ESCUELA POLITÉCNICA DEL EJÉRCITO

SEDE LATACUNGA

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE ENLACES INALÁMBRICOS Y SUS SEGURIDADES EN EL ILUSTRE MUNICIPIO DE LATACUNGA"

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS E INFORMÁTICA

MONTENEGRO CARRERA ROBERTO SANTIAGO

Latacunga, diciembre 2009

DECLARACION

Yo, Roberto Santiago Montenegro Carrera, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido presentada para ningún grado o calificación profesional; y, que he consultado e investigado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual a la Escuela Politécnica del Ejército, según lo establecido por la ley de propiedad intelectual, por su Reglamento y por la normativa institucional vigente.

ROBERTO MONTENEGRO CARRERA
C.I. 1706878038

CERTIFICACION

Se certifica que el presente trabajo fue desarrollado por ROBERTO SANTIAGO MONTENEGRO CARRERA, bajo mi supervisión.

_____

Ing. Javier Montaluisa

DIRECTOR DEL PROYECTO

_____

Ing. Santiago Jácome

CODIRECTOR DEL PROYECTO

Agradecimientos

Agradezco de todo corazón a mi Dios por iluminar mi mente, alma y espíritu para concluir el presente proyecto.

A mí compañera de toda mi vida "mi amada esposa", y a mi querido hijo, quienes junto a mi han sufrido noches y días de perseverancia hasta conseguir la tan anhelada meta profesional.

A mis profesores y director de carrera quienes con sus conocimientos han aportado enormemente y de manera certera con sus conocimientos tan explícitos.

A mi director y codirector de tesis quienes con sus instrucciones y guías me han ayudado a discernir, investigar y encontrar conclusiones claras, para tener resultados apropiados, genuinos e innovadores que permitirán al municipio enlazar e integrar a todos sus direcciones y departamentos con tecnología inalámbrica de punta de acuerdo con los avances tecnológicos hasta hoy conocidos.

Dedicatoria

Este proyecto va dedicado de manera muy especial a mi familia, quienes en todo momento han impulsado y han incentivado a continuar perseverando en este desafió profesional y me han motivado para que continué preparándome en la ESPE.

A mis maestros y amigos de la ESPE, la Universidad más prestigiosa del Ecuador, quienes en verdad saben y han demostrado sus conocimientos.

TABLA DE CONTENIDOS

CONTENIDOS GRÁFICOS

RESUMEN

La Ilustre Municipalidad de Latacunga es una institución que regula el buen funcionamiento de la ciudad y sus habitantes consiguiendo el buen vivir de todos los ciudadanos de esta región, aquí se elaboran ordenanzas municipales, que rigen para el control, a través de líneas de fábrica, aprobación de planos, patentes municipales, permisos de funcionamiento, alcantarillado, agua potable, etc, sus dependencias se encuentran laborando como si fueran instalaciones independientes del municipio, los procesos y la información procesada son externas a su edificio central, por lo que los usuarios sienten malestar al ser atendidos de manera deficiente y tiene que trasladarse a grandes distancias para utilizar los servicios de las instalaciones municipales.

El presente proyecto pretende integrar las instalaciones dependientes del municipio, a través de una red inalámbrica de largo alcance con tecnología Wi-Fi, lo que solucionará la integración de estas dependencias ya que debido a las grandes distancias, han venido trabajando en forma separada de edificio principal, brindando una solución informática en cuanto a comunicaciones, manejo de información, base de datos e internet, ya que aplicando esta tecnología en este proyecto lograra que todas las instalaciones a pesar de sus distancias trabajen de manera coordinada on-line en forma eficaz, eficiente y segura con todas las demás instalaciones del I. Municipio de Latacunga, entrelazando información que requieran unas con otras lo que permitirá que se envié y reciba información de manera rápida dando solución tanto a la municipalidad que va a servir mejor a sus usuarios como a los ciudadanos van a ser mejor atendidos.

PRESENTACION

Al momento la Ilustre Municipalidad de Latacunga y todas sus dependencias se encuentran laborando como si fuesen instalaciones totalmente separadas o independientes, por esta razón los procesos y la información ejecutada trabaja aisladamente de los sistemas que maneja el Municipio en su edificio central.

Por lo que es necesario integrar a través de una red inalámbrica de largo alcance a las siguientes instalaciones:

a) Municipio de Latacunga, Oficinas Administrativas de la Alcaldía, Palacio Municipal

b) Santo Domingo CAPTUR (Cámara Provincial de Turismo)

c) Casa de los Marqueses (Casa de la Cultura)

d) Calvario (Antenas Principales)

e) Patronato Municipal de Amparo Social (Quirófanos y Salas de Recuperación e Hidratación)

f) Centro de cobros Sur (junto a los SSHH Barrio Sur) Calle

g) OPAP (Bodegas del Municipio, Obras Publicas y Agua Potable)

h) Terminal Terrestre

i) Plaza San Felipe

j) Mercado Mayorista

k) Mercado Cerrado

l) Instituto Geográfico Militar (SAN AGUSTIN)

m) Centro de Cobros Puente Alaquez

n) Centro de Cobros Lasso - Tanicuchi

o) Loma de Alcoceres (Backup de información municipal)

p) Cerro de Putzalagua (Enlace para las bodegas del Municipio OPP) 20Km

Muchas ocasiones es necesario los servicios y/o documentación de ciertas dependencias, por lo que es necesario trasladarse de un lugar a otro, para proceder a realizar el requerimiento, la mayoría de ocasiones se cumple, pero se ha perdido un valioso tiempo en el traslado, consulta y en el proceso del cumplimiento del requerimiento, en otras ocasiones la dependencia se encuentra cerrada, por lo que no se logra realizar ninguna acción y se perdió el tiempo sin lograr cumplir con el objetivo que se tenía previsto para realizar en estas dependencias.

Estos departamentos o dependencias se encuentran trabajando en forma separadas, aisladas y en forma unilateral, por lo que los requerimientos de información de una a otra dependencia son escasos y para conseguir dicha información es necesario trasladarse a la dependencia para satisfacer la necesidad, por lo que la implementación del tema propuesto, permitirá trabajar en forma conjunta e integrar tanto a las dependencias Municipales como también los Sistemas que se manejan, lo que permitan la comunicación de todas las dependencias a través de estos medios como si se tratará de una sola instalación, lo que finalmente evitará la perdida de tiempo, trabajo multitarea y en tiempo real, es decir se podrá consultar si alguna dependencia tiene el requerimiento de otra o no existe disponible el requerimiento y en el mismo momento se realizará la acción requerida.

Estos inconvenientes a ocasionado un tremendo malestar no solo al interior del Municipio, sino también a las personas que vienen a cancelar sus haberes por los varios rubros, por lo que la institución deja de recaudar por lo incomodo que le

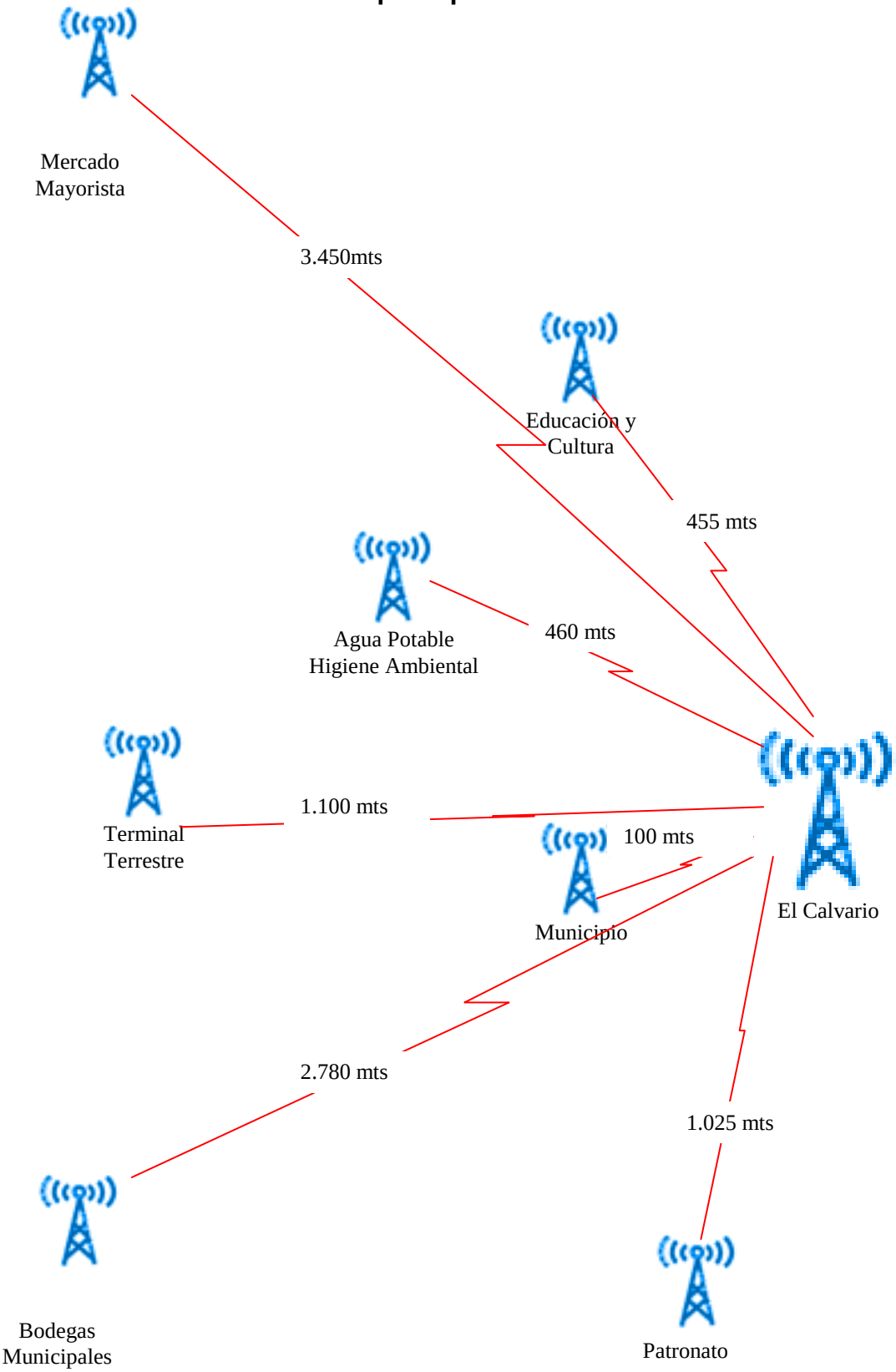
resulta al usuario desplazarse hasta el Edificio Central del Municipio a cancelar sus impuestos lo que no ocurriría con la implementación de la nueva tecnología que permitirá tener puntos de cobro en las diferentes instalaciones donde existe una gran afluencia de ciudadanos como son el Mercado Mayorista, Terminal Terrestre, entre otros.

Para solucionar los problemas anteriormente descritos y para la implementación del mismo se utilizará la tecnología Wi-Fi. (Wireless Fidelity) y Wi-Max de ser necesario, que son las redes inalámbricas de largo alcance de última tecnología. La investigación de la tecnología Wi-Fi, a permitido considerar, que es un sistema de bajo costo, capaz de ofrecer conectividad a 128 Kbs sobre distancias de un radio 30 Kms, sin satélites, ni estaciones de repetición, la limitación es la Línea de Vista. Este sistema depende de la actividad solar, y aprovecha la capacidad que tienen las ondas electromagnéticas de rebotar en la ionosfera para salvar obstáculos y mantener activos enlaces de voz y datos a largas distancias.

Se utilizará en el diseño, un modelo de red con Ruteo simple, esto permitirá que las funciones sean distribuidas entre varios puntos del sistema. Para la seguridad de la Red Inalámbrica la información será vigilada, purificada, ruteada y permitida a través de Claves Wep y Wpa, y las seguridades propias de los proveedores de equipos de conectividad, impidiendo el ingreso a quienes no están autorizados.

Con esta nueva tecnología propuesta en el presente proyecto, se pretende incrementar puntos de cobro en las diferentes instalaciones donde existe una gran concentración de usuarios, para facilitar que el ciudadano pueda realizar sus pagos en sitios cercanos como son Mercado Mayorista, Terminal Terrestre y otros sitios donde la I. Municipalidad lo requiera. El siguiente esquema ilustra como quedarán conectados todas las áreas municipales con lo enlaces inalámbricos.

DISTANCIAS TOMADAS DESDE EL CALVARIO
Hacia las principales Direcciones



CAPITULO I

1. FUNDAMENTACION DEL PROYECTO

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

Una red inalámbrica posibilita la unión de dos o más dispositivos sin la mediación de cables. Es una red en la cual los medios de comunicación entre sus componentes son ondas electromagnéticas, algunas de las técnicas utilizadas en las redes inalámbricas son: infrarrojos, microondas, láser y radio En los últimos años las redes de área local inalámbricas (WLAN, Wireless Local Área Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una “Red Híbrida” y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén, una oficina. o en la actualidad de un hogar modernizado, al momento contamos con 2 tipos de enlaces inalámbricos:

- De Larga Distancia.- Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Area Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps.
- De Corta Distancia.- Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se están muy retirados entre sí, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

En resumen llamamos enlace inalámbrico a aquella red que posibilita la unión de dos o más dispositivos sin la mediación de cables. Entre las principales ventajas podemos citar:

- Permiten la movilidad.
- Facilitan la reubicación de las estaciones de trabajo evitando la necesidad de tirar cableado.
- Rapidez en la instalación.
- Menores costes de mantenimiento.

1. DESCRIPCIÓN DEL PROYECTO

La Ilustre Municipalidad de Latacunga y todas sus dependencias se encuentran laborando independientemente como si fuesen instalaciones totalmente separadas o independientes, por esta razón los procesos y la información procesada es independiente de los sistemas que maneja el Municipio en su edificio central. Po lo que es necesario integrar a todas las dependencias a través de una red inalámbrica de largo alcance y corto alcance

2. OBJETIVOS DE LA INVESTIGACIÓN

1.2.1 OBJETIVO GENERAL

Presentar una propuesta tecnológica y económica de un sistema de Enlaces Inalámbricos de largo alcance en el I. Municipio de Latacunga, que integre a todas las dependencias y permita la transmisión de datos, video y Telefonía IP interna con sus correspondientes seguridades, que facilite la integración de todas sus dependencias.

1.2.2 OBJETIVOS ESPECÍFICOS

- Diseñar la propuesta técnica y económica de red inalámbrica.
- Usar la tecnología Inalámbricas estática y móvil para la conectividad de equipos en cualquier parte de la red.
- Utilizar un modelo de red con Ruteo simple, en el diseño, esto permite que las funciones del Ruteador sean distribuidas entre varios puntos del sistema.

- Proteger la información Ruteada desde el momento que es almacenada en el Ruteador, el sistema es protegido contra Hackers, o usuarios no autorizados, impidiendo el ingreso a quienes no están autorizados.
- Incrementar más puntos de recaudación en los sitios donde se instalen los puntos remotos de la red inalámbrica, lo que permitirá aumentar los ingresos a la Municipalidad y facilitara el pago de impuestos a la ciudadanía.
- Seleccionar y comparar equipos y tecnologías
- Plantear medidas de seguridad para la implementación de la Red Inalámbrica

3. METODOLOGIA

Se propondrá aplicar una metodología que combina las explicaciones teóricas con aplicaciones totalmente prácticas y basadas en experiencias reales con Intranets, Redes de área local y extendida, aplicaciones distribuidas, con redes corporativas, Internet inalámbrica y enlaces inalámbricos, además de las aplicaciones con equipos portátiles con detección de redes (kismet y netstumbler), detección de Hacker y seguridades de redes estáticas e inalámbricas. Además del estudio de factibilidad económica para la ejecución del proyecto y beneficios que se tendrá con la implementación del presente proyecto

4. JUSTIFICACIÓN DEL PROYECTO

1.4.1 JUSTIFICACIÓN TEÓRICA

Para solucionar los problemas anteriormente descritos y para la implementación de enlaces inalámbricos utilizare la tecnología Wi-Fi. (Wireless Fidelity) y WiMax.

Wi-Fi (o Wi-Fi, Wi-Fi, Wifi, wifi) es un conjunto de estándares para redes inalámbricas basados en todas las especificaciones IEEE 802.11x.

Wi-Fi se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad también se utilice para accesos inalámbricos e Internet. Además es un sistema de bajo costo capaz de ofrecer conectividad a 64Kbps sobre distancias de hasta 100 Kms (teóricamente), sin satélites, ni estaciones de repetición, y sin las limitaciones de perdida de señal de los cables.

Una desventaja de este sistema es la dependencia de la actividad solar, ya que aprovecha la capacidad que tienen las ondas electromagnéticas de rebotar en la ionosfera para salvar obstáculos y mantener activos enlaces de voz y datos a largas distancias.

1.4.2 JUSTIFICACIÓN PRÁCTICA

Wi-Fi es una tecnología novedosa y han empezado a utilizar, en hogares o empresas, por lo que el I. Municipio de Latacunga se encuentra inmerso en la actualización Tecnológica de sus instalaciones para esto es necesario comprender 4 conceptos claves:

- Seguridad: Se utilizarán estándares que garanticen la seguridad de las transmisiones a través de la tecnología inalámbrica.
- Provecho: mejorar la experiencia del usuario final, incidir en las ventajas o aplicaciones para éste, conseguir en definitiva que la tecnología se convierta en una comodidad para quien lo utiliza y no algo que lo aterra.
- Flexibilidad: dado el gran número de aplicaciones y tecnologías emergentes, el usuario final debe contar con la posibilidad de actualizar ambas, de modo que

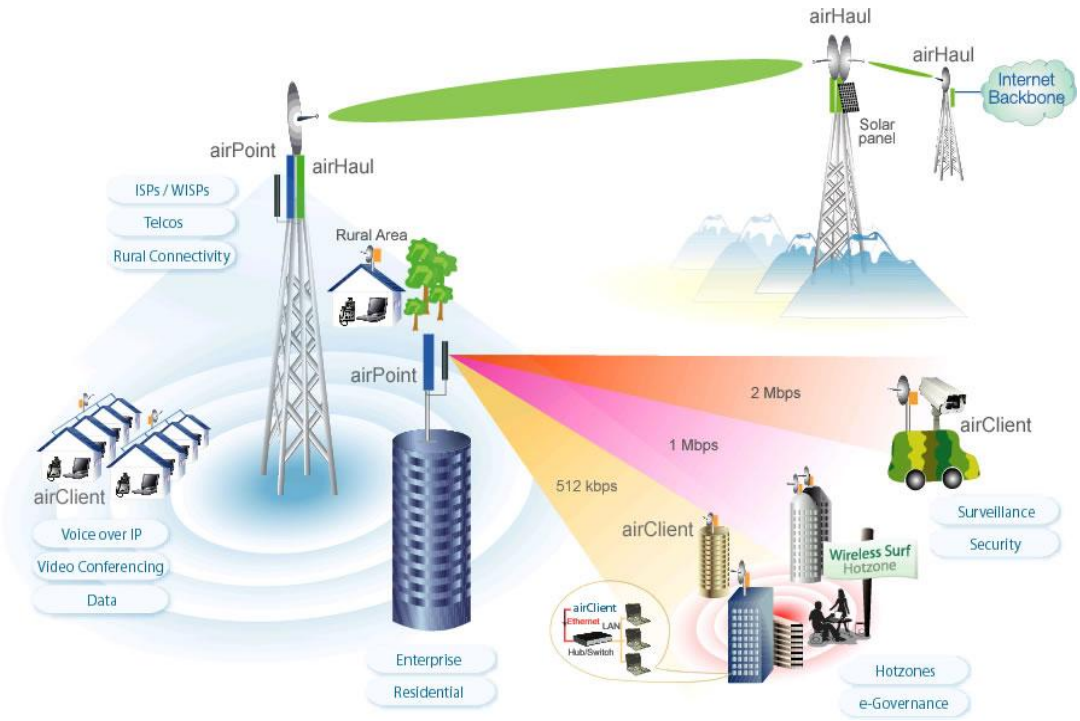
pueda planear a medio y largo plazo, más que limitarse a las necesidades inmediatas.

- Educación y Cultura: actualmente, la Wi-Fi ejerce el papel de principal difusor de las tecnologías inalámbricas y sus ventajas.

Con la Implementación del presente proyecto se integrarán todas las instalaciones Municipales anteriormente descritas, se crearán nuevos puestos de trabajo al poner puntos satélites de cobro en las diferentes dependencias donde el Municipio crea conveniente, así mismo se utiliza la telefonía IP interna, para la comunicación entre las diferentes Departamentos Municipales así como también la transmisión y recepción de información y datos.

Los Sistemas que maneja actualmente el I. Municipio se integrarán en las dependencias que no todavía no utilizan los mismos, logrando de esta manera tener la información requerida en el momento en que se requiere, solucionando el grave problema de la comunicación, mejorando el nivel tecnológico de la Institución.

ESQUEMA DE CONEXIÓN IMPLEMENTADO CON WI-FI



Es posible una gama de instalaciones en función de la estructura que se requiere o que se va a montar

1.5 TÉCNICAS DE LAS TECNOLOGÍAS WI-FI

- Se utilizarán estándares que garanticen la seguridad de las transmisiones a través de la tecnología inalámbrica.
- Mejorar la experiencia del usuario final, incidir en las ventajas o aplicaciones para conseguir en definitiva que la tecnología se convierta en una comodidad para quien lo utiliza y no algo que lo aterra.
- La Wi-Fi actualmente ejerce el papel de principal difusor de las tecnologías inalámbricas y el usuario final puede aprovechar sus ventajas.

1.6 BENEFICIOS DE ESTA TECNOLOGIA

Las redes LAN inalámbricas (WLAN) ofrecen diversas ventajas sobre las redes LAN convencionales (Ethernet, Token-Ring, fibra óptica) porque pueden ser móviles. Los beneficios son evidentes para computadoras portátiles y computadoras de escritorio, dado que el usuario puede verdaderamente trasladarse de un punto a otro y permanecer conectado a la red LAN y a sus recursos. Los beneficios para el mercado de computadoras de escritorio, sistemas de empresas y servidores no son tan evidentes. La red puede establecerse sin incurrir en los gastos y las exigencias de colocar cables e instalar conectores en paredes. Además, las redes inalámbricas son flexibles, dado que las máquinas de escritorio pueden cambiarse de lugar sin ningún trabajo de infraestructura. Esto resulta particularmente útil al instalar sitios temporales o al trabajar en lugares "fijos" que periódicamente cambian de ubicación, tales como las empresas que se trasladan a otra oficina más grande cuando exceden la capacidad de sus instalaciones actuales.

1.6.1 REQUISITOS DE LAS LAN INALÁMBRICAS

Además de incluir los requisitos de cualquier otra red LAN, incluyendo:

- Alta capacidad.
- Cobertura de pequeñas distancias
- Conectividad total de las estaciones conectadas
- Capacidad de difusión

Existe un conjunto de necesidades específicas para entornos de LAN Inalámbricas:

- Rendimiento: El uso del protocolo MAC debe ser eficiente para maximizar la capacidad.

- Número de Nodos: pueden dar soporte a muchos nodos mediante el uso de varias celdas.
- Conexión a la LAN Troncal: se da la interconexión con estaciones situadas en una LAN troncal cableada. Se da soporte a las LAN Inalámbricas con infraestructura por medio de Módulos de control que conectan ambos tipos de LAN, a los usuarios nómadas y a las LAN Inalámbricas ad-hoc.
- Área de Servicio: La superficie de cobertura tiene un diámetro típico entre 100 y 300 metros.
- Consumo de Batería: Cuando los usuarios móviles usan adaptadores sin cable necesitan una batería de larga vida.
- Robustez en la transmisión y seguridad: El diseño de una LAN inalámbrica debe permitir transmisiones fiables incluso en entornos ruidosos y debe ofrecer cierto nivel de seguridad contra escuchas.
- Funcionamiento de red ordenada: Es probable que dos o más redes operen en alguna zona donde sea posible la interferencia entre ella, esto frustra el funcionamiento del algoritmo MAC y pueden permitir accesos no autorizados a una LAN particular.
- Sin intervención/nómada: El protocolo MAC usado debe permitir a las estaciones móviles desplazarse de una celda a otra.
- Configuración dinámica: Los aspectos de direccionamiento MAC y de gestión de red de la LAN deberían permitir la inserción, eliminación y traslado dinámicos y automáticos de sistemas finales sin afectar a otros usuarios.

Equipos Inalámbricos

CAPITULO II

2 TECNOLOGÍA INALÁMBRICA WI-FI

2.1 WI-FI (WIRELESS FIDELITY)

Wireless es un término que significa "SIN CABLES", y que designa a todos aquellos aparatos que, en su funcionamiento no requieren la conexión física entre él y otro. La tecnología de redes inalámbricas ofrece movilidad y una instalación sencilla, además permite la fácil ampliación de una red. Es decir, que podemos estar moviéndonos por nuestra empresa, calle, parque, cafetería, aeropuerto sin perder la conectividad con Internet. Esto es algo que actualmente está tomando gran importancia, ya no tanto para las grandes empresas, sino para todo el mundo

El mundo de las comunicaciones esta recibiendo serie de cambios en su base muy importantes. Los aparatos que hasta ahora tenían una conexión a trabes de una frecuencia de propagación por aire, han pasado o pasaran a tener un conexión cableada. Un caso muy importante de este tipo es el de la televisión domestica, que paso de la conexión por antena a los servicios de fibra óptica, por otro lado las comunicaciones que tenían medio físico cableado, como el teléfono, están pasando y pasaran en un porcentaje muy elevado a ser conexiones inalámbricas.

La causa de este cambio de mentalidad en las comunicaciones se debe encontrar en que los aparatos como el televisor es fijo y por lo tanto puede estar conectados permanentemente de una misma red cableada. De esta manera se deja libre el espacio de radiofrecuencia que se ocupa, dejándolo libres para otros servicios futuros móviles. En el caso particular del teléfono se puede comprobar fácilmente, ya que es un medio personal de comunicación, que es de gran provecho para la

sociedad que este sea de carácter inalámbrico con todos las ventajas que genera no estar limitados por cables.

Si nos basamos en el gran y continuo crecimiento que tiene la informática y la telecomunicación, podemos asegurar que los PC y los teléfonos tendrán cada vez más importancia en el mundo laboral, es necesario la utilización de redes inalámbricas para un desplazamiento ágil, cómodo, rápido y confiable de los trabajadores en el entorno de su trabajo, este principio básico es cada vez mas reconocido como parte fundamental de la productividad y competitividad de la empresa.

La expresión Wi-Fi (abreviatura de Wireless Fidelity) se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que permite la creación de redes de trabajo sin cables (conocidas como WLAN, Wireless Local Area Netwoks).

En un principio, la expresión Wi-Fi era utilizada únicamente para los aparatos con tecnología 802.11b, el estándar dominante en el desarrollo de las redes inalámbricas, de aceptación prácticamente universal, que funciona en una banda de frecuencias de 2,4 GHz y permite la transmisión de datos a una velocidad de hasta 11Mbps (aunque la velocidad real de transmisión depende en última instancia del número de usuarios conectados a un punto de acceso). Con el fin de evitar confusiones en la compatibilidad de los aparatos y la interoperabilidad de las redes, el término Wi-Fi se extendió a todos los aparatos provistos con tecnología 802.11 (ya sea 802.11a, 802.11b, 802.11g, 802.11i, 802.11h, 802.11e, 802.11n con diferentes frecuencias y velocidades de transmisión).

Entre las predicciones tecnológicas, todas las grandes consultoras coinciden en señalar el desarrollo de las tecnologías Wi-Fi como una de las principales tendencias futuristas. Por lo que se refiere a la distribución de las aplicaciones Wi-Fi, Aberdeen estima que los computadores personales (portátiles y de sobremesa) será el principal destino de las mismas, pero no desestima el impacto que tendrán en teléfonos móviles y PDAs.

Como muestra de las grandes expectativas que se tiene, se pretende extender una red de acceso inalámbrico, con 20 puntos de acceso en los principales. Basándose en la tecnología Wi-Fi, el objetivo de posibilitar el acceso inalámbrico y de banda ancha a Internet desde su red de puntos de acceso.

Wi-Fi es una tecnología novedosa y han empezado a utilizar, en hogares o empresas para conectarse a cortas y largas distancias, el problema son las seguridades que en la mayoría de hogares quedan sin protección de los crackers. Antes de consolidarse definitivamente, deberá resolver una serie de incógnitas que dependen en la actualidad sobre su viabilidad como son:

- Seguridad: una de las mayores tareas pendientes, a la espera de estándares que garanticen la seguridad de las transmisiones inalámbricas.
- Provecho: mejorar la experiencia del usuario final, incidir en las ventajas o aplicaciones para éste, conseguir en definitiva que la tecnología se convierta en una comodidad.
- Flexibilidad: dado el gran número de aplicaciones y tecnologías emergentes, el usuario final debe contar con la posibilidad de actualizar ambas, de modo que pueda planear a medio y largo plazo, más que limitarse a las necesidades inmediatas.
- Educación: actualmente, la Wi-Fi ejerce el papel de principal difusor de las tecnologías inalámbricas y valedor de sus ventajas. A medida que el mercado

crezca y se segmente, así como las necesidades particulares del usuario final, otros agentes deberán hacerse cargo de este papel o colaborar en la tarea.

2.1.1 ESTÁNDARES

Wi-Fi. (Wireless Fidelity), es un conjunto de estándares basados en especificaciones IEEE 802.11 (802.11a, 802.11b, 802.11g, 802.11i, 802.11h, 802.11e, 802.11n con diferentes frecuencias y velocidades de transmisión).
802.11. Radiofrecuencia 2.4 GHz o infrarrojo (850 a 950 nm). 1-2 Mbps
802.11a (1999)
Extensión de 802.11 en de la banda de los 5GHz UNII, OFDM. 54 Mbps.
802.11b (1999)
Espectro ensanchado de secuencia directa DSSS (300 m), 11Mbps.
802.11 e (2004). Calidad de servicio QoS y VoIP para 802.11 a ,h y g.
802.11 f (2003). Roaming con IAPP (Inter Access Point Protocol).
802.11g (2003).
20-54 Mbps usando DSSS y OFDM en la banda de 2.4 GHz
Es compatible hacia atrás con 802.11b.
802.11h. Desarrollado por exigencia de la Unión Europea (2003).
Selección de frecuencia dinámica (DFS) y control de potencia (TPC).
802.11i Estándar adicional para seguridad: RC4 o AES. (2004).
802.11n 540 Mbits/s, Multiple Input Multiple Output (MIMO). (2006).
WECA (Wireless Ethernet Compatibility Alliance)
Conformidad y Certificación Wi-Fi (Wireless Fidelity) para sus productos.

Estos estándares fueron creados para ser utilizados en redes locales inalámbricas de largo alcance, es frecuente que en la actualidad también se utilice para acceder a Internet y otras aplicaciones. Existen algunos programas capaces de capturar paquetes, trabajando con Wi-Fi en modo promiscuo, de forma que puedan calcular

la contraseña de la red y de esta forma acceder a ella, las claves de tipo WEP son relativamente fáciles de conseguir para cualquier persona con un conocimiento medio de informática.

La alianza Wi-Fi arregló estos problemas sacando el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad.

Los dispositivos Wi-Fi ofrecen gran comodidad en relación a la movilidad que ofrece esta tecnología, sobre los contras que tiene Wi-Fi es la capacidad de terceras personas para conectarse a redes ajenas si la red no está bien configurada convirtiéndose en una red no segura.

2.1.1.1 CARACTERÍSTICAS Wi-Fi

- Wireless Ethernet.
- Técnica de acceso al medio: CSMA/CA
- Topología en estrella con Access Point
- Alcance moderado: 1000 mts
- Estándares para:
- OFDM (802.11a y g) hasta 54 Mbps. El mercado se está desplazando hacia 802.11g
- DSSS (802.11g/n) hasta 11 Mbps Dominante en el mercado

2.1.2 COMUNICACIONES Wi-Fi

El mundo de las comunicaciones esta recibiendo serie de cambios en su base muy importantes. Los aparatos que hasta ahora tenían una conexión a través de una frecuencia de propagación por aire, han pasado o pasaran a tener un conexión cableada. Un caso muy importante de este tipo es el de la televisión domestica, que paso de la conexión por antena a los servicios de fibra óptica, por otro lado las comunicaciones que tenían medio físico cableado, como el teléfono, están pasando y pasaran en un porcentaje muy elevado a ser conexiones inalámbricas. La causa de este cambio de mentalidad en las comunicaciones se debe encontrar en que los aparatos como el televisor es fijo y por lo tanto puede estar conectados permanentemente de una misma red cableada. De esta manera se deja libre el espacio de radiofrecuencia que se ocupa, dejándolo libres para otros servicios futuros móviles.

En el caso particular del teléfono se puede comprobar fácilmente, ya que es un medio personal de comunicación, que es de gran provecho para la sociedad que este sea de carácter inalámbrico con todos las ventajas que genera no estar limitados por cables. Si nos basamos en el gran y continuo crecimiento que tiene la informática y la telecomunicación, podemos asegurar que los PC y los teléfonos tendrán cada vez mas importancia en el mundo laboral, es necesario la utilización de redes inalámbricas para un desplazamiento ágil, cómodo, rápido y confiable de los trabajadores en el entorno de su trabajo, este principio básico es cada vez mas reconocido como parte fundamental de la productividad y competitividad de la empresa.

2.1.2.1 COMUNICACIONES Wi-Fi FRECUENTES

- Microondas terrestres:

  Por lo general se utilizan antena parabólica de aproximadamente 3 metros de diámetro, tienen que estar fijadas rígidamente. Este emite in estrecho haz que debe estar perfectamente enfocado con la otra antena, en este caso receptor. Es conveniente que las antenas este a una cierta distancia del suelo para impedir que algún obstáculo se interponga en las has. La distancia máxima entre antenas sin ningún obstáculo es de 7,14 Km, claro que esta distancia se puede aumentar si se aprovecha a la curvatura de la tierra haciendo refractar las microondas en la atmósfera terrestre.

  El uso principal de este tipo de transmisión se da en las telecomunicaciones de largas distancias, se presenta como alternativa del cable coaxial o la fibra óptica. Este sistema necesita menor numero de repetidores o amplificadores que el cable coaxial pero necesita que las antenas estén alineadas. Los principales usos de las Microondas terrestres son para la transmisión de televisión y voz.

  También se usan para enlazar punto a punto dos edificios. La banda de frecuencia van desde 2 a 40 GHz. Cuanto mayor es la frecuencia utilizada mayor es el ancho de banda lo que da mayor velocidad virtual de transmisión.

- Microondas por satélite.

  La que hace básicamente es retrasmitir información, se usan como enlace de dos transmisores/receptores terrestres denominados estación base. El satélite funciona como un espejo donde la señal rebota, su principal función es la de amplificar la señal corregirla y retransmitirla a una o más antenas. Estos satélites son geoestacionarios, es decir se encuentra fijos para un observador

que está en la tierra. Es importante que los satélites mantengan fija esta orbita geoestacionaria ya que de lo contrario podrían perder la alineación con las antenas terrestres.

- Operan en una serie de frecuencia llamada TRANSPODERS.

  Si dos satélites utilizan la misma banda de frecuencia o están lo suficientemente próximos pueden interferirse mutuamente. Para evitar esto debe tener un separación de 4 º(grados) (desplazamiento angular). Las comunicaciones satelitales se utilizan principalmente para la difusión de televisión, transmisiones telefónicas de larga distancia y redes privadas entre otras. También se usan para proporcionar enlaces punto a punto entre las centrales telefónicas en las redes públicas. El rango de frecuencia está comprendido entre 1 y 10 GHz.

- Espectro infrarrojo (IR)

  Los infrarrojos son útiles para las conexiones locales punto a punto, así como para aplicaciones multipunto dentro de un arrea de cobertura limitada, ejemplo: una habitación. Una significativa diferencia entre este tipo y las microondas es que las primeras no pueden atravesar paredes. El espectro infrarrojo a diferencia de las microondas no tiene problemas de interferencia o seguridad, tampoco tiene problemas de asignación de frecuencia, ya que estas bandas no necesitan permiso.

  Son muy utilizadas en aplicaciones LAN verticales (Ejemplo: inventario de almacén), clientes conectándose en grandes áreas abiertas, impresión inalámbrica y la transferencia de archivos.

- Transmisión por onda de Luz.

  La señalización óptica se ha utilizado durante siglos, un caso muy primario son los faros ubicados en las costas, en cierta forma estos dispositivos envían una cierta información a otro dispositivo. Una aplicación moderna y un poco más complicada es la conexión de las redes LAN de dos edificios por medio de laceres montados en sus respectivas azoteas.

  La señalización óptica coherente con laceres es inherentemente unidireccional, de modo que cada edificio necesita su propio láser y su propio foto detector, este esquema proporciona un ancho muy alto y un costo muy bajo. También es relativamente fácil de instalar y, a diferencia de las microondas no requiere una licencia de la FCC (Comisión Federal de Comunicaciones).

  La ventaja del láser, un haz muy estrecho, es aquí también una debilidad. Apuntar un rayo láser de 1mm a 500 metros de distancia, requiere de una gran precisión, por lo general se le añaden lentes al sistema para enfocar ligeramente el rayo. Una desventaja de los rayos láser es que no pueden atravesar la niebla ni la lluvia , este sistema solo funciona bien los días soleados.

- Ondas de Radio.

  Las ondas de radio son fáciles de genera, pueden viajar distancias muy largas y penetrar edificios sin problemas, de modo que se utilizan mucho en la comunicación tanto en interiores como en exteriores. Las ondas de radio también son omnidireccionales, lo que significa que viaja en todas las direcciones desde la fuente , por lo que el transmisor y le receptor no tiene que alinearse físicamente.

2.1.2.2 ANTENAS UTILIZADAS EN ENLACES INALÁMBRICOS

- Direccional.

  También llamada sistema de banda angosta (narrow band) o de frecuencia dedicada, la antena de transmisión emite la energía electromagnética en un haz; por tanto en este caso las antenas de emisión y recepción deben estar perfectamente alineadas. Para que la transmisión pueda ser enviada en una dirección especifica , debemos tener en cuenta la frecuencia , la cual debe ser mucho mayor que la utilizada en transmisiones omnidireccionales.

- Omnidireccionales.

  O también llamadas sistemas basados en espectros dispersos o extendidos (spread spectrum), al contrario que las direccionales, el diagrama de radiación de la antena es disperso, emitiendo en todas direcciones, pudiendo la señal ser recibida por varias antenas. En general cuanto mayor es la frecuencia de la señal transmitida es mas factible concentrar la energía en un hay direccional.

Esta antena Wi-Fi ofrece un soporte de 12 pulgadas de plomo finalizando en un conector N - Hembra .

El sistema de montaje consta de 02 abrazaderas según se aprecia en la imagen adjunta.

Especificaciones

Frecuencia	2400-2500 MHz
Ganancia	15 dBi
Ancho de onda Horizontal	360°
Ancho de onda Vertical	8°
Impedancia	50 Ohm
Polarización	Vertical
Max. ingreso de energia	100 Watts
Peso	1.5 Kg
Dimensiones /Diámetro	1.03m x 38.6 mm

2.1.3 SEGURIDADES CON WI-FI

Un problema que presenta este tipo de redes es el de su seguridad. Es decir, es más difícil evitar que entren usuarios no deseados en una red inalámbrica que en una red cableada. Por otra parte, hay ya algunas voces que opinan que el uso de bandas de frecuencias que no necesitan licencias, pueden dar problemas a la larga cuando el número de usuarios crezca, y que las operadoras, que son las que

controlan el acceso a Internet, no permitirán el acceso con la facilidad y bajo precio que lo están haciendo actualmente, para eso es necesario tomar en cuenta ciertas reglas de seguridad que se detallan a continuación:

2.1.3.1 PERMISOS DE ACCESO

La seguridad basada en autentificación de usuario es la más usada, nos permite administrar y asignar derechos a los usuarios de la red. Permitiendo o denegando los accesos a los recursos a través de una base de datos en el servidor. El trabajo del administrador deberá incluir la administración de usuarios.

Otra manera de administrar usuarios es mediante el uso de grupos de usuarios, el cual nos da la facilidad de aplicar las políticas de seguridad a grupos específicos los cuales heredaran estas a los miembros de dicho grupo.

Se debe tomar en cuenta el uso de cortafuegos que permita administrar el acceso de usuarios de otras redes así como el monitorear las actividades de los usuarios de la red, permitiendo el tener una bitácora de sucesos de red.

- Las bitácoras son de gran utilidad para aplicar auditorias a la red. La revisión de los registros de eventos dentro de la red permite ver las actividades de los usuarios dentro de la red, esto permite al administrador darse cuenta de los accesos no autorizados por parte de los usuarios y tomar las medidas que faciliten incrementar la seguridad.
- La auditoria permite monitorear algunas de las siguientes actividades o funciones
- Intentos de acceso. Conexiones y desconexiones de los recursos designados.
- Terminación de la conexión.

- Desactivación de cuentas.
- Apertura y cierre de archivos.
- Modificaciones realizadas en los archivos.
- Creación o borrado de directorios.
- Modificación de directorios.
- Eventos y modificaciones del servidor.
- Modificaciones de las contraseñas.
- Modificaciones de los parámetros de entrada.

Estas medidas se podrán implementar más o menos fáciles dependiendo de nuestro sistema operativo de red, ya que algunos sistemas operativos tienen la facilidad de administrar las auditorias que el administrador determine en forma sencilla. Se puede implementar algoritmos de encriptación de datos para la información relevante. Hay algunos organismos que certifican este tipo de software y garantizan la confidencialidad de los datos a través de la red, en especial en Internet, donde la seguridad de nuestra información es delicada.

La especificación del estándar 802.11 originalmente utiliza tres métodos para la protección de la red. SSID (Identificador de Servicio): es una contraseña simple que identifica la WLAN. Cada uno de los clientes debe tener configurado el SSID correcto para acceder a la red inalámbrica.

- Filtrado de direcciones MAC. Se definen tablas que contienen las direcciones MAC de los clientes que accesarán a la red.
- WEP (Privacidad Equivalente a Cable): es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. El IEEE creo el estándar 802.X diseñado para dar

controlar los accesos a los dispositivos inalámbricos clientes, Access point y servidores. Este método emplea llaves dinámicas y requiere de autentificación por ambas partes. Requiere de un servidor que administre los servicios de de autentificación de usuarios entrantes.

- El WAPA añade una mayor capacidad de encriptación así como métodos de identificación de usuarios que no se contemplaron en el estándar 802.X.
- OTRAS AMENAZAS Los virus informáticos son pequeños programas de computadora que al igual que un virus biológico, infecta equipos de computo y se propaga a través de la red o utilizando otros medios de transmisión como Memorias, disquetes, discos ópticos, etc.
- El crecimiento de las redes y en especial de la Internet ha facilitado la propagación de virus de forma acelerada, un método de propagación de virus común es el uso de correo electrónico. Al abrir un correo infectado por virus puede infectar el equipo y puede ser capaza de reenviarse a otros usuarios de correo utilizando la libreta de direcciones del usuario. Hay que tomar en cuenta que cualquier medio de intercambio de datos puede ser un medio potencial de propagación de virus.

2.1.3.2 PREVENCIÓN

- Se debe tener políticas de prevención contra estas amenazas que ponen en riesgo la integridad de la red. Esto se puede evitando abrir correos sospechosos, entrar en páginas de Internet con contenidos pornográficos, de juegos y paginas sospechosas. Instalar programas antivirus. Actualmente hay una gran variedad de proveedores de estos servicios, hay que elegir el que más se adapte a nuestras necesidades. Algunos cuentan con detectores de spayware, robots, antispam, entre estas amenazas potenciales.

- Asegurar el Punto de Acceso

- Cambia la contraseña por defecto: Todos los fabricantes establecen un password por defecto de acceso a la administración del Punto de Acceso. Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible que el observador la conozca.
- Evita contraseñas como tu fecha de nacimiento, el nombre de tu pareja, etc. Intenta además intercalar letras con números.
- Aumentar la seguridad de los datos transmitidos:
- Usa encriptación WEP/WPA.
- Activa en el Punto de Acceso la encriptación WEP. Mejor de 128 bits que de 64 bits… cuanto mayor sea el número de bits mejor. Los Puntos de Acceso más recientes permiten escribir una frase a partir de la cual se generan automáticamente las claves. Es importante que en esta frase intercales mayúsculas con minúsculas y números, evites utilizar palabras incluidas en el diccionario y secuencias contiguas en el teclado (como "qwerty", "fghjk" o "12345").
- Algunos Puntos de Acceso más recientes soportan también encriptación WPA (Wi-Fi Protected Access), encriptación dinámica y más segura que WEP.
- Si se activa WPA en el Punto de Acceso, tanto los accesorios y dispositivos WLAN de una red como el sistema operativo deben soportarlo, es necesario instalar una actualización).
- Ocultar tu red Wi-Fi
- Cambia el SSID por defecto.

2.1.3.3 USO DE LA TECNOLOGÍA WI-FI INALÁMBRICAS ESTÁTICA Y MÓVIL

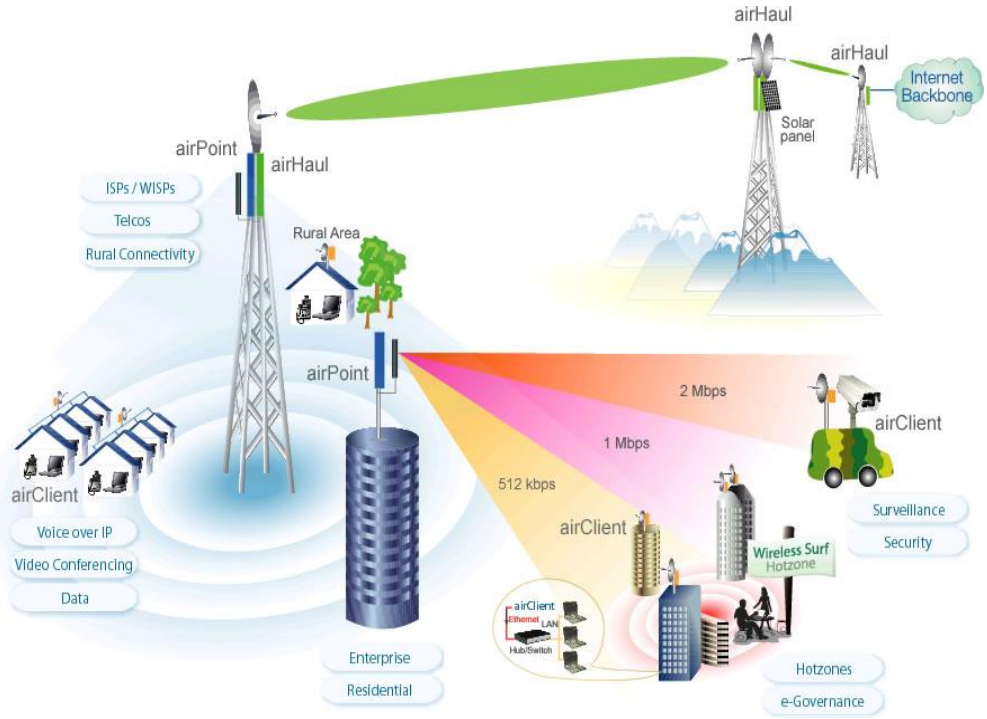
Es similar a una red de oficina pero ampliado al área más amplia. Wi-Fi posee una política descentralizada; lo que implica pequeños nodos para áreas no mayores a 10 Km. de radio, estrategia que garantiza una excelente cobertura y un señal permanente. Nos basamos en los equipos normados WI-FI (IEEE 811.2b, 811.2g o 811.2n), lo que aumenta la calidad del servicio a utilizar equipos que satisfacen la normativa internacional vigente. Esto se puede observar al ver funcionar los equipos en Windows XP SP2 donde el mismo sistema operativo esta preparado para conectarse a este tipo de redes.

La expresión Wi-Fi (abreviatura de Wireless Fidelity) se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que permite la creación de redes de trabajo sin cables (WLAN). Entre las predicciones tecnológicas para 2007, se señala unánimemente el desarrollo de las tecnologías Wi-Fi como una de las principales tendencias de la nueva tecnología. A continuación se detallan algunas características de los elementos WI-FI:

- Punto para enlace Wi-Fi 2.4Ghz 802.11b 802.11g y 811.2n.
- Una la red de su oficina con otra u otras en red LAN.
- Comparta una cuenta de su proveedor Internet en todas sus oficinas.
- Elimina el uso de alquiler canales dedicados.
- Elimina el uso de cables para unir oficinas.
- Fácil instalación.

- Movilidad pues cada punto se puede mover y solo se requiere direccionar las antenas.

ESQUEMA DE CONEXIÓN IMPLEMENTADO CON WI-FI



Es posible una gama de instalaciones en función de la estructura que se requiere o que se va a montar

2.1.4 VENTAJAS Y DESVENTAJAS

2.1.4.1 VENTAJAS

- Conseguir en definitiva que la tecnología se convierta en una comodidad para quien lo utiliza

- Evitar el manejo de cableado cuando un usuario es asignado a otro lugar
- Manejar equipos móviles con la seguridad que se va atener señal dentro del rango establecido
- Se requieren menos recursos para su instalación

2.1.4.2 DESVENTAJAS

- Las redes inalámbricas son más vulnerables
- Se tiene que utilizar más recursos para evitar el acceso a este tipo de redes
- La información se encuentra mas vulnerable que con una red alámbrica.
- Se debe configurar de manera mas adecuada sino serán un blanco perfecto para los cracker.

CAPITULO III

3 SEGURIDAD DE ENLACES INALÁMBRICOS

Toda organización debe estar a la vanguardia de los procesos de cambio. Donde disponer de información continua, confiable y en tiempo, constituye una ventaja fundamental.

- Donde tener información es tener poder.
- Donde la información se reconoce como:
- Crítica, indispensable para garantizar la continuidad operativa de la organización.
- Valiosa, es un activo corporativo que tiene valor en sí mismo.
- Sensitiva, debe ser conocida por las personas que necesitan los datos.
- Donde identificar los riesgos de la información es de vital importancia.
- La seguridad informática debe garantizar:
- La Disponibilidad de los sistemas de información.
- El Recupero rápido y completo de los sistemas de información
- La Integridad de la información.
- La Confidencialidad de la información.

3.1 DEFINICIÓN DE SEGURIDAD

La seguridad se ha convertido en uno de los principales desafíos a que se enfrentan los responsables políticos y el estudio de una respuesta adecuada a este problema constituye una tarea cada vez más compleja. Hace tan solo unos años, la seguridad de la red era fundamentalmente un problema para los monopolios de Estado que ofrecían servicios especializados basados en redes públicas, fundamentalmente la red telefónica. La seguridad de los sistemas informáticos se limitaba a las grandes organizaciones y a los controles de acceso. La elaboración de una política de seguridad constituía una tarea relativamente fácil. La situación ha cambiado radicalmente debido a una serie de transformaciones producidas en el mercado mundial, entre las que cabe citar la liberalización, la convergencia y la mundialización.

En la actualidad predomina la propiedad y gestión privadas de las redes. Los servicios de comunicación están abiertos a la competencia y la seguridad forma parte de la oferta de mercado. No obstante, muchos clientes ignoran la amplitud de los riesgos en materia de seguridad a la hora de conectarse a la red y toman su decisión sin estar perfectamente informados.

Las redes y los sistemas de información están en un proceso de convergencia. Cada vez están más interconectados, ofrecen el mismo tipo de servicio sin discontinuidad y personalizado y comparten en cierta medida la misma infraestructura. Los equipos terminales (PC, teléfonos móviles, etc.) se han convertido en un elemento activo de la arquitectura de la red y pueden conectarse a distintas redes.

Las redes son internacionales. Una parte significativa de la comunicación actual es trans-fronteriza y transita por terceros países (a veces sin que el usuario final sea consciente de ello), por lo que cualquier solución a los problemas de seguridad habrá de tener en cuenta este factor. La mayoría de las redes están formadas por productos comerciales procedentes de proveedores internacionales. Los productos de seguridad deberán ser compatibles con las normas internacionales.

3.2 SEGURIDAD DE LA INFORMACIÓN

La seguridad de las redes y de la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Las redes son sistemas de almacenamiento, procesamiento y transmisión de datos. Están compuestos de elementos de transmisión (cables, enlaces inalámbricos, satélites, encaminadores, pasarelas, conmutadores, etc.) y de servicios de apoyo (sistema de nombres de dominio incluidos los servidores raíz, servicio de identificación de llamadas, servicios de autenticación, etc.). Conectadas a las redes existe un número cada vez mayor de aplicaciones (sistemas de entrega de correo electrónico, navegadores, etc) y de equipos terminales (teléfono, computadores servidores, computadores personales, teléfonos móviles, organizadores personales, aparatos electrodomésticos, máquinas industriales, etc.).

Los requisitos generales de seguridad de las redes y los sistemas de información presentan las siguientes características generales interdependientes:

- Disponibilidad – Significa que los datos son accesibles y los servicios operativos aún en caso de alteraciones del tipo de cortes de corriente, catástrofes naturales, accidentes o ataques. Esta característica es particularmente importante cuando una avería de la red de comunicaciones pueda provocar interrupciones en otras redes críticas como el transporte aéreo o el suministro de electricidad.

- Autenticación – Confirmación de la identidad declarada de usuarios o entidades jurídicas. Son necesarios métodos de autenticación adecuados para muchos servicios y aplicaciones, como la conclusión de un contrato en línea, el control del acceso a determinados servicios y datos (por ejemplo, para el telé trabajo) y la autenticación de los sitios Web (por ejemplo, en el caso de los bancos en Internet). La autenticación debe contemplar la posibilidad de mantener el anonimato, dado que muchos servicios no necesitan la identidad del usuario y sólo requieren la confirmación fiable de determinados criterios (las denominadas credenciales anónimas) como la capacidad de pago.

- Integridad – Confirmación de que los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados. La integridad es especialmente importante en relación con la autenticación para la conclusión de contratos o en los casos en los que la exactitud de los datos es crítica (datos médicos, diseño industrial, etc.).

- Confidencialidad – Protección de las comunicaciones o de los datos almacenados contra su interceptación y lectura por parte de personas no autorizadas. La confidencialidad es especialmente necesaria para la transmisión de datos sensibles y uno de los requisitos a la hora de dar respuesta a las inquietudes en materia de intimidad de los usuarios de las redes de comunicación.

Es preciso tener en cuenta todos los factores que pueden amenazar la seguridad, y no únicamente los de carácter malintencionado. Desde el punto de vista de los usuarios, los peligros derivados de los incidentes del entorno o de errores humanos que alteren la red pueden ser tan costosos como los ataques malintencionados.

Un sistema de seguridad habitualmente utilizado en Internet es el denominado “Secure Socket Layer” (SSL), que encripta la comunicación entre un servidor web y el navegador del usuario. En el pasado, el desarrollo de esta tecnología, en particular su versión más potente (128 bit), se ha visto frenado por anteriores restricciones a su exportación por parte de los países desarrollados

3.3 SEGURIDAD EN BASES DE DATOS

Aunque hablar de seguridad En Base de Datos en las Redes Inalámbricas parece una utopía, esto empieza a cambiar gracias al uso del **protocolo 802.1x**, que aunque es poco conocido, ofrece las seguridades de una red física para base de datos. Sin embargo, asusta pensar que más del 98% de las empresas emplean el protocolo 802.11.

La seguridad de las Bases de Datos con redes inalámbricas está más que cuestionada hoy en día. Muchas de las redes existentes en la actualidad, basadas en el protocolo 802.11, ni siquiera se encuentran cifradas, por lo que el acceso a estas redes es tan sencillo como dejar que Windows se conecte de manera automática o, como mucho, que tengamos que encontrar una IP válida para conectarnos a la red.

Pongamos un ejemplo sencillo: imaginemos un banco en el que tuviésemos dinero a la vista y ni siquiera tuviésemos personal de seguridad vigilando la entrada. En el mejor de los casos, alguien se colaría y cogería el dinero sin que ningún trabajador se diera cuenta. Los usuarios con algunos conocimientos cifran las redes basadas en el protocolo 802.11 mediante WEP (Wired Equivalent Privacy). Este es un procedimiento mediante el cual todas las comunicaciones establecidas por la red se encuentran cifradas con una clave compartida para todos los usuarios, que se emplea tanto para cifrar como para descifrar los mensajes enviados. En este caso, el acceso a dichas redes, se complica un poco… pero no mucho: bastará con usar algún programa sniffer como AirSnort o WEPcrack, para monitorizar la red y sacar la clave que se está empleando para cifrar los datos. Asusta pensar que algunas claves, pueden ser descubiertas con una PDA con Linux y algún programa de este tipo en menos de 2 horas.

Sigamos con nuestro ejemplo: el banco, para evitar más robos, decide poner un agente de seguridad en la puerta que pida una clave, para acceder a las instalaciones. Tras unas horas, un ladrón, lo suficientemente cerca, escucha la clave y se introduce en el banco, mencionando dicha clave. Como vemos, no ha servido de mucho. La solución parece sencilla: modificaremos nuestra clave de nuestra Base de Datos lo suficientemente rápido como para que nadie sea capaz de descifrarla. Este procedimiento, auque posible, es inabordable: necesitaríamos de un administrador en nuestra red que, cada 2 horas, cambiase la clave de nuestra red en todos y cada uno de los equipos. Este procedimiento es imposible de llevar a cabo de manera automática, porque cualquier procedimiento que se intente, necesitaría que todos los computadores conectados se enterasen del cambio a la vez, ya que si por cualquier motivo un ordenador no estuviese conectado en el momento del cambio, se quedaría fuera de la red y tendría que ser reconfigurado manualmente. En nuestro ejemplo del banco: ¡el agente de seguridad tendría que estar llamando por teléfono a todos sus empleados para decirles la clave.

3.3.1 PROTOCOLO 802.1X , AUTENTIFICACIÓN Y MANEJO DE CLAVES

Con el fin de solucionar estos problemas surge el protocolo 802.1x, que aunque lleve ya algunos años en el mercado, pocas empresas lo utilizan, debido a su complejidad de instalación. Este protocolo ofrece un marco en el que se lleva a cabo un proceso de autentificación del usuario, así como un proceso de variación dinámica de claves, todo ello ajustado a un protocolo, denominado EAP (Extensible Authentication Protocol). Mediante este procedimiento, todo usuario que esté empleando la red se encuentra autentificado y con una clave única, que se va modificando de manera automática y que es negociada por el servidor y el cliente de manera transparente para el usuario. El servicio soporta múltiples procesos de autenticación tales como Kerberos, Radius, certificados públicos, claves de una vez, etc. Aunque no es el objetivo de este artículo enumerar los diferentes procesos de autentificación, basta con mencionar que Windows 2003 Server ® o XP, soportan este servicio.

Para entender cómo funciona el protocolo 802.1x sigamos el siguiente esquema.

El cliente, que quiere conectarse a la red, manda un mensaje de inicio de EAP que da lugar al proceso de autentificación. Siguiendo con nuestro ejemplo, la persona que quiere acceder al banco pediría acceso al guardia de seguridad de la puerta. El punto de acceso a la red respondería con una solicitud de autentificación EAP. Además, antes de preguntarle, el guarda de seguridad le diría una contraseña al cliente, para que éste sepa que realmente es un guardia de seguridad.

El cliente responde al punto de acceso con un mensaje EAP que contendrá los datos de autentificación. Nuestro cliente le daría el nombre y los apellidos al guardia de seguridad además de su huella digital. El servidor de autentificación

verifica los datos suministrados por el cliente mediante algoritmos, y otorga acceso a la red en caso de validarse. En nuestro caso, el sistema del banco verificaría la huella digital, y el guardia validaría que se correspondiese con el cliente.

El punto de acceso suministra un mensaje EAP de aceptación o rechazo, dejando que el cliente se conecte o rechazándolo. Nuestro guardia de seguridad le abrirá la puesta o no, en función de la verificación al cliente.

Una vez autentificado, el servidor acepta al cliente, por lo que el punto de acceso establecerá el puerto del cliente en un estado autorizado. Nuestro cliente estará dentro del banco.

De esta manera, el protocolo 802.1x provee una manera efectiva de autentificar, se implementen o no claves de autentificación WEP. De todas formas, la mayoría de las instalaciones 802.1x otorgan cambios automáticos de claves de encriptación usadas solo para la sesión con el cliente, no dejando el tiempo necesario para que ningún usuario sea capaz de obtener la clave. Se piensa que en futuro, el uso del protocolo 802.1x está en proceso de convertirse en un estándar, y sería más que adecuado que pensases en él como la solución para tu red inalámbrica. Windows XP® implementa 802.1x de manera nativa, aunque necesita algún servidor Windows Server en la red.

3.4 SEGURIDAD EN INTERNET E INTRANET

Actualmente las redes se encuentran ampliamente digitalizadas y controladas por computadores. En el pasado la razón de perturbación de la red más frecuente era un fallo en el sistema informático que controla la red y los ataques a las redes estaban dirigidos principalmente a dichos computadores.

En la actualidad, los ataques más peligrosos suelen cebarse en los puntos débiles y más vulnerables de los componentes de las redes (sistemas operativos, encaminadores, conmutadores, servidores de nombres de dominio, etc.)

Si bien los ataques al sistema telefónico no han constituido una gran preocupación en el pasado, los ataques a Internet se han hecho bastante frecuentes. Esto se debe al hecho de que las señales de control telefónicas están separadas del tráfico y pueden ser protegidas, mientras que Internet permite a los usuarios acceder a los computadores clave de gestión. No obstante, la red telefónica puede hacerse más vulnerables en el futuro en la medida en que pueda integrar elementos clave de Internet y su plan de control esté abierto a agentes externos.

3.5 ATAQUES INFORMÁTICOS

Según el último informe de seguridad de Cisco, que analiza los ataques producidos en 2007 y pronostica tendencias para este año, "*las amenazas y los ataques tienen un carácter más global y sofisticado, y esta tendencia continuará en los próximos años"*.

Cisco ha ampliado en este informe el espectro habitual de ataques informáticos, pasando del análisis sobre los habituales gusanos, troyanos, spam, phishing, etc… a un análisis por categorías que engloba siete conceptos de amenaza: física, legal, humana, geopolítica, de vulnerabilidad, de responsabilidad y de identidad.

Analizar las amenazas informáticas es cada vez más complicado, porque los ataques y sus motivaciones también han ganado complejidad con el paso del tiempo. Según Cisco, "hace años, virus y gusanos saqueaban los sistemas informáticos con el único propósito de hacer daño y adquirir fama". No obstante, últimamente este tipo de ataques se ha combinado con otros destinados a robar

dinero o información personal de los usuarios de Internet, con las conocidas técnicas de phishing, por ejemplo. “Este enfoque de robo y riqueza”, según Cisco, “ha evolucionado posteriormente en un fenómeno mundial” que suele responder a una combinación de motivaciones.

3.5.1.1 PRECAUCIÓN CONTRA ATAQUES INFORMÁTICOS

Los expertos en seguridad de Cisco han diseñado una serie de recomendaciones relacionadas con cada una de las categorías de amenaza que define el informe de seguridad.

- Auto diagnóstico: realizar auditorías periódicas y evaluar los medios que se pueden utilizar para evitar a las amenazas.
- Modas: según se ha podido observar, los ataques van allí donde hay más gente. Por tanto, si una aplicación está haciendo furor en la Red, será un blanco perfecto.
- Concienciación: los empleados suelen poner en peligro la seguridad informática de la empresa porque no se sienten responsables de ella.
- Formación: para que el punto anterior funcione, los empleados y toda la plantilla de la empresa deben saber qué prácticas son seguras y cuales no.
- Configurar una red segura, capaz de colaborar, inspeccionar, adaptase y resolver problemas de seguridad a lo largo de todo su recorrido.
- Identificar proveedores de seguridad que puedan ofrecer productos adaptados a toda la infraestructura de red.

Internet depende del funcionamiento del sistema de nombres de dominio (DNS) por medio del cual se traducen direcciones de la red abstractas (por ejemplo, IP N° 147.67.36.16) en nombres comprensibles (por ejemplo, www.espe.edu.ec) y viceversa. Si falla una parte del DNS no se podrá localizar algunos sitios Web y los sistemas de envío del correo electrónico podrán dejar de funcionar. La corrupción

de los servidores raíz DNS u otros servidores de nombres de dominio de nivel superior podría provocar una perturbación general. Se han descubierto ciertos puntos débiles en los programas utilizados por la mayor parte de los servidores de nombres de dominio.

3.5.2 EJECUCIÓN DE PROGRAMAS MALINTENCIONADOS

Que modifican y destruyen los datos, que funcionan con programas informáticos, lamentablemente pueden usarse también para desactivar un ordenador y para borrar o modificar los datos. Como ya se ha explicado, cuando esto ocurre en un ordenador que forma parte de la gestión de una red, los efectos de estas alteraciones pueden tener un alcance considerable. Un virus es un programa informático malintencionado. Es un programa que reproduce su propio código adhiriéndose a otros programas de modo que cuando se ejecuta el programa informático infectado se activa el código del virus.

Existen otros tipos de software maligno: algunos afectan únicamente al ordenador en el que se copian, mientras que otros se propagan a otros computadores conectados en la red. Por ejemplo, existen programas (denominados "bombas lógicas") que permanecen en letargo hasta que son activados por un acontecimiento específico, como una fecha (por ejemplo, viernes 13). Otros programas parecen benignos pero cuando se lanzan ponen en marcha un ataque maligno ("caballos de Troya"). Otros programas (denominados "gusanos") no infectan otros programas como si se tratara de un virus, sino que crean copias de ellos mismos, copias que crean a su vez más copias que acaban inundando el sistema.

3.5.3 DAÑOS OCASIONADOS

Los virus pueden ser muy destructivos como ponen de relieve los elevados costes que originaron recientes ataques (por ejemplo, "I Love You", "Melissa" y "Kournikova"). Una media del 11% de los usuarios de Internet europeos atraparon un virus en su ordenador doméstico.

3.5.4 SOLUCIONES

Los programas antivirus son la única defensa. Están disponibles en varias modalidades. Por ejemplo, el escáner y desinfectantes de virus identifican y borran los virus conocidos. Su principal debilidad reside en el hecho de que no identifican fácilmente nuevos virus aun cuando se actualicen regularmente. Otro ejemplo de defensa antivirus lo constituye el comprobador de la integridad. Para que un virus pueda infectar un ordenador debe cambiar alguna cosa en ese sistema. El control de integridad permitiría identificar dichos cambios del sistema aun cuando los produzca un virus desconocido. A pesar de la existencia de productos de defensa relativamente bien desarrollados, han aumentado los problemas creados por los programas malignos.

Dos son las razones principales:

- en primer lugar, el grado de apertura de Internet permite que los piratas aprendan los unos de los otros y desarrollen métodos para eludir los mecanismos de protección; en segundo lugar, Internet se extiende y llega a un número cada vez mayor de usuarios, muchos de los cuales no se dan cuenta de la necesidad de tomar precauciones.

- La seguridad dependerá del grado de difusión de los programas de protección. A la hora de efectuar una conexión a la red o de recibir datos, el usuario formula hipótesis sobre la identidad de su interlocutor en función del contexto de la comunicación. La red ofrece algunas indicaciones, pero el mayor riesgo de ataque procede de la gente que conoce el contexto, es decir, los "insiders".

Cuando un usuario marca un número o teclea una dirección Internet en el ordenador, debería alcanzar el destino previsto. Esto es suficiente para un gran número de aplicaciones, pero no para las transacciones comerciales importantes o las comunicaciones médicas, financieras u oficiales, que exigen un nivel más elevado de integridad, autenticación y confidencialidad.

Las declaraciones falsas de personas físicas o jurídicas pueden causar daños de diversos tipos. Los usuarios pueden descargar programas malignos de un sitio Web que se presenta como una fuente fiable. Programas de rechazo de este tipo pueden transmitir datos confidenciales a personas no autorizadas. La declaración falsa puede ser la causa del rechazo de un contrato, etc.

El daño principal es sin duda el hecho de que la falta de autenticación constituya un freno a posibles transacciones comerciales. Numerosos estudios señalan que las preocupaciones en materia de seguridad constituyen una de las principales razones para no llevar a cabo transacciones por Internet. Si la gente pudiera confiar plenamente en que su interlocutor es quien afirma ser, el nivel de confianza en las transacciones de Internet aumentaría sensiblemente.

3.6 SEGURIDADES EN REDES INALÁMBRICAS

Hay diversos medios para proteger una red Red Inalámbrica, WI-FI, etc., los más comunes son:

3.6.1 FILTRADO MAC

El punto de acceso (AP) sólo permite la entrada a la red de los equipos con la MAC especificada. La MAC es una manera de identificación única de tarjetas de red, ya sean WI-FI o no. Notaremos que esto está habilitado porque al intentar conectar a la red no podremos, a pesar de ser la señal buena. Se soluciona observando en Kismet un cliente legítimo de esa red y cambiando nuestra MAC por esa.

3.6.2 DHCP DESHABILITADO

El AP no nos asigna las IPs. Nos permite conectar pero al cabo de un rato nos pone "Conectividad limitada o nula".

3.6.3 ESSID OCULTO

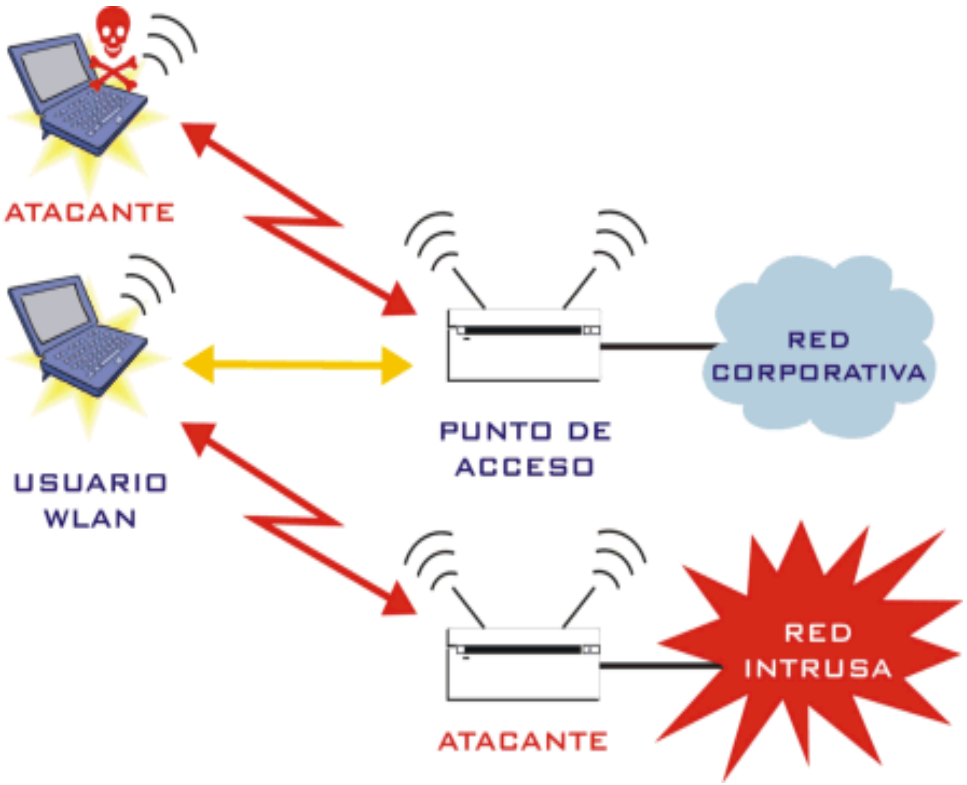
Son redes ocultas, que sólo se ven con determinados programas, como puede ser el Kismet.Clave WPA. Muy difíciles de descifrar, por suerte hay pocas. La solución a la protección WPA está en el manual de Hwagm Clave WEP

Las más comunes. Se basan en el cifrado WEP (Wireless Equivalent Privacy). Son

relativamente vulnerables. Además, estos medios de encriptación a veces se pueden complementar entre ellos, por ejemplo una red con WEP, filtrado MAC y DHCP deshabilitado, u otra con WPA y filtrado MAC. Lo que nunca os vais a poder encontrar va a ser una red con WPA y WEP al mismo tiempo.

Con la proliferación del uso de portátiles y PDAs con capacidades inalámbricas Wi-Fi, cada vez es mayor la demanda de conexiones a wireless access points. Las redes wireless se difunden con rapidez, a medida que el IEEE va aprobando nuevos estándares Wi-Fi como el 802.11i, 802.11e y 802.11n.

La gran comodidad y ventajas que suponen estas nuevas opciones de conexión inalámbricas han hecho que muchísimos usuarios no se hayan percatado de los peligros a que están expuestas las redes Wi-Fi (al no haber ya una conexión física) si no adoptan las medidas de seguridad aconsejadas por los expertos.



Como se observa en el gráfico, existen diversas maneras de poner a prueba la seguridad Wi-Fi de una red inalámbrica.

3.6.4 UNA ALTERNATIVA DE SEGURIDAD

Consiste en que el intruso intente conectarse a un access point de la red inalámbrica para luego ganar acceso a la red corporativa, la otra alternativa consiste en "implantar" un access point "pirata" para atraer a los usuarios desprevenidos o muy curiosos a una red de hackers o red pirata.

Es preciso comprender que en las redes wireless la información se transmite por medio de ondas de radio frecuencia y, esta, está en el aire y es imposible impedir que sea observada y/o capturada por cualquiera que se encuentre en un radio aproximado de 100 metros. Enumeran los principales peligros que debemos mitigar para mejorar la seguridad Wi-Fi. Cualquier otro usuario en un radio aproximado de 100 metros puede ser un "intruso potencial", bien con intención o sin ella.

Como administradores de una red, ¿quién nos asegura que cada uno que intente conectarse a la misma es "de los nuestros". Debemos asegurarnos que, una vez establecida la conexión, esta sea SEGURA, o lo que es lo mismo, ENCRIPTADA.

En las redes inalámbricas WI-FI existen 2 tramos por los que viajan los paquetes que llevan la información:

- Un tramo es inalámbrico (aéreo): es el que va desde cada equipo Wi-Fi hasta el access point.

- Otro tramo es cableado: es el que va desde el access point hasta el servidor de la organización.

Al no poder impedir de ninguna manera que la información que está en el aire sea vista por cualquiera, esta debe ser protegida por medio de protocolos de encriptación. En la actualidad se utilizan WEP, WPA y WPA2. Pero la encriptación es una protección necesaria, muy necesaria, pero no suficiente pues no sirve para impedir accesos no deseados a nuestra red corporativa.

CAPITULO IV

ESTRUCTURA DE LA PROPUESTA

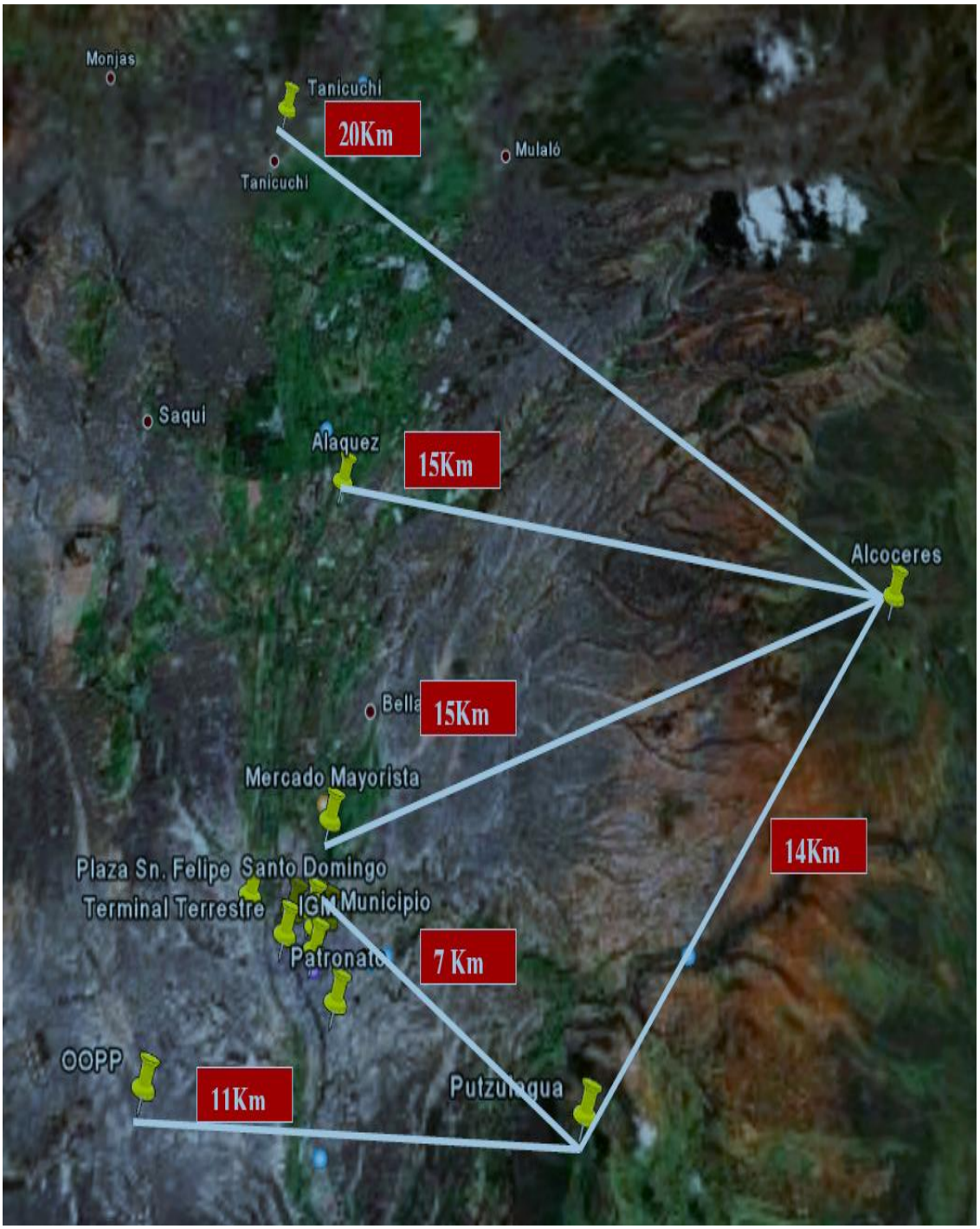
4 PROPUESTA TECNOLOGICA DE LA RED INALÁMBRICA

4.1 OBJETIVO:

Enlazar mediante una Red Inalámbrica Segura las siguientes instalaciones del Municipio de Latacunga:

- Municipio de Latacunga, Oficinas Administrativas de la Alcaldía, Palacio Municipal
- Santo Domingo CAPTUR (Cámara Provincial de Turismo)
- Casa de los Marqueses (Casa de la Cultura)
- Calvario (Antenas Principales)
- Patronato Municipal de Amparo Social (Quirófanos y Salas de Recuperación e Hidratación)
- Centro de cobros Sur (junto a los SSHH Barrio Sur) Calle
- OPAP (Bodegas del Municipio, Obras Publicas y Agua Potable)
- Terminal Terrestre
- Plaza San Felipe
- Mercado Mayorista
- Mercado Cerrado
- Instituto Geográfico Militar (SAN AGUSTIN)
- Centro de Cobros Puente Alaquez

- Centro de Cobros Lasso - Tanicuchi
- Loma de Alcoceres (Backup de información municipal)
- Cerro de Putzalagua (Enlace para las bodegas del Municipio OPP) 20Km



Vista de la propuesta

4.2 MEDIDAS DE SEGURIDAD DE LA RED INALÁMBRICA

Para que un intruso se pueda meter un nuestra red inalámbrica tiene que ser nodo o usuario, pero el peligro radica en poder escuchar la transmisión. De información y saber la forma como nos estamos comunicando. Por esta razón es necesario tener en cuenta algunos criterios que se detallan a continuación:

- Cambiar las claves por defecto cuando instalemos el software del Punto De Acceso.
- Control de acceso seguro con autentificación bidireccional.
- Control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.
- Configuración WEP (muy importante), la seguridad del cifrado de paquetes que se transmiten es fundamental en la redes inalámbricas, la codificación puede ser mas o menos segura dependiendo del tamaño de la clave creada y su nivel , la mas recomendable es de 128 Bits.
- Crear varias claves WEP, para el punto de acceso y los clientes y que varíen cada día.
- Utilizar opciones no compatibles, si nuestra red es de una misma marca podemos escoger esta opción para tener un punto mas de seguridad, esto hará que nuestro posible intruso tenga que trabajar con un modelo compatible al nuestro.
- Radio de transmisión o extensión de cobertura, este punto no es muy común en todos los modelos, resulta más caro, pero si se puede controlar el radio de transmisión al círculo de nuestra red podemos conseguir un nivel de seguridad muy alto y bastante útil.
- Todos estos puntos se debe tomar en cuenta ya que las redes inalámbricas están en plena expansión y se pueden añadir ideas nuevas sobre una mejora sobre su seguridad.

4.2.1 ALCANCE DEL PROYECTO

En base a los requerimientos descritos por el Departamento de Sistemas del Ilustre Municipio de Latacunga, se describieron los siguientes requerimientos:

- Enlazar las varias oficinas del municipio en una red inalámbrica segura para poder tener un control centralizado de toda la facturación del municipio.
- Tener un ancho de banda mínimo para que los clientes puedan enviar correos electrónicos y que exista sincronización del sistema de facturación
- Tener un ancho de banda mínimo para compartir el acceso a Internet entre los diferentes edificios del municipio con el backbone del municipio ubicado en las oficinas de la Alcaldía de Latacunga.

4.3 MÉTODOS Y TECNOLOGÍA A UTILIZARSE

Se utilizaría una combinación de la tecnología inalámbrica de equipos de conexión punto-punto y punto-multipunto.

4.4 ESTUDIO PRELIMINAR

En base al estudio realizado el día Miércoles 21 de Noviembre del 2008, se pudo realizar una inspección de las diferentes oficinas, así como su respectiva línea de vista entre cada una de ellas.

Después de realizado el estudio se determinaron las siguientes conclusiones que son las más aconsejables para tener un rendimiento óptimo.:

Se recomienda instalar una torre de 12 metros de altura en el sector de “El Calvario”, para cubrir y enlazar las siguientes oficinas:

- Palacio Municipal de Latacunga (Punto – Punto con el Calvario)
- Santo Domingo CAPTUR (Cámara Provincial de Turismo)
- Casa de los Marqueses (Casa de la Cultura)
- Patronato (Quirófanos y Salas de Recuperación e Hidratación)
- Centro de cobros Sur (junto a los SSHH Barrio Sur)
- Mercado Cerrado
- Instituto Geográfico Militar (SAN AGUSTIN)

Para tener una línea de vista sin obstáculos a la torre que se instalaría en el Calvario, se recomienda instalar los siguientes tramos de torre con su respectiva altura en los siguientes edificios:

Ord.	**Dpto. Municipal**	**Tramo de torre Requerido Si/No**	**Altura del tramo**
1	Palacio Municipal	Si	3 m
2	Santo Domingo	No	-
3	Casa de los Marqueses	No	-
4	Patronato	Si	3m
5	Centro de cobros sur	Si	9 m
6	Mercado cerrado	Si	12 m
	Instituto Geográfico Militar (Ltga)	No	-

Se recomienda instalar una repetidora en el cerro de Putzalagua para poder cubrir las siguientes oficinas:

- OPAP (Bodegas del Municipio, Obras Públicas y Agua Potable)
- Plaza San Felipe
- Terminal Terrestre.

Se recomienda instalar una repetidora en la Loma de Alcoceres para poder cubrir las siguientes oficinas:

- Mercado Mayorista
- Centro de Cobros Lasso - Tanicuchi
- Centro de Cobros Puente Alaquez
- Calvario - Municipio (Punto – Punto)

4.5 PROPUESTA

Se recomienda dividir el proyecto en tres partes:

4.5.1 Primera etapa

4.5.1.1 Primer día

- Traslado a Latacunga y entrega de todo el material necesario para la primera parte (Bodegas del Municipio)
- Separación y clasificación de los materiales para los diferentes días de trabajo
- Planificación de las instalaciones con el Departamento de Sistemas del I.M.L.

4.5.1.2 Segundo día

- Instalación de la torre de 12m en el Calvario: AM
- Instalación de antenas sectoriales y radios en el Calvario: PM
- Instalación del Software de Administración de Redes en el Dpto. de Sistemas del I.M.L.

4.5.1.3 Tercer día

- Instalación de la torre de 3m en el Palacio Municipal: AM
- Instalación de antenas y radios en el Palacio Municipal: AM
- Pruebas de enlace Calvario – Palacio Municipal: AM
- Instalación de antenas y radios en Santo Domingo: PM
- Pruebas de enlace Santo Domingo – Calvario – Palacio Municipal: PM

4.5.1.4 Cuarto día

- Instalación de antenas y radios en Casa de los Marqueses: AM
- Pruebas de enlace Casa de los Marqueses – Calvario – Palacio Municipal: AM
- Instalación de la torre de 3m en el Patronato: PM
- Instalación de antenas y radios en el Patronato: PM
- Pruebas de enlace Patronato – Calvario – Palacio Municipal: PM

4.5.1.5 Quinto día

- Instalación de la torre de 9m en el Centro de Cobros Sur (CCS): AM

- Instalación de antenas y radios en el Centro de Cobros Sur: AM
- Pruebas de enlace CCS – Calvario – Palacio Municipal: AM
- Instalación de antenas y radios en el San Agustín: PM
- Pruebas de enlace San Agustín – Calvario – Palacio Municipal: AM

4.5.1.6 Sexto día

- Instalación de la torre de 12m en el Mercado Cerrado: AM
- Instalación de antenas y radios en el Mercado Cerrado: PM
- Pruebas de enlace Mercado Cerrado – Calvario – Palacio Municipal: PM

4.5.2 Segunda Etapa

4.5.2.1 Primer día

- Traslado a Latacunga y entrega de todo el material necesario para la segunda parte (Bodegas del Municipio)
- Separación y clasificación de los materiales para los diferentes días de trabajo
- Planificación de las instalaciones con el Departamento de Sistemas del I.M.L.

4.5.2.2 Segundo día

- Instalación de antenas en la Estación Putzalagua. (Se asume que no es necesario instalar una torre en esta estación y que ya existen una torre del municipio donde instalar los equipos): AM
- Instalación de antenas y radios en el Palacio Municipal: AM
- Pruebas de enlace Putzalagua – Palacio Municipal: AM

- Instalación de un tramo de torre de 3m. en la terraza del OPAP: PM
- Instalación de antenas y radios en el OPAP: PM
- Pruebas de enlace OPAP – Putzalagua – Palacio Municipal: PM

4.5.2.3 Tercer día

- Instalación de un tramo de torre de 3m. en la terraza del Terminal Terrestre (TT): AM
- Instalación de antenas y radios en el Terminal Terrestre: AM
- Pruebas de enlace TT – Putzalagua – Palacio del Municipio: AM
- Instalación de un tramo de torre de 9m. en la Plaza San Felipe (PF): PM
- Instalación de antenas y radios en la Plaza San Felipe: PM
- Pruebas de enlace Plaza San Felipe – Putzalagua – Palacio del Municipio: PM

4.5.3 Tercera etapa

4.5.3.1 Primer día

- Traslado a Latacunga y entrega de todo el material necesario para la tercera parte (Bodegas del
- Municipio)
- Separación y clasificación de los materiales para los diferentes días de trabajo
- Planificación de las instalaciones con el Departamento de Sistemas del Municipio de Latacunga

4.5.3.2 Segundo día

- Instalación de antenas en la Loma de Alcoceres. (Se asume que no es necesario instalar una torre en esta estación y que existe una torre del Municipio donde instalar los equipos): AM
- Instalación de antenas en el Calvario para enlazar a la loma de Alcoceres: PM
- Pruebas de enlace Alcoceres – Calvario – Palacio Municipal: PM

4.5.3.3 Tercer día

- Instalación del tramo de torre de 3m. en la terraza del Mercado Mayorista (MM): AM
- Instalación de antenas y radios en la terraza del Mercado Mayorista: AM
- Pruebas de enlace MM – Alcoceres – Calvario – Palacio Municipal: PM

4.5.3.4 Cuarto día

- Instalación del tramo de torre de 12m. en el Centro de Cobros Lasso - Tanicuchi: AM
- Instalación de antenas y radios en el Centro de Cobros Lasso - Tanicuchi: PM
- Pruebas de enlace Tanicuchi – Alcoceres – Calvario – Palacio Municipal: PM

4.5.3.5 Quinto día

- Instalación de un tramo de torre de 12m. en el Centro de Cobros Puente Alaquez: AM
- Instalación de antenas y radios en el Centro de Cobros Puente Alaquez: PM
- Pruebas de enlace Alaquez – Alcoceres – Calvario – Palacio Municipal: PM

4.5.4 REQUERIMIENTOS

4.5.4.1 REQUERIMIENTOS TÉCNICOS GENERALES

Para poder realizar las respectivas instalaciones, es necesario contar con los siguientes lineamientos:

- Autorización respectiva para instalar los tramos de torre en los correspondientes terrenos o terrazas de edificios
- Contar con la autorización respectiva de los edificios vecinos en caso de que se piense utilizar la infraestructura de los edificios adyacentes: i.e. casa de la cultura, SAN AGUSTIN, Santo Domingo
- Una vez armada y configurada la red armada, se debe declarar estos enlaces con el SUPTEL como una red privada y sin fines de comercialización.

4.5.4.2 REQUERIMIENTOS TÉCNICOS ADMINISTRATIVOS

La administración de la red interna una vez configurada estaría a cargo del personal autorizado del departamento de sistemas del municipio.

Se necesita poder capacitar a un técnico dedicado 100% a la administración y mantenimiento de la red inalámbrica.

Este técnico necesita tener los conocimientos necesarios en la administración de redes y poder solucionar problemas en el campo por si solo.

4.5.5 RESUMEN DE SERVICIOS

La provisión, instalación y configuración de la red inalámbrica del municipio conforme y de acuerdo al cronograma detallado en las diferentes etapas del proyecto. La configuración y puesta en funcionamiento del conjunto compuesto por los equipos, el software licenciado y los servicios que integran la solución de implementación de un enlace inalámbrico en la banda libre Spread Spectrum entre los diferentes edificios del municipio listados en el objetivo de esta propuesta.

La implantación se realizará en conformidad con el cronograma de actividades previsto por el Ilustre Municipio de Latacunga (IML).

La capacitación de los equipos utilizados a las personas designadas por el IML. El IML se compromete a designar y recibir dicha capacitación que consistirá en lo siguiente:

- Configuración y mantenimiento de los radio clientes
- Configuración y mantenimiento de los radio repetidores
- Administración de la seguridad de la red
- Administración del control de acceso y ancho de banda de cada cliente

4.6 MATERIALES NECESARIOS PARA LA IMPLEMENTACION

4.6.1 Primera etapa

CANTIDAD	DESCRIPCION
2	Radio cliente Spread Spectrum de 5.7 GHz (15 Mbps ancho de banda)
1	Radio Access Point 200 mW
2	Antenas sectoriales (90 grados)
2	Spliter frecuencia 5.8 Ghz
6	Radio Clente Spreed Spectrum de 5.8 Ghz (200 mW 54 Mbps ancho de banda)
5	Pig Tails 50 cm (2 extras)
5	Caja térmica (1 extra)
8	UPS AVR Trip-Lite 550 va
1	Rollo de cable UTP Cat-6 (200 mts)
1	Software Administrativo
1	PC Servidor Linux
13	Tramos de torre de 3 mts galvanizados
13	Materiales de instalación por tramo de torre (3mts.)
5	Conexiones a tierra por torre

4.6.2 Segunda etapa

CANTIDAD	DESCRIPCION
2	Radio cliente Spread Spectrum de 5.8 GHz (15 Mbps ancho de banda)
1	Radio Access Point 200 mW
1	Spliter frecuencia 5.8 Ghz
1	Antena sectorial (90 grados)
3	Radio Clente Spreed Spectrum de 5.8 Ghz (200 mW 54 Mbps ancho de banda)
2	Pig Tails 50 cm (1 extras)
2	Caja térmica
4	UPS AVR Trip-Lite 550 va
1	Rollo de cable UTP Cat-6 (100 mts)
5	Tramos de torre de 3 mts galvanizados
5	Materiales de instalación por tramo de torre (3mts.)
3	Conexiones a tierra por torre

4.6.3 Tercera etapa

CANTIDAD	DESCRIPCION
2	Radio cliente Spread Spectrum de 5.1 – 5.8 GHz (15 Mbps ancho de banda)
1	Radio Access Point 200 mW
2	Antena sectorial (90 grados)
2	Spliter frecuencia 5.8 Ghz
3	Radio Clente Spreed Spectrum de 5.8 Ghz (200 mW 54 Mbps ancho de banda)
4	UPS AVR Trip-Lite 550 va
1	Rollo de cable UTP Cat-6 (200 mts)
9	Tramos de torre de 3 mts galvanizados
9	Materiales de instalación por tramo de torre (3mts.)
3	Conexiones a tierra por torre

4.7 TIEMPO DE RESPUESTA Y DISPONIBILIDAD DE LA RED INALÁMBRICA

Para el tiempo de resolución de contingencias o incidencias, contando a partir del momento de recibir la notificación o desde que se acepta a trámite la incidencia hasta que se envía la notificación de que ésta ha sido resuelta.

La incidencia quedara resuelta y cerrada una vez que el usuario/a comprueba que funciona correctamente la conexión a la red Inalámbrica.

Se establece un tiempo máximo de resolución de incidencias de 24 horas para la resolución de estas contingencias ordinarias, considerándose como tales a aquellas que ameritan configuración y soluciones rápidas, pero las incidencias extraordinarias como cambio de equipo, etc, se estima un máximo de 72 horas.-

4.7.1 DISPONIBILIDAD DE LA RED INALAMBRICA

Disponibilidad del enlace 99.6% real al mes en el Backbone del municipio, excepto cuando los enlaces se caigan por fuerza mayor: falta de luz, caída de un rayo, nuevos obstáculos en la línea de vista, robo de equipos, des-alineamiento de las antenas, etc.

4.7.2 CONDICIONES DE SERVICIO DE LA RED INALÁMBRICA

Este servicio tiene como objetivo dotar de apoyo a los usuarios para la configuración del PC ó portátil para la conexión de forma automática y segura, autenticada y cifrada en el momento en que se establezca la conexión con la red

4.7.3 TIEMPOS DE RESPUESTA GARANTIZADOS

En base a las especificaciones tecnicas de los equipos

- max 10ms al primer router del Backbone del municipio hasta 1Km
- max 50ms al primer router del backbone del municipio hasta 2Km
- max 100ms al primer router del backbone del municipio hasta 10Km
- max 200ms al primer router del backbone del municipio hasta 15Km
- max 300ms al primer router del backbone del municipio hasta 20Km

4.8 ANÁLISIS DE FACTIBILIDAD ECONÓMICA, PRESUPUESTO Y FUENTES DE FINANCIAMIENTO

4.8.1 PROPUESTA ECONÓMICA

Si Cuando se desea enlazar distancias superiores a 5 kmts con enlaces WI-FI o WIMAX, los equipos Motorola permiten mayor rendimiento en transmisión y seguridades pero su costo es muy elevado, existen otros equipos como Alvarium, que en distancias menores a 5 kmts se comportan en forma similar a Motorola y su costo es inferior en un 25% menos.

En cambio con distancias superiores a 5 kmts decae su transmisión y no soporta muchos ruidos existentes en el ambiente como son lluvias, días nublados, frecuencias de radio que se cruzan, etc que con equipos alvarion se demoran más en separar estos ruidos.

Los equipos Canopy son para distancias más extensas mayores a 100 Kmts, su conexión es con rebote satelital, su costo también es elevado cada equipo bordea los 50.000 USD, utilizada la ultrafrecuencia y su señal es nitida, en cambio motorola separa estos mismos ruidos en forma más rápida, pero su costo es más elevado que equipos Alvarion.

los equipos Dlink son para uso con distancias menores a 1.0000 mts, su costo es mínimo, los equipos 3com son también utilizados para intranets de distancias menores a 200 mts.

Por estas razones y por ajustarnos al presupuesto del I. municipio de Latacunga para la presente propuesta que no supera los 35.000 dólares, estimo conveniente trabajar con equipos Alvarium y dispositivos compatibles, que por su costo y beneficio se ajustan al presupuesto institucional.

Los costos de los equipos propuestos, están dentro de lo presupuestado, solicitado y al alcance del presupuesto del I. Municipio de Latacunga y se lo realizará en tres etapas de acuerdo a la disponibilidad económica, de la siguiente manera:

Primera etapa	15.657,60
Segunda etapa	8.232,00
Tercera etapa	9.906,40
Total del costo del proyecto	32.796,00

Lo financiará el I. Municipio de Latacunga.

4.9 CONCLUSIONES Y RECOMENDACIONES

4.9.1 CONCLUSIONES

- Debido a la constante innovación tecnológica, las instituciones se sienten obligadas a mantener un dinamismo en el manejo de las seguridades con la informática, por lo que es preciso frecuentemente cambiar las claves y permisos de los usuarios especialmente cuando se trabaja en el área de redes y enlaces inalámbricos.

- La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de estas situaciones.

- La ocurrencia de delitos informáticos en las organizaciones alrededor del mundo no debe en ningún momento impedir que éstas se beneficien de todo lo que proveen las tecnologías de información (comunicación remota, Ínter conectividad, comercio electrónico, etc.); sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

- Las redes basadas en claves WEP son seguras, pero existe software que sin tener experiencia en Linux se pueden romper las seguridades WAP, WEP. Por lo que es necesario configurar las seguridades con mac address.

- Es necesario colocar varias antenas para tener una conectividad multipunto con alto rendimiento, es decir el primer enlace que logra conectarse va a ser el punto de conectividad e instalarlos en sitios estratégicos como son loma de alcoceres, el calvario y putzalagua, para tener mayor cobertura, para cubrir

sitios como pastocalle, tanicuchi y lasso. Y colocar en estos sitios puntos de cobro de impuestos municipales.

- Con la implementación de los mencionados enlaces inalámbricos las dependencias municipales lograrán estar siempre conectadas a la misma red, tendrán la información requerida al instante, se logrará satisfacer las necesidades y requerimientos en forma instantánea es decir on-line.

4.9.2 RECOMENDACIONES

- Por lo expuesto anteriormente se recomienda que se implemente el presente proyecto de manera inmediata, ya que sus dependencias quedarán integradas.

- De ser posible adquirir equipos Alvarium ya que para la transmisión de información lo hacen de manera clara oportuna y la filtración de ruidos lo hacen con mayor solvencia y rapidez.

- Utilizar la conexión inalámbrica con sus respectivas seguridades integrará todas las dependencias municipales vía aérea sin necesidad de cables a través de wireless de alta fidelidad.

4.10 CRONOGRAMA DE ACTIVIDADES

6.5. BIBLIOGRAFÍA

http://www.red2000.com.mx

http://www.syscom.com.mx

http://www.solunet.com.ar

http://www.weblinknet.com

http://www.compucentro.net.mx/inalambricos.htm

http://www.weblinknet.com/servicios/empresa/empresa.htm

http://www.fi.uba.ar/materias/6629/wi.pdf

http://www.solunet.com.ar/conexiones-internet/enlaces-inalambricos

http://www.jocoya.cl/enlace-inalambrico.htm

http://www.enlacesinalambricos.net/

http://www.madrimasd.org/RedTelematicaMadrid/default.asp

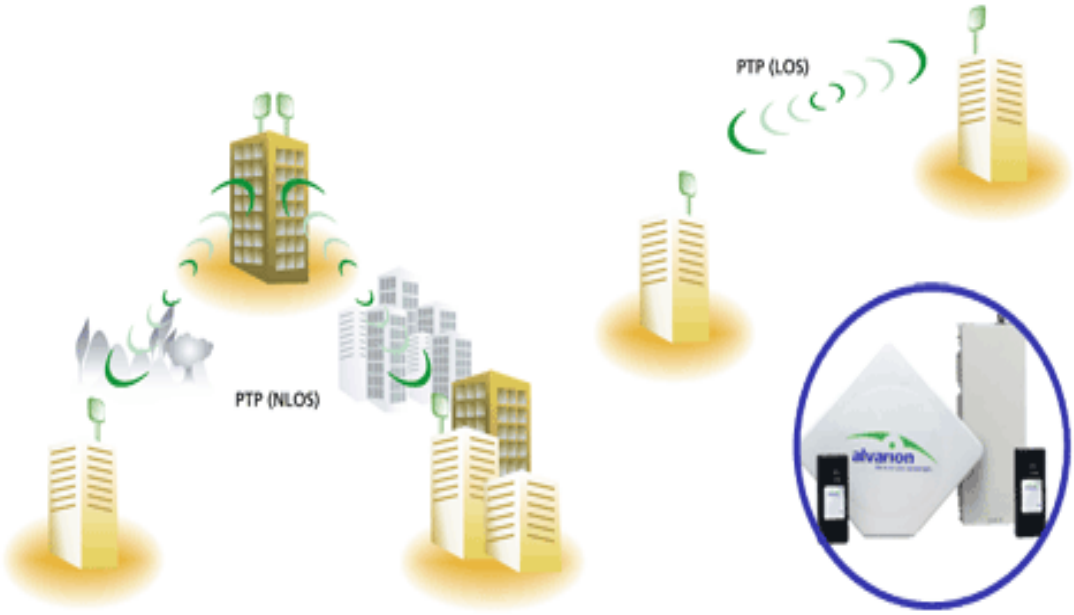
http://rediris.es

http://www.rediris.es/red/

http://www.dante.net/geant

Empresas:

- Gigowireless,
- D.I.T.,
- Telecom System.


PTP (LOS)
PTP (NLOS)
alvarion

Anexo A:

Antena de Bajo Perfil:

Specifications

Electrical Specifications

Frequency	2400-2500 MHz
Gain	14 dBi
Horizontal Beam Width	30 degrees
Vertical Beam Width	30 degrees
Impedance	50 Ohm
Max. Input Power	25 Watts
VSWR	< 1.5:1 avg.
Lightning Protection	DC Short

Mechanical Specifications

Output Connector	"N" type Female
Mounting	1-1/4" (32 mm) to 2" (51 mm) dia. Masts
Vertical Tilt	0-60°
Weight	.95 lbs. (.43 Kg)
Dimensions	8.5 x 8.5 x 1 (inches) 216 x 216 x 26 (mm)
Radome Material	UV-inhibited Polymer
Flame Rating	UL 94HB
Polarization	Horizontal or Vertical
Operating Temperature	-40° C to to 85° C (-40° F to 185° F)
RoHS Compliant	Yes
Wind Survival	>150 MPH (241 KPH)

Anexo B:

Caja Térmica NEMA

110 VAC Weatherproof 18"x16"x8" Enclosures for Wireless LAN Equipment

Features

- Molded fiberglass reinforced polyester enclosure
- Large size is ideal for applications requiring more then one radio
- Stainless steel quick release latches with padlock hasps
- Fully gasketed lid
- Integral mounting flange
- NEMA Type 4X / IP65 rated* (NB181608-100/1H0)
- NEMA Type 3R / IP42 rated (NB181608-10F/1HF/10V)
- RoHS Compliant
- Features aluminum mounting plate
- Thermostat-controlled heating or cooling models
- Vented version available
- Optional solid state dual set point temperature controller available
- 110 VAC Outlets
- Mounting plate can accommodate WLAN equipment from Cisco®, Symbol®, D-Link®, HyperLink and more..
- Optional universal equipment shelf and mounting brackets available
- Fully customized configurations available

Anexo C:

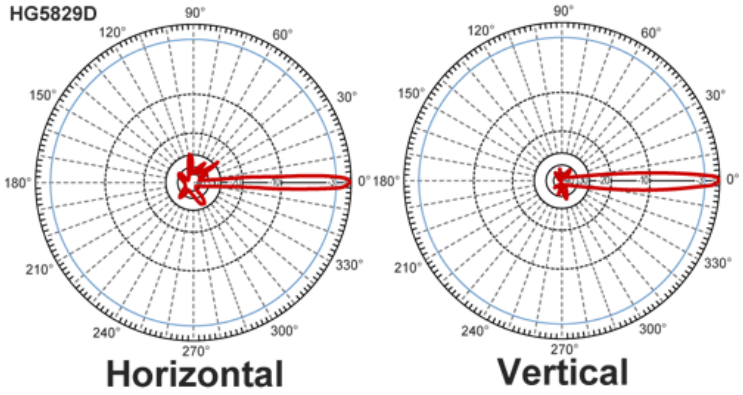
Torre de Bajo Perfil:

Características Técnicas:

Dimensiones: 50 cm. x lado (3 lados)
Tamaño: 3 m. altura
Peso: 90 lbs.

Anexo D:

Antena Parabólica:



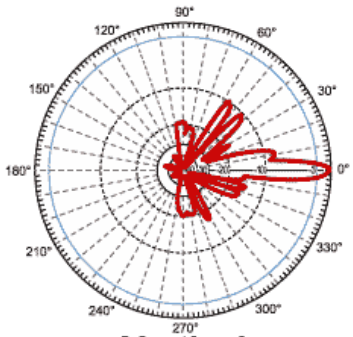
Model	HG5829D
Frequency	5725-5850 MHz
Gain	29 dBi
Polarization	Horizontal or Vertical
Horizontal Beam Width	6°
Vertical Beam Width	6°
Front to Back Ratio	35 dB
Impedance	50 Ohm
Max. Input Power	100 Watts
VSWR	< 1.5:1 avg.
Weight	13.2 lbs. (6 kg)
Diameter	23.6 in. (600 mm)
Mounting	1.5" (38mm) to 3" (76mm) dia. masts
Operating Temperature	-40° C to to 85° C (-40° F to 185° F)
Lighting Protection	DC Short
Connector	N-Female
RoHS Compliant	Yes
Radome Cover Part Number	HGR-06

Wind Loading Data

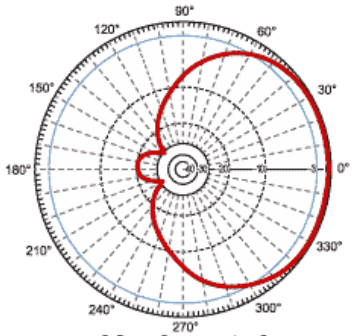
Model: HG5829D		
Wind Speed (MPH)	**Loading**	**With Radome**
100	113 lb.	75 lb.
125	177 lb.	116 lb.

Anexo E:

Antena Sectorial:



Vertical



Horizontal

Mechanical Specifications

Weight	10 lbs. (4.54 Kg)
Dimensions	39 x 6 x 2.5 inches (99 x 15.3 x 6.4 cm)
Radome Material	UV-Inhibited Polymer
Operating Temperature	-40° C to to 85° C (-40° F to 185° F)
Mounting	2 inch (5 cm) O.D. pipe max.

Polarization	Vertical
Downtilt (mech)	0 to 20 degrees (adjustable)
RoHS Compliant	Yes

Wind Loading Data

Wind Loading	Front Surface	Side Surface
Area	1.63 sq. ft. (.15 sq. meters)	0.68 (.06 sq. meters)
@ 100 MPH (161 KPH)	74 lbs. (33.5 Kg)	35 lbs.(15.8 Kg)