icto Cruz se cuenta con una torre en la cual se ubicaran las antenas pertenecientes a la empresa. Esta torre pertenece a la Cooperativa de Ahorro y Crédito Alfonzo Jaramillo la cual se ha arrendado ya una parte de la infraestructura de la misma para poder acondicionar los equipos de CompuFácil.

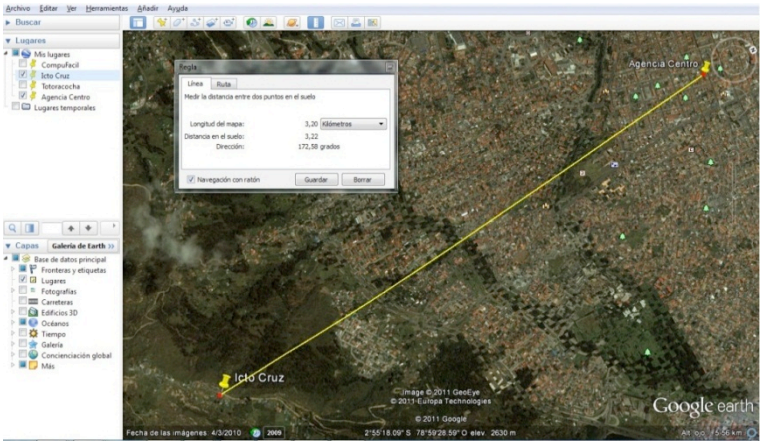
4.7. DISEÑO DE LA RED.

Para poder realizar el análisis y simulación de los enlaces se usó el software Radio Mobile y la calculadora de enlaces de Ubiquiti que se la puede encontrar en esta dirección http://www.ubnt.com/airlink/, se puede también realizar estos análisis con otros que tienen mayores prestaciones como SPLAT se ha elegido Radio Mobile y la calculadora por su sencillez, entorno gráfico y

aceptable fiabilidad que presentan estos dos sistemas. El sistema Radio Mobile usa un modelo de terreno irregular (ITM), como modelo de propagación en el rango de las frecuencias de 20MHz a 20GHz.

Para diseñar o emular los radio enlaces vamos a establecer valores como ganancia de antenas, sensibilidad de radios, potencia de transmisión, de acuerdo al tipo de equipo que se eligió para este propósito y así confirmar la adquisición de estos.

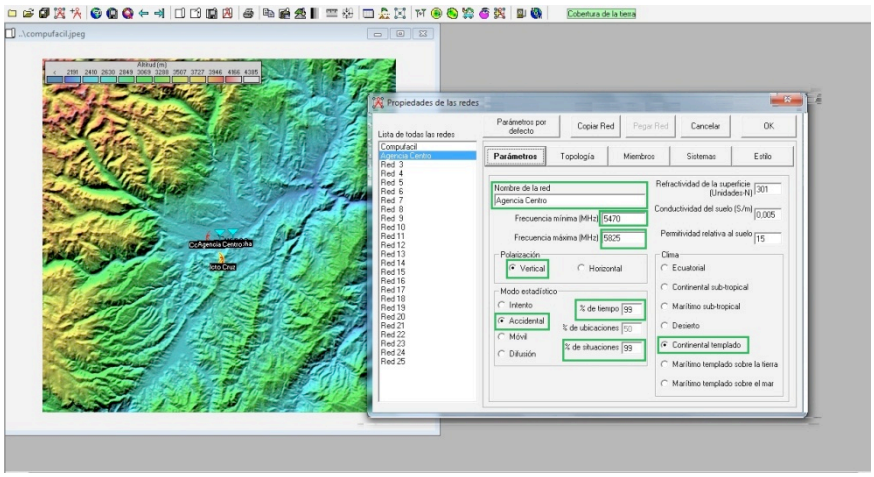
A continuación procederemos a indicar la configuración y la muestra de resultados obtenidos por Radio Mobile.



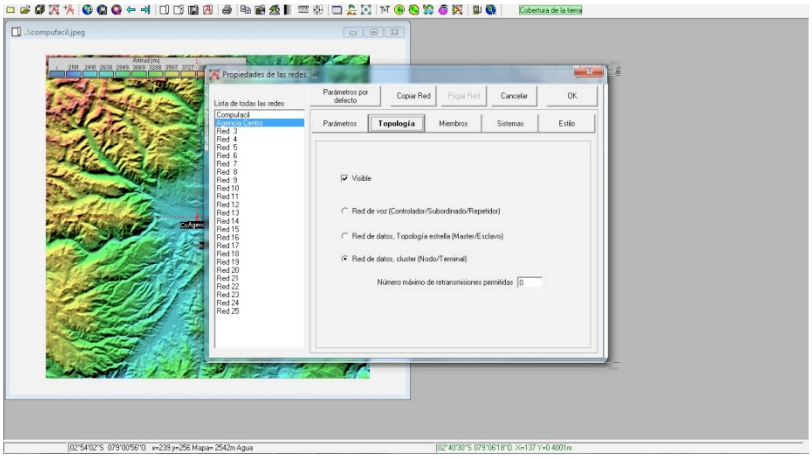
Para obtener las coordenadas que se usaran en Radio Mobile de cada una de las agencias usamos Google Earth, agregando marcadores en los distintos puntos de las agencias.

Con los datos del proceso anterior procedemos a crear las redes en Radio Mobile para este proceso tendremos que contar con:

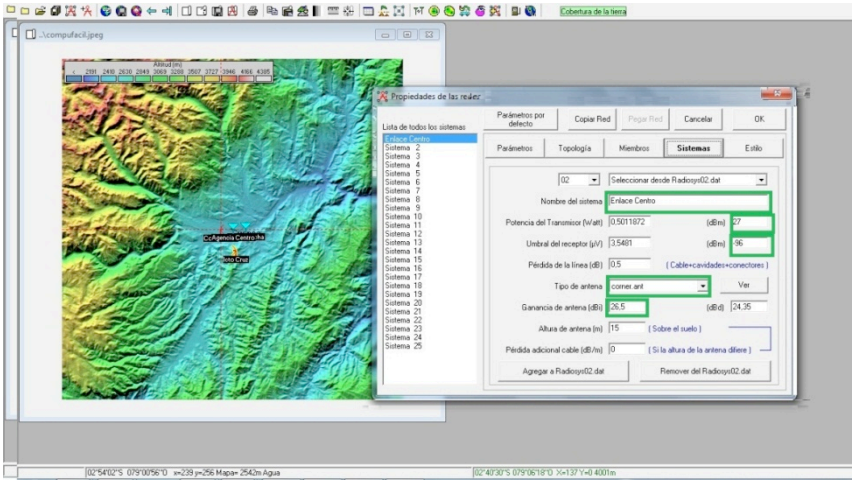
- Nombre para la Red
- Frecuencia mínima: 5470 MHz
- Frecuencia máxima: 5825 MHz
- Polarización: Vertical
- Modo Estadístico: Accidental
- Clima: Continental Templado



Una vez configurados estos parámetros de la red, se procede a configurar la Topología donde vamos a elegir el tipo de Red de Datos. La que configuraremos como estrella.

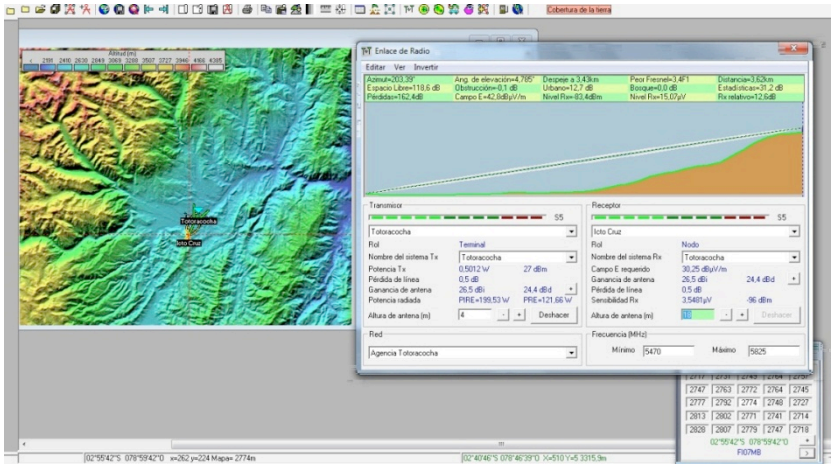


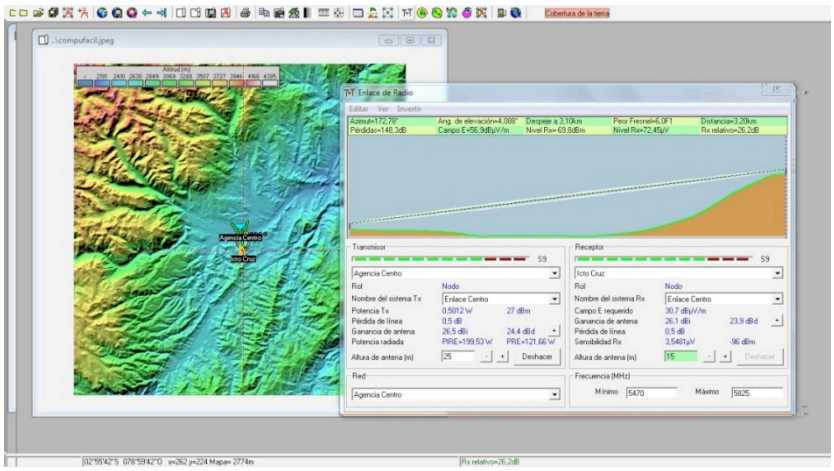
La siguiente parte es configurar la parte de Sistemas donde indicaremos las características de los dispositivos que tenemos previsto usar.

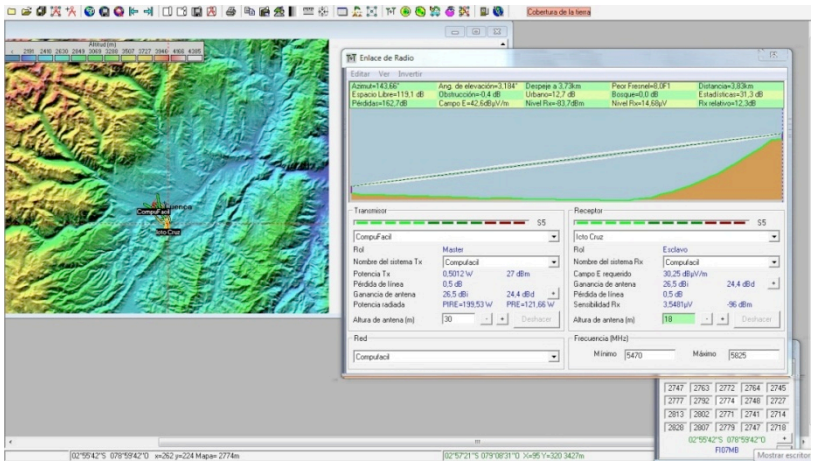


Y luego de indicar los miembros de la red, se procede a ejecutar el cálculo e interpretación  .

Esto nos muestra la pantalla donde nos indica la elevación del terreno así como los dos dispositivos, en el cual no indica que este enlace si es viable.

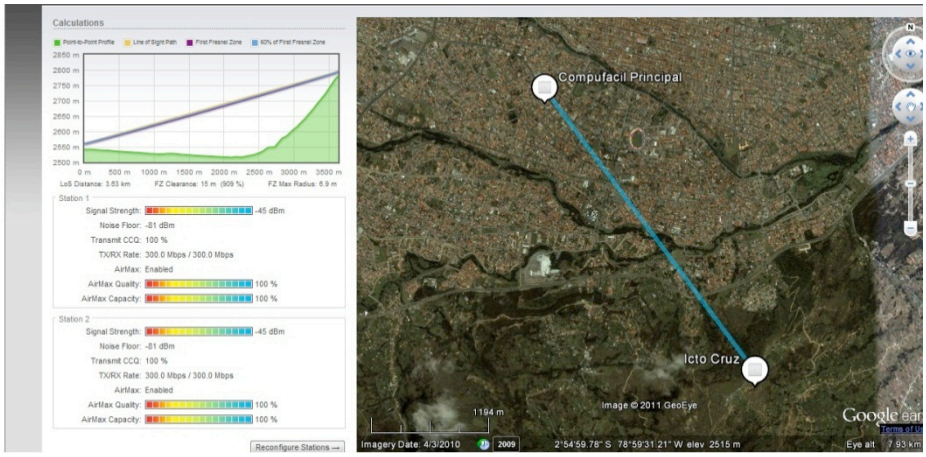






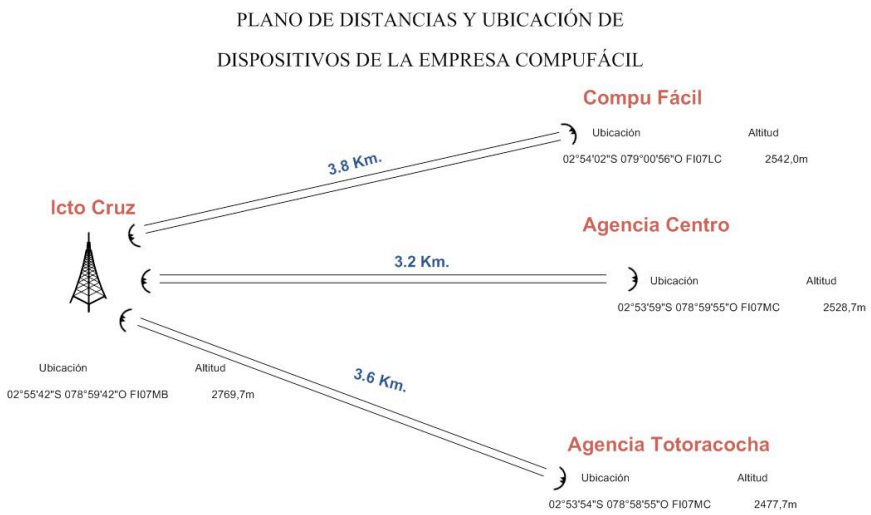
Para una mejor apreciación de este resultado, he exportado los resultados que nos da Radio Mobile a Google Earth graficándonos de mejor manera como lo muestra la imagen

El resultado del análisis con esta herramienta nos confirma lo ya realizado con la Calculadora de enlaces que provee Ubiquiti, confirmándonos que los enlaces se pueden realizar sin problema alguno, con los equipos seleccionados como se muestra en imagen.



4.8. DISEÑO DE PLANO Y DISTANCIAS DE ANTENAS

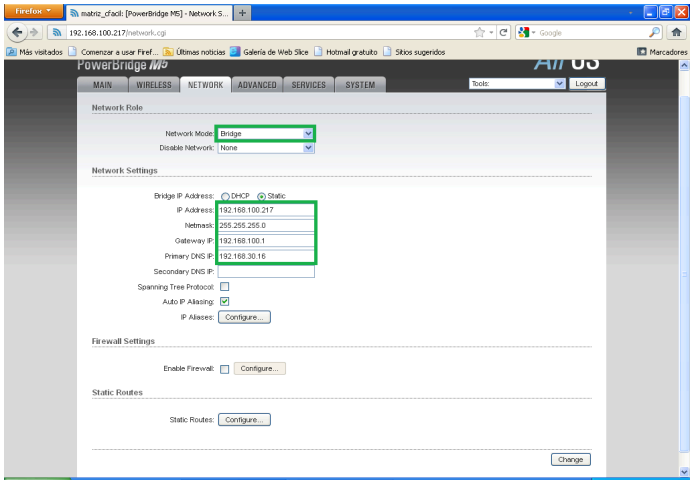
En el presente Gráfico se puede visualizar las distancias de los enlaces los cuales fueron calculados con Radio Mobile en este podemos ver que desde Icto Cruz a la matriz de CompuFácil existen 3.8 Km que es la distancia más extensa que se une con los enlaces de las antenas, además podemos ver su localización en coordenadas y altura de cada una de estas y de acuerdo a lo calculado podemos proceder a la instalación de nuestros dispositivos.



4.9. IMPLEMENTACIÓN.

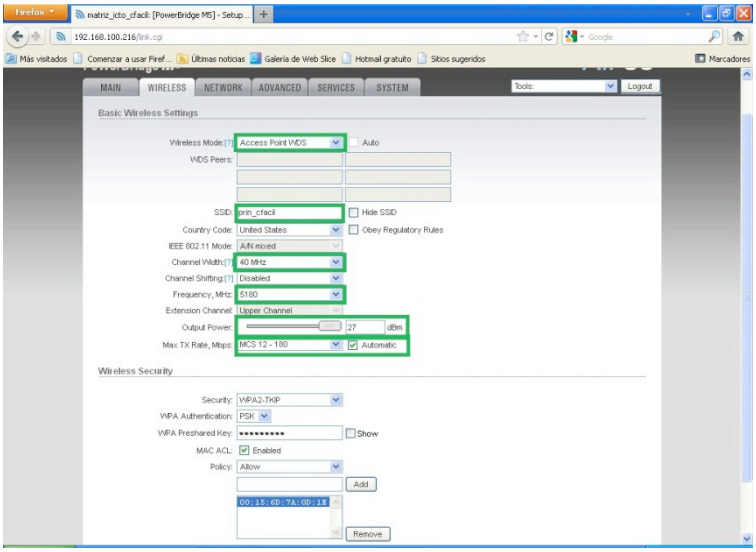
Para el proceso de instalación se los dispositivos PowerBridge M5 se inicia en el sector de Icto Cruz en el cual se tiene la torre para las antenas y dispone de una line de vista limpia con las tres agencias, proceso para el cual previamente se configuro y verifico que existía enlace entre las antenas designadas para la conexión de cada agencia.

Conectar la antena a nuestra pc mediante un cable cruzado y en la pestaña de NETWORK procedemos a colocar nuestras configuraciones de red, como dirección IP, mascara de red, puerta de enlace o Gateway y la dirección de nuestro servidor DNS. También se configura la opción de modo de red la cual tiene que ir como “Bridge” que nos permite emitir todos los paquetes tanto de administración y de datos de nuestra red desde una interfaz a otra sin enrutamiento alguno de forma transparente para el usuario.

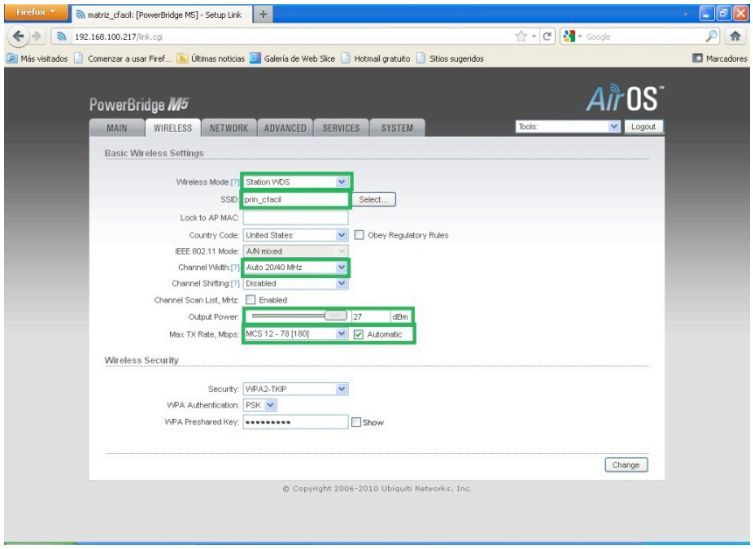


Se configura la opción de WIRELESS para el enlace entre las dos antenas, en esta pestaña se configuro el principal con las siguientes opciones:

- Mode wireless: Acces Point WDS
- SSID: prin_cfacil
- Channel Width: 40 MHz.
- Frequency, MHz: 5180
- Outut Power: 27 dbm
- Max TX Rate, Mbps: Mcs 12-80



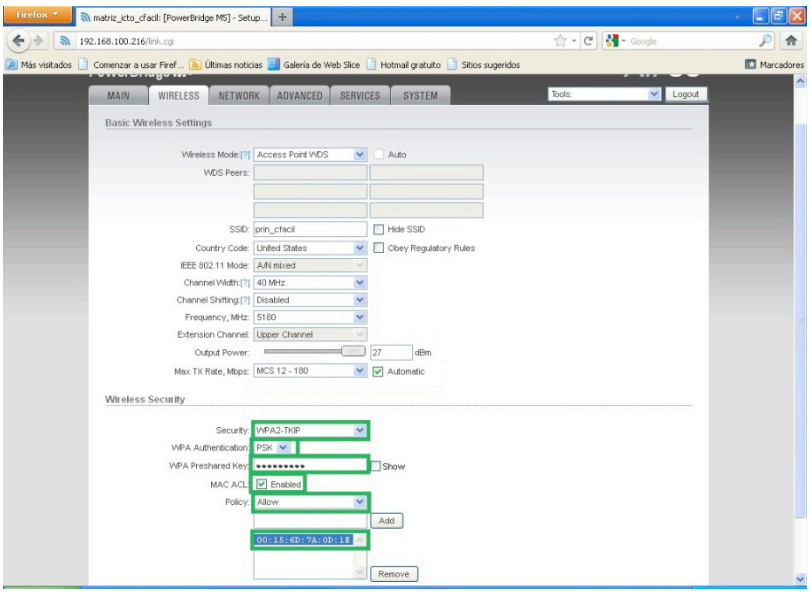
El cliente se configuro de como “Station WDS” la cual se une a la red “print_cfacil”, el canal a usar tiene que ser el mismo de la principal por lo que se configuro en 20/40 MHz, a más de la potencia de la antena y el Maz Tx Rate que continúan siendo los mismos que de la principal.



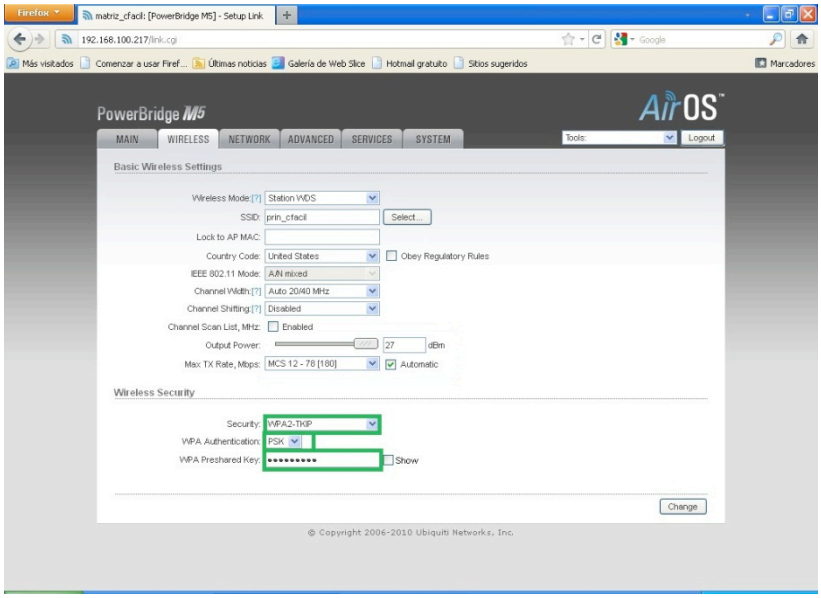
Una vez que se comprobó que el enlace está trabajando se procede a configurarla seguridad de los dispositivos siendo esta parte muy importante si queremos evitar que intrusos puedan acceder a nuestra red.

En esta pestaña configuramos:

- Seguridad: WPA2-TKP
- WPA Autentication: PSK
- WPA Preshared Key: asignamos la contraseña para el enlace
- MAC ACL: habilitada
- Policy: Allow
- Agregamos la dirección MAC del cliente con que se unirá asegurándonos así que esta antena responderá solo peticiones de este.



En la estación que se conectara configuramos tan solo tres opciones que tienen que ser de las mismas características que el AP al que nos conectamos.

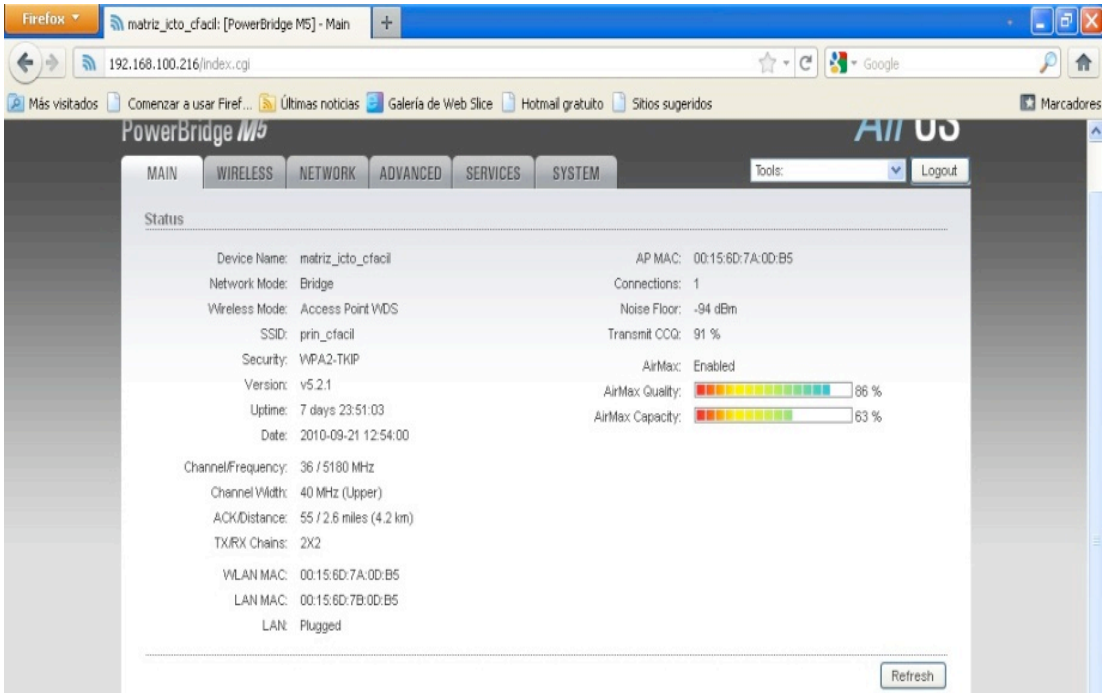


Este proceso de configuración se repite para cada uno de los enlaces a agregarse como son los de Totoracocha y de la Agencia del Centro de la ciudad.

El proceso de montaje de las antenas se realiza sin mayor inconveniente tanto en Icto Cruz y el resto de agencias podemos observar las imágenes de las mismas ya instaladas. En el proceso de alineación de las antenas se realizó

con ayuda de los indicadores de los dispositivos que nos grafican la calidad de señal con la que cuenta el enlace al momento de direccionarlos.


PowerBridge M5


Firefox
matriz_icto_cfacil: [PowerBridge M5] - Main
192.168.100.216/index.cgi
Google
Más visitados
Comenzar a usar Firef...
Últimas noticias
Galería de Web Slice
Hotmail gratuito
Sitios sugeridos
Marcadores
PowerBridge M5
MAIN
WIRELESS
NETWORK
ADVANCED
SERVICES
SYSTEM
Tools:
Logout
Status
Device Name: matriz_icto_cfacil
Network Mode: Bridge
Wireless Mode: Access Point WDS
SSID: prin_cfacil
Security: WPA2-TKIP
Version: v5.2.1
Uptime: 7 days 23:51:03
Date: 2010-09-21 12:54:00
Channel/Frequency: 36 / 5180 MHz
Channel Width: 40 MHz (Upper)
ACK/Distance: 55 / 2.6 miles (4.2 km)
TX/RX Chains: 2X2
WLAN MAC: 00:15:6D:7A:0D:B5
LAN MAC: 00:15:6D:7B:0D:B5
LAN: Plugged
AP MAC: 00:15:6D:7A:0D:B5
Connections: 1
Noise Floor: -94 dBm
Transmit CCQ: 91 %
AirMax: Enabled
AirMax Quality: 86 %
AirMax Capacity: 63 %
Refresh

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

1. Los datos obtenidos nos muestra que tenemos una mejora considerable en la velocidad de trasferencia de datos con respecto a la velocidad que se obtenía mediante enlaces por internet para el uso de sistemas como la Ajesoft y RCMS.

2. Que los enlaces de múltiples antenas MIMO son un aspecto importante en el estándar 802.11n ya que permite tener una calidad de señal muy buena.

3. Uno de los problemas a los que se enfrenta actualmente la tecnología WI-FI es la progresiva saturación del espectro radioeléctrico, debido a la gran masificación de usuarios afectando en gran medida a los enlaces de largo alcance que están expuestos a un riego de interferencia.

4. Al cuantificar las ventajas obtenidas por los enlaces inalámbricos podemos verificar que estos poseen n nivel confiable para su utilización.

5. Que existen alternativas para el análisis de enlaces inalámbricos pero se decidió utilizar Radio Mobile

6. Que Radio Mobile es una herramienta confiable para el análisis de factibilidad de los enlaces inalámbricos y de fácil configuración.

7. La inversión realizada en este proyecto está totalmente justificada en base a los beneficios que se obtienen ya que se puede administrar de mejor manera los recursos y la información de la empresa lo que permite la posibilidad de implementación de nuevos proyectos para la empresa

5.2. RECOMENDACIONES

1. Verificar el uso de contraseñas seguras ya que es un enlace que podría estar susceptible a ingresos de personas no autorizadas de no ser así.

2. Realizar mantenimiento y monitoreo de los equipos y enlaces constantemente para evitar deterioro en la calidad de transmisión de los paquetes de datos.

3. Adquirir equipos de repuesto para en caso de un fallo las reparaciones se realicen en el menor tiempo posible.

4. Recomendar la implementación de los sistemas a otras empresas.

BIBLIOGRAFÍA

http://es.wikipedia.org/wiki/wi-fi

http://histinf.blogs.upv.es/2010/12/02/historia-de-las-redes-inalambricas/#more-1150

http://bibdigital.epn.edu.ec/bitstream/15000/1364/1/CD-0750.pdf

http://www.ubnt.com/wiki/Eligiendo_productos_airmax

http://landashop.com/catalog/powerbridge-airmax-carrier-class-p-1739.html

http://ubnt.com/downloads/pbm5_datasheet.pdf

http://www.digitalstoreperu.com/temas/anexos/estandar%20wifi.htm

http://www.masadelante.com/faqs/wireless

http://www.linksysbycisco.com/LATAM/es/learningcenter/Est%C3%A1ndares_inal%C3%A1mbricos

http://mercadosunidos.wordpress.com/2009/04/05/estandares-inalambricos-y-la-nueva-generacion-80211n/

http://download.ehas.org/docs/manual_radiomobile.doc

http://bibdigital.epn.edu.ec/bitstream/15000/1364/1/CD-0750.pdf

ANEXOS

ENCUESTA PARA ANÁLISIS DE SITUACIÓN ACTUAL DE ACCESO A SISTEMAS EN LAS AGENCIAS DE COMPUFÁCIL

Estimado _____,

Por favor sírvase llenar la presente encuesta, que ayudará a mejorar la conectividad dentro de la empresa. Califique las siguientes preguntas de **1 a 5**, siendo 1 la más baja calificación y 5 la más alta.

a) Frecuencia de Acceso a los sistemas empresariales

1 2 3 4 5

b) Cómo calificaría la velocidad de conexión de las aplicaciones?

1 2 3 4 5

c) Cómo calificaría la asistencia de soporte en la resolución de problemas?

1 2 3 4 5

d) La atención al cliente se ve afectada por la velocidad de respuesta de los sistemas

1 2 3 4 5

e) Con qué frecuencia su equipo se infectaba de virus?

1 2 3 4 5

Gracias.