INSTITUTO POLITECNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA
MECANICA Y ELECTRICA

"PROYECTO DE INSTALACIÓN DE RED INALÁMBRICA
DE CFE EN EL ÁREA METROPLOLITANA"

TESIS

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMUNICACIONES Y ELÉCTRONICA

PRESENTA:

ELIZABETH ESPINOSA ELIZALDE

ASESORES:

ING. PEDRO GUSTAVO MAGAÑA DEL RIO
ING. GERARDO CARDENAS GONZÁLEZ

MEXICO, D.F. 2008

INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELECTRICA

UNIDAD PROFESIONAL "ADOLFO LÓPEZ MATEOS"

TEMA DE TESIS

QUE PARA OBTENER EL TITULO DE	**INGENIERO EN COMUNICACIONES Y ELECTRÓNICA**
POR LA OPCIÓN DE TITULACIÓN	**TESIS Y EXAMEN ORAL INDIVIDUAL**
DEBERA(N) DESARROLLAR	**C. ELIZABETH ESPINOSA ELIZALDE**

"PROYECTO DE INSTALACIÓN DE RED INALÁMBRICA DE CFE EN ÁREA METROPOLITANA"

CON LA FINALIDAD DE TENER UN MEJOR SERVICIO Y MAYOR CALIDAD EN CUANTO TECNOLOGÍA SE REFIERE, COMISIÓN FEDERAL DE ELECTRICIDAD TIENE EN MENTE LA APLICACIÓN DE UNA RED INALÁMBRICA LA CUAL DARÁ SERVICIOS A DIFERENTES PUNTOS DE LA EMPRESA.
ESTO ES CON EL FIN DE TENER RESULTADOS EFICIENTES Y SEGUROS DENTRO Y FUERA DE LA EMPRESA.
ES IMPORTANTE UNA EMPRESA DE CLASE MUNDIAL SE ENCUENTRE A LA VANGUARDIA EN CUANTO A SEGURIDAD SE REFIERE Y ESTO IMPLICA INSTALAR UN PROYECTO QYE DE LOS RESULTADOS ESPERADOS POR EL CLIENTE, PUESTO QUE LAS NECESIDADES SON MUCHAS Y DEBEN CUBRIRSE.

- INTRODUCCIÓN
- ANTECEDENTES
- ALTERNATIVAS DE SOLUCIÓN
- MARCO TEÓRICO
- PROPUESTA
- RESULTADOS
- CONCLUSIONES
- ANEXOS
- GLOSARIO
- BIBLIOGRAFÍA

MÉXICO D.F. A 29 DE AGOSTO DE 2008

A S E S O R E S

ING. PEDRO GUSTAVO MAGAÑA DEL RIO

ING. GERARDO CARDENAS GONZÁLEZ

M. EN C. SALVADOR RICARDO MENESES GONZÁLEZ
JEFE DEL DEPARTAMENTO ACADÉMICO DE

OBJETIVO GENERAL

Con la finalidad de tener un mejor servicio y mayor calidad en cuanto tecnología se refiere, Comisión Federal de Electricidad tiene en mente la aplicación de una red inalámbrica la cual dará servicios a diferentes puntos de la empresa.

Esto es con el fin de tener resultados eficientes y seguros dentro y fuera de la empresa.

Es importante que una empresa de clase mundial se encuentre a la vanguardia en cuanto a seguridad se refiere y esto implica instalar un proyecto que de los resultados esperados por el cliente, puesto que las necesidades son muchas y deben de cubrirse.

DEDICATORIA Y AGRADECIMIENTOS

Primero quiero darle Gracias a
Dios por darme esta vida tan
Maravillosa, por darme la familia
Más hermosa del mundo.
Por darme la paciencia y la inteligencia
De llegar hasta donde hoy me encuentro

Quiero agradecerme a mi por
Todas las cosas buenas que eh
Obtenido a base de mucho esfuerzo y
Por lograr realizar este gran proyecto.

Quiero dedicar y agradecer esta tesis a mis
Papas puesto que siempre me han apoyado y con
Su infinito amor me ha guiado por un muy buen
Camino, gracias por todos los momentos tan lindos
Que hemos pasado juntos, por sus enseñanzas y
Por creer siempre en mí.
Los amo con todo mi corazón.

A mis hermanos que son mis mejores
Amigos cómplices de tantas travesuras
Y aventuras diarias, por darme la fortaleza
Y la capacidad de confiar en alguien como
Los son ustedes.

A mis amigos que siempre me han apoyado
Y aguantado tantas cosas, por enseñarme
A quererlos como mis hermanos, por el
Espíritu de guerreros que siempre muestran
Para poder pelear contra todos.
Por sus sonrisas y momentos felices
Que vivimos juntos y que hoy nos
Hacen vernos más fuertes.

A mis profesores por compartirme lo más valioso
Que poseen su conocimiento, y hacerme ver que ser Ingeniero
No es cuestión de sexos si no de valentía, coraje, respeto
y ardua dedicación para ser mejores día a día

A Comisión Federal de Electricidad
Por brindarme la oportunidad de participar
En los proyectos, por todos los buenos momentos
que pase, y mejor aún por permitirme aprender
más del campo de las comunicaciones.

A los Ingenieros de CFE que siempre me han apoyado
Y que me han adoptado como un miembro más del equipo
Trabajo, por todo el conocimiento que me infundieron
Por todos los lindos momentos que pase con ellos
Por las amistades que pude cosechar y por
Enseñarme que siempre hay que luchar
Para ser mejores

Proyecto de Instalación de Red Inalámbrica de CFE en el Área Metropolitana.

INDICE

CAPITULO QUINTO

INTRODUCCIÓN

INTRODUCCIÓN.

Actualmente la tendencia del mercado informático y de las comunicaciones se orienta en un claro sentido: unificación de recursos. Cada vez, ambos campos, comunicaciones e informática, se encuentran más vinculados. Este aspecto es una de las principales variables que determinan la necesidad por parte de las empresas, de contar con proveedores especializados en instalaciones complejas, capaces de determinar el tipo de topología más conveniente para cada caso, y los vínculos más eficientes en cada situación particular. Todo ello, implica mucho más que el tendido de cables.

Se llama comunicación inalámbrica a aquélla que se lleva a cabo sin el uso de cables de interconexión entre los participantes; por ejemplo, una comunicación; con teléfono móvil es inalámbrica, mientras que una comunicación en un teléfono fijo no lo es.

No cabe duda que la tecnología inalámbrica está ocupando rápidamente las preferencias de todo tipo de usuarios. La telefonía móvil está cada vez más cerca de convertirse en un sistema de comunicación personal universal en el mundo occidental, como en otras partes del mundo, ese es un pequeño ejemplo del impacto que están dejando las comunicaciones inalámbricas.

Del mismo modo la tecnología esta en las comunicaciones inalámbricas está dentro de las redes que dan servicio desde simples hogares domésticos, hasta grandes empresas e industrias. Así como los avances en diferentes ámbitos de la vida de igual manera la tecnología da cada vez da pasos agigantados y firmes para dar un mejor servicio y mayor calidad en la transmisión y recepción de datos.

Una características de los dispositivos inalámbricos es que tienen es que son susceptibles de poder comunicarse entre sí y, aunque también pueden

comunicarse por medio de cables, estos alcanzan su mayor potencial a través de las comunicaciones inalámbricas.

En este trabajo se muestra la instalación de una red inalámbrica en Comisión Federal de Electricidad.

En el capitulo I, a grandes rasgos se describen las alternativas de solución que se tomaron para poder decidir que tecnología se utilizara en el proyecto, por medio de un estudio realizado.

En el capitulo II, se muestra la descripción general de la tecnología Wi-Fi, y los protocolos con los cuales se maneja.

En el capitulo III, se trata de la propuesta, para el desarrollo del proyecto desde su implantación hasta su termino.

En el capitulo IV, es el de resultados, en el cual se da la información de como están trabajando los equipos y la respuesta de los usuarios con dicha tecnología.

En el capitulo V, es el de conclusiones donde se da el punto terminal del trabajo, así como las experiencias vividas en el.

ANTECEDENTES

ANTECEDENTES

Surge la necesidad de instalar un proyecto nuevo en Comisión Federal de Electricidad el cual consiste en implantar una nueva tecnología en con junto con lo que ya se tenía como estructura base. No se trata de que se eliminen los elementos con los que se contaban y trabajaban. Más bien consiste en incrementar y mejorar el servicio.

De esta forma se trata de que haya mejor resultados y el cliente esté satisfecho con el resultado de la solicitud.

Dentro de la empresa Comisión Federal de Electricidad existe una red estructurada, la cual da servicio a todos los usuarios de dicha empresa, ya sean trabajadores de CFE u otro personal como son invitados, proveedores y personal externo, dicho personal tiene la necesidad de utilizar un punto de acceso a la red.

Es importante mencionar que, dentro de la empresa Comisión Federal de Electricidad, la red interna esta diseñada para soportar los servicios requeridos por el personal, lo que implica que en cada piso de cada edificio exista un cuarto de comunicaciones donde se encuentra el equipo que soporta dichos servicios.

Dentro de los cuartos de comunicaciones se pueden observar los equipos con que se cuenta, y los cuales no permitían identificar punto de red de los usuarios.

Se requiere de un servicio que proporcione la solución al problema de proveer comunicación en diferentes salas u oficinas por medio de una red, pero no deben de existir el tendido de cableado por fuera, y por norma no puede haber determinada cantidad de puntos de acceso en un solo lugar; por ejemplo en un auditorio donde se presenta una conferencia y se requiera que las personas en el sitio se conecten a la red, no existirán 200 puertos físicos para conectarse simultáneamente. Este tipo de problemática se presenta y por esa razón se requiere una solución que cubra las necesidades presentadas, así como garantía

de seguridad tanto a los equipos como a la información que se maneja internamente.

CAPITULO I

ALTERNATIVAS DE SOLUCIÓN

CAPITULO I

ALTERNATIVAS DE SOLUCIÓN

La tecnología da pasos agigantados en cuanto a comunicaciones se refiere, y más aún si son de la forma inalámbrica, por esa razón se requiere de mayor conocimiento en cuanto a los requerimientos utilizados.

Cada vez más empresas se encuentran preocupadas por estar a la vanguardia en comunicaciones y en Comisión Federal de Electricidad, no es la excepción se este trabajando para alcanzarlo, sin embargo, cada día los cambios a nivel tecnológico son mas grandes y complejos, por esa misma razón, es indiscutible que cada vez todas las pequeñas y grandes empresas y/o establecimientos se preocupen por dar una mayor calidad de servicio y mejor cobertura de comunicaciones.

Cada vez se necesita más precisión y mejoramiento de los servicios que se dan es cada lugar, y al mismo tiempo se puede verificar y comprobar el funcionamiento adecuado de los servicios dados.

1.1 **Tipos de redes de inalámbricas de datos.**

Es claro que las redes inalámbricas es un avance de mucha importancia para la tecnología ya que da paso a nuevas estructuras, nuevas formas de enviar y recibir información, pero lo más importante es que está dando resultados sorprendentes para diferentes formas de comunicación.

Por esta razón se realizo un estudio para tener un conocimiento más amplio acerca de las comunicaciones inalámbricas el cual arrojo como resultado que existen diferentes opciones para instalar una red inalámbrica.

En este entorno, se denota que no es de extrañar que el crecimiento de tecnologías es cada vez mayor el número de soluciones inalámbricas: GSM (Global System for Mobile communications, `Sistema global para las comunicaciones móviles'), UTMS (Universal Mobile Telecommunications System, `Sistema universal para las telecomunicaciones móviles'), Wi-Fi (Wireless Fidelity, 'Fidelidad inalámbrica'), Bluetooth (tecnología inalámbrica que permite intercomunicar equipos a una distancia de varios metros.), Dect (Digital Enhanced Cordless Telecommunications 'Es una tecnología de radio para aplicaciones de voz'), GRPS (General Packet Radio Service, 'Servicio de comunicación vía wireless'), 3G (tercera generación), WiMax (Interoperatividad mundial para accesos de microondas), etc.

La descripción de algunas de ellas que se estudiaron, para la aceptación del proyecto son:

1.1.1 Redes inalámbricas de área personal

Bluetooth

Bluetooth es una de las tecnologías de las redes inalámbricas de área personal más conocidas. Al contrario que otras tecnologías esta no está pensada para soportar redes de computadoras, sino más bien, para comunicar una computadora o cualquier otro dispositivo con sus periféricos: un teléfono móvil con su auricular, una PDA (Personal Digital Assistant, 'Asistente Personal Digital) con su computadora, una computadora con su impresora, etc.

Las comunicaciones Bluetooth se llevan a cabo mediante el modelo maestro/esclavo. Un Terminal maestro puede comunicarse hasta con siete esclavos simultáneamente. No obstante, el maestro siempre puede suspender las comunicaciones con un esclavo (mediante una técnica llamada *parking*) y activar una nueva comunicación con un nuevo dispositivo esclavo. Con este sistema un maestro puede establecer comunicación con un máximo de 256 esclavos, donde sólo siete comunicaciones pueden permanecer activas simultáneamente

Bluetooth utiliza la técnica FHSS (Frequency Hopping Spread Spectrum, `Espectro expandido por salto de Frecuencia`) en la banda de frecuencia de 2.4 GHz. Puede establecer comunicaciones asimétricas, donde la velocidad máxima en una dirección es de 721 Kbps y 57.6 Kbps en la otra, o asimétrica de 432.6 Kbps en ambas direcciones.

ZigBee

La aportación fundamental de esta nueva tecnología es que está pensada específicamente para aplicaciones domóticas, donde se ha considerado más importante el bajo costo de los dispositivos y bajo consumo de energía antes que la velocidad de transmisión. Esta velocidad esta comprendida entre los 20 y 250 Kbps.

Otra particularidad de ZigBee, es que se ha pensado para que pueda operar en distintas bandas de frecuencia para las que no se necesitan licencias de uso.

DECT

El objetivo de la tecnología DECT (Digital Enhanced Cordless Telecommunications 'Es una tecnología de radio para aplicaciones de voz') es facilitar las comunicaciones inalámbricas entre terminales telefónicos inalámbricos. Mediante esta tecnología varios terminales telefónicos inalámbricos pueden compartir una misma línea telefónica, disfrutando además de ciertas facilidades típicas de una centralita.

DECT trabaja en una banda de frecuencias de 1.9 Ghz y utiliza la técnica TDMA (time división múltiple access 'divide un canal de frecuencia de radio en varias ranuras de tiempo'). La velocidad máxima actual a la que trabaja DECT es de 2 Mbps con alcance de hasta 200 metros.

La mayor limitación que presenta DECT ha sido, que solamente trabaja en el rango de frecuencias de 1880 a 1900 MHz. Al tratarse de una banda que no es de uso público no está disponible en todos los países.

A pesar de que técnicamente DECT podría haber sido competidor de Bluetooth o incluso de otros sistemas inalámbricos de mayor alcance, como Wi-Fi, el hecho que de que trabaje en la banda 1.9 GHz y que esté muy orientado a voz le puso grandes limitaciones para competir con estas otras tecnologías.

Infrarrojo

La luz infrarroja es un tipo de radiación electromagnética invisible para el ojo humano. Los sistemas de comunicaciones con infrarrojo se basan en la emisión y recepción de haces de luz infrarroja. La mayoría de los mandos a distancia de los aparatos domésticos (televisión, video, equipos de música, etc.) utilizan comunicación por infrarrojo. Por otro lado, la mayoría de las PDA (Personal Digital Assistant - Asistente Personal Digital), algunos modelos de teléfonos móviles y muchas computadoras portátiles incluyen un dispositivo infrarrojo como medio de comunicación entre ellos.

La tecnología de infrarrojos parece que ha encontrado su nicho en las comunicaciones a muy corto alcance. Esto convierte a IrDA ofrece la ventaja adicional de la seguridad, ya que las emisiones que hace infrarrojo se quedan en un entorno mucho más privado que las propagaciones de ondas de radio.

1.1.2 Redes inalámbricas de área local

Wi-Fi (Wireless Fidelity)

Durante varios años, las redes inalámbricas de computadoras se llevan a cabo utilizando soluciones particulares de cada fabricante. Estas soluciones, llamadas propietarias, tenían el gran inconveniente de no permitir interconectar equipos de distintos fabricantes. Cada fabricante desarrollaba su propia solución y la comercializaba por su cuenta.

En caso de las redes locales inalámbricas, el sistema que se está imponiendo es el propuesto por la asociación WECA (*Wíreless Ethernet Compability Alliance*, `Alianza de Compatibilidad Ethernet inalámbrica`) y normalizado por IEEE con el estándar 802.11b. a está norma se le conoce más habitualmente como Wi-Fi o *Wíreles Fidelity* (`Fidelidad inalámbrica`).

Con el sistema Wi-Fi se puede establecer comunicaciones a una velocidad máxima de 11 Mbps, alcanzándose distancias de hasta varios cientos de metros. No obstante, más reciente a esta tecnología permite alcanzar los 22, 54 y hasta los 100 Mbps (Mega bits por segundo).

HomeRF

A principios de 1999 HomeRF (una solución de redes inalámbricas para hogares "inteligentes") sacó la versión 1.0 de su protocolo SWAP (`Protocolo de acceso compartido inalámbrico`). La versión 2.0 salió en mayo del 2001.

SWAP trabaja en una banda de frecuencias de 2.4 GHz y permite configuraciones de punto a punto y en red.

La versión 1.0 permite transmitir datos a 1.6 Mbps y mantener hasta cuatro comunicaciones dúplex de voz. Tiene un alcance de unos 50 metros y una

potencia de transmisión de 100 mW. Utiliza un protocolo similar a IEEE 802.11 para datos y otro similar a DECT para voz. La versión 2.0 alcanza los 10Mbps.

HiperLAN

HiperLAN (`Red de área local de radio de alto rendimiento`). La primera versión de este estándar HiperLAN/1, trabaja en la banda de frecuencias de 5 GHz y alcanza velocidades de hasta 24 Mbps.

HiperLAN/2 ofrece velocidades de transmisión de 54 Mbps utilizando el sistema OFDM (Multiplexado Ortogonal por División de Frecuencia). Las frecuencia utilizadas son de 5.25 a 5.35 GHz para sistemas de interior a 200 mW de potencia y de 5.47 a 5.725 GHz para sistemas de exterior a 1000 mW de potencia.

1.1.3 Redes inalámbricas de área metropolitana

LMDS

LMDS (es una tecnología inalámbrica vía radio para comunicaciones entre puntos fijos). Esto quiere decir que no es una tecnología pensada para ser utilizada por terminales en movimiento. El rango de frecuencias utilizado varía entre 2 y 40 GHz dependiendo de la regularización del país en que se utilice.

LMDS utiliza un transmisor central emitiendo su señal sobre un radio de hasta 5 kilómetros. Las antenas de los receptores se sitúan generalmente en los techos de los edificios para procurar una visibilidad directa con el transmisor central.

Un inconveniente de los sistemas LMDS es que no existe un estándar que asegure la compatibilidad de los equipos de distintos fabricantes.

WiMax

WiMax (Interoperatividad mundial para accesos de microondas) es una tecnología de transmisión inalámbrica de datos que permite crear zonas de accesos concurrentes de hasta 48 Km de radio a velocidades de hasta 70 Mbps sin necesidad de visibilidad directa.

Uno de los mas grandes inconvenientes que ha tenido siempre WiMax era que no permitía la movilidad. Sin embargo, en diciembre del 2005 quedó aprobado lo que se conoce como WiMax Móvil o 802.16e, el cual permite la utilización de terminales en movimiento.

1.1.4 Redes inalámbricas de área globales.

GSM

GSM (Global System for Mobile comunications, Sistema Global para Comunicaciones Móviles) es una tecnología estandarizada por el ETSI (*European Telecomunications Standards Institute*, `Instituto europeo de estándares de telecomunicaiones`).

GSM puede transmitir datos de 13 Kbps sin necesidad de utilizar módem. Para conectar una computadora o PDA a un teléfono GSM, sólo hace falta un cable adaptador y el *software* apropiado para cada equipo. Un modo especial de transmisión de datos que admite GSM es el envío y recepción de mensajes cortos de texto (hasta 160 caracteres) mediante el servicio SMS (Short Message Service, `Servicio de mensajes cortos`) desde el propio Terminal de telefonía móvil. Estos

mensajes pueden intercambiarse tanto con otros terminales móviles, como con terminales de telefonía fija e Internet.

CDMA

CDMA (Code divison Multiple Access, ‘Acceso Múltiple de División de Código’) es una tecnología desarrollada por la empresa Qualcomm. El gran mérito de esta tecnología es que supone una nueva forma de establecer comunicaciones inalámbricas multiusuario con un aprovechamiento de la capacidad seis veces mejor que TDMA. CDMA estuvo lista en 1988, aunque, posteriormente, con la ayuda de AT&T, Motorota y otros fabricantes, se desarrolló una nueva versión dual (analógica y digital) a la que se llamó IS-95, y que ha sido la que se ha instalado en diferentes países. La primera implantación de CDMA tuvo lugar en Hong Kong en 1995, CDMA también ofrece el servicio SMS de mensajes cortos.

2.5G

Aunque los sistemas 2G (Es una tecnología digital de telefonía móvil) tienen ciertas capacidades de transmisión de datos, fundamentalmente se trata de un sistema que da soporte a servicios de voz. Para ofrecer servicios de datos, se ha pensado en una nueva generación de redes celulares, la tercera generación o 3G. No obstante, mientras se desarrolla convenientemente la tecnología para poder ofrecer servicios 3G, se ha creado una ampliación de la tecnología 2G a la que se ha llamado 2,5G. Esta tecnología de transición añade nuevas capacidades de transmisión de datos a la infraestructura de la red celular existente.

3G

3G (Formato contenedor de multimedia definido por Third Generation Partnership Project)

En el paso de las redes celulares analógicas a las digitales, cada una de las tres regiones importantes desde el punto de vista del desarrollo tecnológico de la tecnología celular (Europea, Norteamérica y Asia) tomaron caminos distintos. Incluso dentro de cada una de las regiones ha habido variaciones. En cualquier caso, es evidente que lo ideal sería que la tercera generación (3G) se afrontara con el objetivo de conseguir un sistema global común. No obstante, conseguir esto es extremadamente complicado debido a los diferentes intereses económicos, políticos y regulatorios que tiene cada parte.

Se puede decir que la tecnología celular de tercera generación comenzó en 1985 cuando la UIT (Unión Internacional de Comunicaciones) anuncio su iniciativa de crear un nuevo sistema de comunicaciones móviles al que le llamó FPLMTS (Futuro sistema de comunicaciones móviles terrestres). Esta iniciativa se concretó en 1996 con la creación de IMT2000 (Comunicaciones móviles internacionales). El numero 2000 se le puso porque se esperaba que la nueva tecnología estuviera lista para la primera década de este nuevo milenio y porque la banda de frecuencia asignada era 2GHz.

4G

Evidentemente la evolución es imparable. La tercera generación no está todavía bien introducida en el mercado, sin embargo, los desarrolladores de tecnología están continuamente trabajando en nuevos estándares que permitan ir más allá. Las características que se están considerando son las siguientes.

- Velocidades de bajada de 100Mbps y velocidades de subida de 50Mbps por cada 200MHz del espectro de frecuencia.
- Al menos 200 usuarios activos por cada célula de 5MHz.
- Tiempos de latencia menores de 5ms.
- Utilización flexible de bandas de frecuencia (entre 1,25MHz y 20MHz).
- Tamaño óptico de las células de 5Km, pudiendo alcanzarse los 100Km con una respuesta aceptable.
- Coexistencia y transparencia en otros estándares (GSM/GPRS o UMTS).

Adicionalmente, una característica de las redes 4 G va a ser que estén basadas, fundamentalmente, en el protocolo IP.

1.2 Opción elegida

Dentro del estudio realizado se pudo comprobar y verificar los diferentes servicios y aplicaciones que cada una de las tecnologías de comunicación inalámbrica ofrecen, como hemos visto anteriormente, existen muchas tecnologías distintas de comunicaciones inalámbricas. Muchas de estás tecnologías son complementarias, pero otras dan respuesta a una misma necesidad y, por lo tanto, compiten entre ellas por ser las favoritas del mercado. Sin embrago, es importante mencionar que se depuran muchas de estas tecnologías en nuestro caso, puesto que el proyecto requiere la aplicación de una tecnología de redes de área local inalámbricas que permita trabajar en la instrumentación del proyecto, del tal forma que el resultado proporcione la certeza de que la instalación sea con la tecnología adecuada, por esta razón Wi-Fi se ha convertido en un estándar, ganando la batalla a HomeRF y HiperLAN.

El estudio considera que el desarrollo de cinco características básicas que requieren dichas redes de área local, debe ser alto para ser susceptibles de utilizarse como solución. Estas características son:

- Normalización
- Regularización
- Tecnología
- Servicios
- Precio

Wi-Fi se posiciona mejor que el resto en la mayoría de estos puntos presentados en la tabla 3.1:

Características	Wi-Fi	HiperLAN	HiperRF
Normalización	Alto	Alto	Bajo
Regularización	Alto	Medio	Alto
Tecnología	Medio	Alto	Alto
Servicios	Alto	Medio	Medio
Precios	Alto	Bajo	Bajo

1.1 Tabla comparativa

Con las características reunidas y la comparación de las tres posibles tecnologías que se pueden utilizar dentro del proyecto se puede decir que Wi-Fi, es la que mejor reúne los requisitos y las características apropiadas para el proyecto. De esta forma podemos decir que, la tecnología día con día evoluciona rápidamente y los cambios en el ámbito de las comunicaciones inalámbricas también.

Por esa razón se realizó el estudio de toda la gama de tecnología de comunicaciones inalámbricas, de esta forma verificamos que estas se clasifican en diferentes grupos como son: Redes inalámbricas de área personal, Redes

inalámbricas de área local, Redes inalámbricas de área metropolitana y Redes inalámbricas globales.

CAPITULO II

MARCO TEORICO

CAPITULO II

MARCO TEORICO

2.1 Introducción

Los sistemas de cableado estructurado constituyen una plataforma universal por donde se transmiten tanto voz como datos e imágenes y constituyen una herramienta imprescindible para la construcción de edificios modernos o la modernización de los ya construidos. Ofrece soluciones integrales a las necesidades en lo que respecta a la transmisión confiable de la información, por medios sólidos; de voz, datos e imagen.

Las características del sistema de cableado estructurado ofrecen tres ventajas principales al dueño o usuario:

- Debido a que el sistema de cableado es independiente de la aplicación y del proveedor, los cambios en la red y en el equipamiento pueden realizarse por los mismos cables existentes.
- Debido a que los outlets (salidas para conexión) están cableados de igual forma, los movimientos de personal pueden hacerse sin modificar la base de cableado.
- La localización de los hubs y conmutadores de la red en un punto central de distribución, en general un closet de telecomunicaciones, permite que los problemas de cableado o de red sean detectados y aislados fácilmente sin tener que parar el resto de la red.

Reseña de Cableado Estructurado:

El cableado estructurado consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local. Suele tratarse de

cable de par trenzado de cobre, para redes de tipo IEEE 802.3. Sin embargo, también puede tratarse de fibra óptica o cable coaxial.

Normas que rigen al Cableado Estructurado:

El profundo avance de la tecnología ha hecho que hoy sea posible disponer de servicios que eran inimaginables pocos años atrás de la oficina, el correo electrónico, para mencionar solamente algunos de los servicios de aparición más creciente, que coexisten con otros ya tradicionales, como la telefonía, FAX, etc. Sin embargo, para poder disponer de estas prestaciones desde todos los puestos de trabajo ubicados en un edificio de oficinas se hace necesario disponer, además del equipamiento (hardware y software), de las instalaciones físicas (sistemas de cableado) necesarias. Los diversos servicios arriba mencionados plantean diferentes requerimientos de cableado.

Si a ello le sumamos que permanentemente aparecen nuevos productos y servicios, con requerimientos muchas veces diferentes, resulta claro que realizar el diseño de un sistema de cableado para un edificio de oficinas, pretendiendo que dicho cableado tenga una vida útil de varios años y soporte la mayor cantidad de servicios existentes y futuros posible, no es una tarea fácil.

Para completar el panorama, se debe tener en cuenta que la magnitud de la obra requerida para llegar con cables a cada uno de los puestos de trabajo de un edificio es considerable, implicando un costo nada despreciable en materiales y mano de obra.

Si el edificio se encuentra ya ocupado - como ocurre en la mayoría de los casos- se deben tener en cuenta además las alteraciones y molestias ocasionadas a los ocupantes del mismo. Para intentar una solución a todas estas consideraciones (que reflejan una problemática mundial) surge el concepto de lo que se ha dado en llamar *“cableado estructurado”.*

Dos asociaciones empresarias, la Electronics Industries Asociation (EIA) y la de Telecommunications Industries Asociation (TIA), que agrupan a las industrias de electrónica y de telecomunicaciones de los Estados Unidos, han dado a conocer, en forma conjunta, la norma EIA/TIA 568 (1991), donde se establecen las pautas a seguir para la ejecución del cableado estructurado.

La norma garantiza que los sistemas que se ejecuten de acuerdo a ella soportarán todas las aplicaciones de telecomunicaciones presentes y futuras por un lapso de al menos diez años.

2.1.1 Introducción a las redes.

EL vertiginoso avance tecnológico que han experimentado los campos de la electrónica y la computación en los últimos 50 años, permitieron incrementar la capacidad y velocidad de los sistemas de comunicación.

Actualmente existen varios tipos de redes de cómputo establecidas por diferentes plataformas tecnológicas desarrolladas por los fabricantes, cada uno de ellas con normas, reglas y/o algunos parámetros propios del fabricante, así como los electos que pudieran ingresar a una red.

Es un grupo de Computadoras interconectadas a través de uno o más caminos o medios de transmisión. Si se analiza la definición anterior se concluye que los electos básicos de una red de cómputo son las Computadoras, los Medios de Transmisión y los Dispositivos que permiten interconectarlos.

2.1.2.- Redes Inalámbricas

Una red inalámbrica de datos no es más que un conjunto de computadoras, o de cualquier otro dispositivo informático, comunicados entre sí mediante soluciones que no requieran el uso de cables de interconexión. También existen redes inalámbricas de voz, ambas van de la mano y su crecimiento es día a día mayor en el mercado.

Aunque se puede llegar a pensar que las redes inalámbricas están orientadas a dar solución a las necesidades de comunicaciones de las empresas, dado su bajo costo, cada vez más forman parte del equipamiento de los hogares.

Para disponer de una red inalámbrica, sólo hace falta instalar una tarjeta de red inalámbrica en las computadoras involucrados, hacer una pequeña configuración y listo. Esto quiere decir que instalar una red de este tipo es mucho más rápido y flexible que instalar una red de cableado. El solo hecho de pensar de no tener que instalar cables por el suelo y paredes de oficina o casa, es por demás gratificante. Además, las redes inalámbricas hacen posible que sus usuarios se muevan libremente sin perder la comunicación.

Una vez instalada la red inalámbrica, su utilización es prácticamente idéntica a la de una red cableada. Las computadoras que forman parte de la red pueden comunicarse entre sí y compartir toda clase de recursos, se pueden compartir archivos, directorios, impresoras, unidad de disco, o incluso, el acceso a otras redes, como puede ser Internet. Para el usuario, en general, no hay diferencia entre estar conectado en una red cableada o una red inalámbrica. De la misma forma, al igual que ocurre con las redes cableadas, una red inalámbrica puede estar formada por tan sólo dos computadoras o por miles de ellas.

El Wi-Fi, que tanto éxito tiene actualmente, está incorporado en el 90% de las computadoras portátiles que se venden hoy día, conectándolas a unos 100.000 “puntos calientes” de todo el mundo. Esta tecnología ha impulsado nuevos modelos comerciales, nuevos servicios y aplicaciones, y sigue evolucionando.

Esta trayectoria del Wi-Fi fue posible porque la industria entera se adhirió a una norma abierta que respondía a la gran demanda por movilidad de los usuarios. Pero el Wi-Fi también se benefició de un marco reglamentario favorable. A fin de alcanzar su éxito actual, el Wi-Fi necesitaba tener acceso a características técnicas y un espectro que no requiriera licencias. La industria y la mayoría de las administraciones cooperaron para crear las condiciones que permitieran la aparición de la norma.

2.1.3 Puntos de acceso.

Los puntos de acceso, también llamados APs o Wireless Access Point, son equipos hardware configurados en redes Wifi y que hacen de intermediario entre el computadora y la red externa (local o Internet). Los puntos de acceso o punto de acceso, hace de transmisor central y receptor de las señales de radio en una red Wireless.

Los puntos de acceso utilizados en casa o en oficinas, son generalmente de tamaño pequeño, componiéndose de un adaptador de red, una antena y un transmisor de radio.

2.1.4 Tipos de Puntos de acceso.

Existen redes Wireless pequeñas que pueden funcionar sin puntos de acceso, llamadas redes “ad-hoc” o modo peer-to-peer, las cuales solo utilizan las tarjetas de red para comunicarse. Las redes mas usuales que veremos son en modo estructurado, es decir, los puntos de acceso harán de intermediario o puente entre los equipos wifi y una red Ethernet cableada.

También harán la función de escalar a mas usuarios según se necesite y podrá dotar de algunos elementos de seguridad.

Los puntos de acceso normalmente van conectados físicamente por medio de un cable de pares a otro elemento de red, en caso de una oficina o directamente a la línea telefónica si es una conexión doméstica. En este último caso, el AP estará haciendo también el papel de enrutador. Son los llamados Wireless Routers los cuales soportan los estándar 802.11a, 802.11b y 802.11g.

Cuando se crea una red de puntos de acceso, el alcance de este equipo para usuarios que se quieren conectar a el se llama “celda”. Usualmente se hace un estudio para que dichas celdas estén lo mas cerca posible, incluso solapándose un poco. De este modo, un usuario con un portátil, podría moverse de un AP a otro sin perder su conexión de red.

Los puntos de acceso antiguos, solían soportar solo a 15 a 20 usuarios. Hoy en día los modernos APs pueden tener hasta 255 usuarios con sus respectivas computadoras conectándose a ellos.

Si conectamos muchos Puntos de acceso juntos, podemos llegar a crear una enorme red con miles de usuarios conectados, sin apenas cableado y moviéndose libremente de un lugar a otro con total comodidad.

A nivel casero y como se ha dicho, los puntos de acceso inalámbricos nos permitirán conectar varias conexiones Ethernet o Fast Ethernet, y a su vez conectar varios clientes sin cable. Sin embargo debemos ser cautos, en la figura 2.1 se muestran algunos de los puntos de acceso que existen en el mercado.

Fig. 2.1 Tipos de acces Point

Cualquier persona con una tarjeta de red inalámbrica y un portátil puede conectarse a nuestra red Wifi y aprovecharse gratuitamente de nuestro ancho de banda. Para evitar esto, el AP puede hacer filtrados por MAC o dirección física no permitiendo la conexión de clientes desconocidos. Muchos de estos dispositivos llevan ya instalado su propio Firewall con el que proteger la red.

2.1.5 Características.

Podríamos definir una red Wi-Fi, también llamada wíreless, WLAN o red inalámbrica, como un medio de transmisión de datos designado para dar acceso entre si a computadoras utilizando ondas de radio en lugar de cables. Para ello, con dichas ondas de radio mantienen canales de comunicación entre computadoras.

Unas redes inalámbricas Wi-Fi ofrecen ventajas y desventajas con respecto a una red con cables. Las ventajas, como habrás supuesto, son movilidad y la eliminación de molestos cables. Las desventajas las podemos clasificar en posibles interferencias dependiendo del tiempo u otros dispositivos wireless. También tiene ciertas limitaciones para pasar señales por muros sólidos.

La tecnología Wi-Fi está ganando popularidad tanto en entornos de hogar como de empresa, y por ello, día a día continua mejorando tanto técnicamente como económicamente. Normalmente se usa con computadoras portátiles dado su facilidad para desplazarlo de un punto a otro. Cuando se habla de Wi-Fi tenemos que saber que existen varias tecnologías o standards que lo componen y que definen velocidad (hasta 11 MB), frecuencia y otros detalles; 802.11a, 802.11b y 802.11g (esta última soporta las dos anteriores).

Los elementos que una persona necesita para proveerse de una red Wi-Fi incluye:

- Tarjeta de red inalámbrica.
- AP's - Puntos de acceso access point
- Router wireless que llevará incorporado una antena Wi-Fi.

Y con estos dispositivos, por supuesto, tener una buena computadora portátil para acceder a la red sin complicaciones.

Al contratar Internet de una proveedora de servicios de Internet, suelen entregar el router de acceso preparado para Wi-Fi.

Hay que tener también en cuenta que algunos portátiles vienen con la tarjeta de red inalámbrica ya incorporada en el equipo.

Una vez constituida la red Wi-Fi, se podrá compartir archivos, imprimir documentos, compartir la conexión de Internet y muchas mas cosas, desde cualquier punto de la casa u oficina sin ninguna atadura de cables.

2.1.6 Ventajas y desventajas de la red.

Pues bien como ya se ha mencionado las redes inalámbricas hacen exactamente el mismo trabajo que realizan las redes cableadas, interconectan computadoras y otros dispositivos informáticos (impresoras, modem, etc.) para permitirles compartir recursos. Las redes locales permiten conectar desde dos computadoras hasta cientos de ellos situados en un entorno donde la distancia máxima de un extremo a otro de la red suele ser de algunos cientos de metros. Esto quiere decir que las redes de área local se limitan generalmente el ámbito de un edificio. No obstante, distintas redes locales situadas en distintos edificios (edificios que pueden estar en diferentes ciudades o a distancias muy grandes) pueden intercomunicarse entre sí formando un único entorno de red.

En resumen las ventajas que ofrece una red de área local, sea cableada o inalámbrica son las siguientes:

- Permite compartir periféricos: impresoras, escáneres, discos duros en red, etc.
- Permite compartir los servicios de comunicaciones (ADLS, módem cable, RDSI, etc.)
- Permite compartir la información contenida en cada computadora.
- Permite compartir aplicaciones

A partir de esta pequeña explicación, la pregunta sería si la red local que se desea instalar debe ser cableada o inalámbrica. Muchos usuarios responden a esta cuestión simplemente decidiéndose a instalar la última tecnología del mercado, y la última tecnología es la inalámbrica. La inquietud de disponer de la tecnología más moderna es loable y no cabe duda de que las redes inalámbricas ofrecen una mayor comodidad de uso a una mayor facilidad de instalación, pero toda tecnología tiene sus propias limitaciones. Por tanto,

resulta interesante pararse y analizar un poco las ventajas y posibles inconvenientes que tiene la tecnología inalámbrica.

Ventajas:

Las principales ventajas que ofrecen las redes Wi-Fi frente a las redes cableadas son las siguientes.

Movilidad. La libertad de movimiento es uno de los beneficios más evidentes de las redes Wi-Fi. Una computadora o cualquier otro dispositivo (Por ejemplo, una PDA o una *webcam*) pueden sustituirse en cualquier punto dentro del área de cobertura de la red sin tener que depender de si es posible o no hacer llegar un cable hasta ese sitio. Ya no es necesario estar atado a un cable para navegar por Internet, imprimir un documento o acceder a la información de la red local. En la empresa se puede acceder a los recursos compartidos desde cualquier lugar, hacer presentaciones en salas de reuniones, acceder a archivos, etc., sin tener que tener cables por mitad de la sala o depender de si el cable de red es o no suficientemente largo.

Desplazamiento. Con un computadora portátil o PDA no sólo se puede acceder a Internet o cualquier otro recurso de red local desde cualquier parte de la oficina, si no que podemos desplazar sin perder la comunicación. Esto, aparte de resultar cómodo, facilita el trabajo en determinadas tareas.

Flexibilidad. Las redes Wi-Fi no sólo nos permiten estar conectados mientras nos desplazamos con una computadora portátil, sino que también nos permite colocar una computadora de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio de la configuración de la red. A veces, extender una red cableada no es tan fácil ni barato. En algunas ocasiones es posible que se coloquen peligrosos cables por el suelo para evitar poner enchufes de red más cercanos. Las redes Wi-Fi evitan todos estos problemas. Resulta también

especialmente indicado para aquellos lugares donde se necesitan accesos esporádicos. Si en un momento donde existe la necesidad de que varias personas se conecten a la red en la sala de reuniones, la conexión inalámbrica evita llenar el suelo de cables. En sitios donde pueda haber invitados que necesiten conexión a Internet, las redes inalámbricas suponen una alternativa mucho más viable que las redes cableadas.

Ahorro de costos. Diseñar e instalar una red cableada puede llegar a alcanzar un alto costo, no solamente económico, sino también en tiempo y algunas molestias. En algunas empresas como es el caso de Comisión Federal de Electricidad, cuenta con una gran estructura de red cableada la que da soporte a todos los usuarios, sin embargo la instalación de la red Wi-Fi permite ahorrar costos al permitir compartir recursos: acceso a Internet, impresoras, etc.

Escalabilidad. Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar una nueva computadora cuando se dispone de una red Wi-Fi es algo tan sencillo como instalarle una tarjeta y listo. Con las redes cableadas esto mismo requiere instalar un nuevo cableado o. lo que es peor, esperar hasta que el nuevo cableado quede instalado.

Desventajas:

Evidentemente, como todo en la vida, no todo son ventajas, las redes Wi-Fi también tienen unos puntos negativos en sus comparativas con las redes de cable. Los principales inconvenientes son los siguientes:

Menor ancho de banda. Las redes de cable actualmente trabajan a 100 Mbps, mientras que las redes Wi-Fi aplicada en los radios trabajan a una velocidad no mayor de los 54 Mbps, tomando en cuenta que existen otros estándares similares que solo alcanzan una velocidad de 11 Mbps. Es cierto que

existen estándares que alcanzan velocidades mayores (54, incluso 100 Mbps), pero de forma efectiva la velocidad es bastante menor.

Seguridad. Las redes Wi-Fi tienen la particularidad de no necesitar un medio físico para funcionar (podría funcionar incluso en el vacío). Esto fundamentalmente es una ventaja, pero se conveniente en un inconveniente cuando pensamos que cualquier persona con un computadora portátil solo necesita estar dentro el área de cobertura de la red para intentar acceder a ella. Como el área de cobertura no esta definida por paredes o ningún otro medio físico, a los posibles intrusos ya no les será falta estar conectados a un cable. Wi-Fi ofrece la posibilidad de cifrar sus comunicaciones, pero como eso requiere una cierta participación por parte del administrador de la red, en muchas ocasiones se deja la red sin proteger. Por su parte el cable ofrece unas barreras físicas que le son inherentes.

Interferencias. Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda 2.4 GHz. Esta banda de frecuencia no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes Wi-Fi funcionan en la misma banda de frecuencias. Este hecho hace que no se tenga la garantía de que nuestro entorno radio electrónico esté completamente limpio para que nuestra red inalámbrica funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

Incertidumbre tecnológica. La tecnología que actualmente se esta instalando y que ha adquirido una mayor popularidad es la conocida como IEEE 802.11b y 802.11g. Sin embargo, ya existen tecnologías que ofrecen una mayor

velocidad de transmisión y unos niveles de seguridad. Es posible que, cuando se popularice esta nueva tecnología, se deje de comercializar la actual o, simplemente, se deje de presentar tanto apoyo. Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades de los clientes y, aunque existe esta incógnita, los fabricantes no querrán perder el tirón que ha supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales.

2.2 Historia de Wi-Fi

La historia de las tecnologías inalámbricas Wi-Fi (802.11) y WiMAX (802.16) demuestra la importancia que tiene la colaboración entre la industria y el Gobierno para promover las innovaciones y beneficiar a los consumidores.

El Wi-Fi, que tanto éxito tiene actualmente, está incorporado en el 90% de las computadoras portátiles que se venden hoy día, conectándolas a unos 100.000 “puntos calientes” de todo el mundo. Esta tecnología ha impulsado nuevos modelos comerciales, nuevos servicios y aplicaciones, y sigue evolucionando.

Esta trayectoria del Wi-Fi fue posible porque la industria entera se adhirió a una norma abierta que respondía a la gran demanda por movilidad de los usuarios. Pero el Wi-Fi también se benefició de un marco reglamentario favorable. A fin de alcanzar su éxito actual, el Wi-Fi necesitaba tener acceso a características técnicas y un espectro que no requiriera licencias. La industria y la mayoría de las administraciones cooperaron para crear las condiciones que permitieran la aparición de la norma.

El problema principal que pretende resolver la normalización es la compatibilidad. No obstante existen distintos estándares que definen distintos tipos de redes inalámbricas. Esta variedad produce confusión en el mercado y descoordinación en los fabricantes. Para resolver este problema, los principales vendedores de soluciones inalámbricas (3com, Airones, Intersil, Lucent

Technologies, Nokia y Symbol Technologies) crearon en 1999 una asociación conocida como WECA (Wireless Ethernet Compability Aliance, Alianza de Compatibilidad Ethernet Inalámbrica). El objetivo de esta asociación fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurase la compatibilidad de equipos.

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

En el año 2002 eran casi 150 miembros de la asociación WECA. Como la norma 802.11b ofrece una velocidad máxima de transferencia de 11 Mbps ya existen estándares que permiten velocidades superiores, WECA no se ha querido quedar atrás. Por ese motivo, WECA anunció que empezaría a certificar también los equipos IEEE 802.11a de la banda de 5 Ghz mediante la marca Wi-Fi5.

La norma IEEE.802.11 fue diseñada para sustituir a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red Wi-Fi de una red Ethernet, es en la forma como las computadoras y terminales en general acceden a la red; el resto es idéntico. Por tanto una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales de cable 802.3.

Principios de Wifi

- *Wi-Fi*

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

utilizado en redes locales inalámbricas, es frecuente que en la actualidad también se utilice para acceder a Internet.

Wi-Fi es una marca de la *Wi-Fi Alliance* (anteriormente la *WECA: Wireless Ethernet Compatibility Alliance*), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11.

2.2.1 Innovaciones

Se argumenta que Wi-Fi y las tecnologías de consumo relacionadas son la clave para reemplazar a las redes de telefonía móvil como GSM. Algunos obstáculos para que esto ocurra en el futuro próximo son la pérdida del roaming, la autenticación más precaria y la estrechez del espectro disponible.

Cable, ADSL

La principal ventaja que tiene Wireless (WiFI) frente al cable es que permite conectarnos libremente sin estar atados, lo que permite más movilidad y la posibilidad de conectarse muchas personas sin el problema que puede presentar el cable al tener que cablearse físicamente para conectar puntos.

MODEM

Módem es un acrónimo de MOdulador-DEModulador; es decir, que es un dispositivo que transforma las señales digitales del ordenador en señal telefónica analógica y viceversa, con lo que permite al ordenador transmitir y recibir información por la línea telefónica.

Un módem inalámbrico es un módem que se conecta a una red inalámbrica en lugar de a la red telefónica. Cuando se conecta con un módem inalámbrico,

que está conectada directamente a la red inalámbrica ISP (Internet Service Provider) y puede acceder a Internet.

En la siguiente tabla 2.1 se muestran características de 3 diferentes servicios.

ADSL	Cable	Wi-Fi
El usuario debe disponer de línea telefónica.	El usuario ha de contratar los servicios de cable, como televisión o voz.	No requiere línea telefónica o de cable.
El servicio no puede cambiarse a una nueva dirección sin coste adicional.	El servicio no puede cambiarse a una nueva dirección sin coste adicional.	El servicio puede cambiarse a una nueva dirección, siempre que exista cobertura.
Se necesito un equipo especial para conectar	Se necesita un equipo especial para conectar	Se necesita un equipo especial para conectar
El costo de implantación de estructuras es muy elevado y requiere fuertes inversiones para llevar servicio a nuevas zonas.	El costo de implantación de estructuras es muy elevado y requiere fuertes inversiones para llevar servicio a nuevas zonas. Además se necesita cableado por zonas urbanas y levantamiento de pavimentos y calles.	El costo de apertura de nuevas zonas es muy inferior al de las otras tecnologías, permitiendo llegar a zonas más inaccesibles o de nueva construcción.
Las cuotas mensuales han de sumarse a los costos de la línea telefónica.	Los costos mensuales han de sumarse al alquiler de línea y de equipo.	Las cuotas mensuales no conllevan ningún otro cargo adicional.

2.1 Tabla característica

2.2.2 Ventajas y desventajas de Wifi

Una de las desventajas que tiene el sistema Wi-Fi es la pérdida de velocidad en relación a la misma conexión utilizando cables, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta Wi-Fi, 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 WAP 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 y la falta de seguridad que esto trae consigo.

Ventajas de Wi-Fi

Wi-Fi

Wi-Fi es todavía una tecnología novedosa y que han empezado a utilizar, en hogares o empresas, sólo los pioneros tecnológicos (*early-adopters*). Antes de consolidarse definitivamente, deberá resolver una serie de incógnitas que penden en la actualidad sobre su viabilidad:

- 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.
- 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 Alliance 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.

Cabe aclarar que esta tecnología no es compatible con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS, etc. HERR

2.2.3 Seguridad de Wi-Fi

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. Un muy elevado porcentaje de redes son instaladas por administradores de sistemas y redes por su simplicidad de implementación sin tener en consideración la seguridad y, por tanto, convirtiendo sus redes en redes abiertas, sin proteger la información que por ellas circulan. Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP (Wired Equivalent Privacy, 'Sistema de Cifrado') y el WAP (wireless Application Protocol, 'Norma para aplicaciones de comunicación) que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos, o IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.11, que permite la autenticación y autorización de usuarios. Actualmente existe el protocolo de seguridad llamado *WPA2* (estándar 802.11i), que es una mejora relativa a WPA, es el mejor protocolo de seguridad para Wi-Fi en este momento. Para su utilización en PCs con Windows XP se requiere el Service Pack 2 y una actualización adicional. También es necesario tener hardware (Puntos de acceso y clientes) de última generación que soporte WPA2, pues los puntos de acceso antiguos no lo soportan.

Intentar reducir la inseguridad de WiFi o cualquier otro tipo de tecnología de red con sólo 10 reglas es una utopía, sin embargo nunca está de más utilizar esta lista como base en el proyecto de instalación.

Regla1: Discreción.

Debe Evitarse anunciar innecesariamente la presencia de su instalación WiFi. Asegúrese de cambiar el SSID (identificador de servicios) de sus equipos y no dejar el que viene de fábrica.

Debe procurarse instalar las antenas de punto de acceso (AP) y los niveles de potencia de los equipos para evitar la llegada de señal a áreas donde la cobertura no es deseada ni requerida.

Regla 2: Protección contra la clonación.

Hoy día es fácil "convertir" un dispositivo para que se presente como otro dispositivo. Los dispositivos perdidos o robados son también una amenaza. El filtrado por direcciones de Control de Acceso de Medios (MAC) son un método de autenticación que no puede utilizarse en forma individual. Siempre debe ser acompañado de un método de autenticación independiente de los dispositivos, como los nombres de usuarios y contraseñas, directorios de red existentes u otros esquemas de autentificación.

Regla3: Cifrado de datos

Desear privacidad es algo normal. Para esto, los datos transmitidos inalámbrica mente deben ser cifrados. El cifrado básico provisto por WiFi, conocido WEP, es relativamente débil en todas sus formas y su mantenimiento es costoso e ineficiente. En forma complementaria a este método es aconsejable utilizar tecnologías probadamente eficaces en redes como IPSec con cifrado 3DES. Siempre procure utilizar esquemas de seguridad estándar que faciliten la interoperabilidad.

Regla 4: Filtrado de datos

Esta regla en realidad no es exclusiva de las redes inalámbricas, pero es útil recordarla aquí: se debe Limitar y controlar a donde puede ir el tráfico de la red inalámbrica. Un firewall es la herramienta ideal para esta tarea. Si la red inalámbrica va a ser usada para un propósito determinado, como el acceso a recursos empresariales específicos, entonces se debe configurar los filtros de paquetes para que los datos que provienen de la red inalámbrica no puedan llegar a lugares indeseados.

Regla 5: Restricción al acceso físico de los puntos de acceso.

Debe evitarse emplazar APs en escritorios u otros lugares que pueden ser fácilmente accedidos. Visitantes curiosos, inescrupulosos o empleados descuidados pueden fácilmente mover, reemplazar o resetear los APs. La seguridad no puede garantizarse si no se cuida este punto.

Regla 6: Mantener los ojos abiertos.

Debe Monitorearse activamente las configuraciones de los AP. No es suficiente con configurar un AP correctamente. Una vez configurado, el AP debe permanecer apropiadamente configurado. Es fácil para alguien externo ejecutar un reinicio de hardware en un AP que está colocado en un escritorio o el techo. Al monitorear activamente la configuración del AP, puede asegurar que el AP es automáticamente reconfigurado ante eventos de ese tipo que pudiesen ocurrir.

Regla 7: Controlar los equipos clandestinos.

En muchos lugares los APs pueden ser fácilmente instalados por empleados e intrusos y atentar contra las políticas de seguridad de la red. Debe mantenerse

una política activa de detección de transmisiones WiFi con software de tipo sniffer es un requerimiento operacional crítico para la seguridad.

Regla 8: Extremar atención si no usa puntos de acceso.

En una red inalámbrica operando en modo Ad Hoc (o peer to peer), un intruso pueden filtrarse y obtener acceso a la red simplemente usando un cliente legítimo cono un punto de entrada. Los productos conocidos como personal firewall o software firewall complementados con otras herramientas de administración de red que activamente rastreen y administren al cliente antes de permitirle el acceso mediante la LAN inalámbrica son una buena prevención.

Regla 9: Controlar el uso de ancho de banda.

El no cumplir esta regla lo expone a ataques de negación de servicio (DoS) o una ineficiente utilización del ancho de banda en el mejor de los casos. Hay varias maneras de regular la utilización del ancho de banda pero debe tener en cuenta que los equipos WiFi más básicos no dan ninguna solución en este punto. Esto en realidad no es un problema si ubica esta funcionalidad en otra parte adecuada de su red.

Regla 10: El tiempo es oro.

Siempre que sea posible, implemente políticas de administración en tiempo real. En muchas ocasiones las redes WiFi están ampliamente distribuidas. Por ejemplo abarcan campus enteros e incorporan múltiples sitios globales. Las políticas de seguridad (p. Ej. listas de usuarios validados o derechos de acceso) naturalmente cambiaran. Estos cambios deben verse reflejados en tiempo real a través de la red inalámbrica para reducir la ventana de oportunidades para la intrusión, y más importante aún, facilitar el inmediato cierre de las brechas de seguridad detectadas.

IMPACTO EN MEXICO

En México, TELMEX y AXTEL pertenece a WiMAX y WIFI, Forum y esta en vías de implementación. En la ciudad de Monterrey, Nuevo León (la tercera más extensa del país), habrá más de 100 puntos de acceso a Internet inalámbrico de banda ancha gratuitos en parques, jardines y bibliotecas. Además, el Parque Fundidora y la Macro Plaza, ya cuentan con conexión a Internet gratis. En las ciudades de Puebla, Aguascalientes y Veracruz ya se comercializa WIMAX a través de Ultranet2go, miembro del grupo empresarial Ultra Telecom. En próximos meses Ultranet2go llegará a Coatzacoalcos, Tampico, Iguala, Cuernavaca, Xalapa y Matamoros.

Actualmente en CFE (Comisión Federal de Electricidad) es uno de los pasos grandes que esta dando con la innovación de entrada de esta tecnología, como medio de servicio y a su vez de seguridad a la red y a la de los trabajadores.

2.3 Protocolos.

2.3.1 Concepto de protocolo

Un protocolo es un método estándar que permite la comunicación entre procesos (que potencialmente se ejecutan en diferentes equipos), es decir, es un conjunto de reglas y procedimientos que deben respetarse para el envío y la recepción de datos a través de una red. Existen diversos protocolos de acuerdo a cómo se espera que sea la comunicación. Algunos protocolos, por ejemplo, se especializarán en el intercambio de archivos (FTP); otros pueden utilizarse simplemente para administrar el estado de la transmisión y los errores (como es el caso de ICMP), etc.

En cualquier comunicación, bien sea entre personas o entre máquinas, siempre hacen falta una serie de normas que regulen dicho proceso. En el caso de las comunicaciones entre personas, las normas las establece la sociedad y son aplicadas por cada persona de acuerdo con la educación que haya recibido; en el caso de las máquinas, las normas las establecen los organismos de normalización (IEEE, ETSI, UIT, etc.) y son aplicadas por los ordenadores de acuerdo con el protocolo o conjunto de protocolos que se está utilizando.

Obviamente, aunque existen grandes similitudes de procedimientos, la diferencia fundamental entre personas y máquinas es que las personas están dotadas de inteligencia y pueden adaptarse fácilmente a situaciones imprevistas. Los ordenadores, sin embargo, deben tener protocolos muy estrictos, que tengan previos todos los posibles casos que se pueden presentar en una comunicación, sin dejar nada al azar.

En definitiva, un protocolo no es más que un conjunto de reglas que emplean dos equipos informáticos para dialogar entre sí, de forma que puedan establecer y mantener una comunicación sin errores.

Para que los protocolos puedan llevar a cabo sus objetivos, necesitan añadir ciertos datos de control a la información original a transmitir. Estos datos adicionales son incluidos por el terminal emisor y suprimidos por el terminal receptor antes de entregar la información destino.

En un principio, cada fabricante establecía los procedimientos de comunicación de sus propios equipos, siendo casi imposible conectar equipos de fabricantes distintos. Con la expansión de la informática, se hizo evidente que era necesario disponer de protocolos normalizados que permitiesen la interconexión de equipos independientes de quién los fabricase. Con esta idea, a lo largo de los años han ido apareciendo distintos protocolos normalizados, cada uno de ellos normalizados, cada uno de ellos dedicados a distintas aplicaciones o cubriendo distintas necesidades. Muchos de estos protocolos normalizados han surgido a partir de los protocolos desarrollados por empresas u organismos concretos (caso de TCP/IP para conexiones de redes Internet), mientras que otros han sido desarrollados por los organismos de normalización (Wi-Fi).

De forma práctica, los protocolos de comunicación son unos programas que se instalan tanto en la terminal de origen, como en el destino de la comunicación. Parte de estos programas residen en el propio *hardware* del equipo, otra parte puede venir incorporada en el sistema operativo y la restante debe ser instalada por el usuario en el momento de configurar el equipo.

2.3.2 MODELO OSI

OSI (Open Systems Interconnection) Interconexión de Sistemas Abiertos, el cual fue aprobado en 1984 bajo la norma ISO 7498.

El Modelo OSI proporciona una arquitectura de 7 Niveles (capas), alrededor de los cuales se pueden diseñar protocolos específicos que permitan a diferentes usuarios comunicarse abiertamente.

También se puede decir que es un conjunto complejo de de estándares funcionales que especifican interfaces, servicios y formatos de soporte para conseguir interoperabilidad. La principal utilidad del modelo OSI radica en la separación de las distintas tareas que son necesarias para comunicar dos sistemas independientes.

Describe cómo se transfiere la información desde una aplicación de software en una computadora a través de un medio de transmisión hasta una aplicación de software en otra computadora.

Una red Wi-Fi puede estar formada por dos ordenadores o por miles de ellos. Para que un ordenador pueda comunicarse de forma inalámbrica, necesita tener instalado un adaptador de red. Un adaptador de red es un equipo de radio (con transmisor, receptor y antena) que puede ser insertado o conectado a un ordenador, PDA o cualquier otro equipo susceptible de forma parte de la red (impresoras, etc.).

De forma general, a los equipos que forman parte de una red inalámbrica se les conoce como terminales.

Aparte de los adaptadores de red, las redes Wi-Fi pueden disponer también de unos equipos que reciben el nombre de puntos de acceso (AP o *Access Point*,

en ingles). Un punto de acceso es como una estación base utilizada para gestionar las comunicaciones entre los distintos terminales. Los puntos de acceso funcionan de forma autónoma, sin necesidad de ser conectados directamente a ningún ordenador.

Tanto a los terminales como a los puntos de acceso se les conoce por el nombre general de estación.

Las estaciones se comunican entre sí gracias a que utilizan la misma banda de frecuencias y a que internamente tienen instalados el mismo conjunto de protocolos. Aunque los protocolos que usa Wi-Fi están basados en las siete capas del modelo de referencia OSI, el estándar IEEE 802.11b sólo define las dos capas (física y enlace); entre el resto de las capas son idénticas a las empleadas en las rede locales cableadas e Internet y se conoce con el nombre de conjuntos de protocolos IP (I*nternet Protocol* o 'Protocolo Internet')

En el diagrama 2.1 se muestra las capas del modelo OSI.

	MODELO OSI		PROTOCOLOS
7	APLICACIÓN		HTTP, FTP, POP3, etc.
6	PRESENTACIÓN	COMÚN	DNS,LDAP, XML,etc.
5	SESIÓN		
4	TRANSPORTE		UDP, TCP,etc.
3	RED		IP, ICMP, RSVP, etc.
2	ENLACE		LLC, MAC, etc.
1	FÍSICA		Coaxial, FO, radio, etc.

2.1 Protocolos de red local en el modelo OSI

CAPA FISICA: Esta capa define las propiedades físicas de los componentes (frecuencia de radio utilizadas, cómo se transmiten las señales, etc.).

CAPA DE ENLACE: Esta capa define cómo se organizan los datos que se transmiten, cómo se forman los grupos de datos (paquetes, tramas, etc.) y cómo se asegura que los datos llegan al destino sin errores.

CAPA DE RED: Esta capa define cómo organizar las cosas para que distintas comunicaciones puedan hacer uso de una infraestructura común, una red. Por ejemplo, aquí están definidos cómo se identifican los terminales (numeración) o cómo se enlutan los datos.

CAPA DE TRANSPORTE: Esta cada define las características de la entrega de los datos.

CAPA DE SESION: Aquí se describe cómo se agrupan los datos relacionados con una misma función.

CAPA DE PRESENTACION: nos define cómo es presentada la información transmitida.

CAPA DE APLICACIÓN: Define cómo interactuar los datos con las aplicaciones especificas.

Los modelos como OSI pretenden definir todos y cada uno de los factores que intervienen en una comunicación de una comunicación abierta; sin embargo, no todas las comunicaciones de datos son iguales; por ejemplo, existen comunicaciones en las que no hace falta definir una determinada capa. En cualquier caso, de todos los procedimientos definidos por OSI, los que siempre

están presentes en cualquier tipo de comunicación son aquellos que están incluidos dentro de las capas física y de enlace.

2.3.3 Estándares WIFI de Conexión

A partir del estándar IEEE 802.11/ WIFI se fueron desarrollando otros estándares relacionados con WIFI que han ido introduciendo mejoras y solucionando inconvenientes. Los estándares de WIFI relativos a la transmisión de datos son:

- 802.11
- 802.11a
- 802.11b
- 802.11g
- 802.11n

a) Estándar 802.11: Fue el primero y las velocidades de 1 y 2 Mbps eran muy pequeñas y no permitían implementar aplicaciones empresariales de envergadura, por lo tanto se crearon nuevos grupos de trabajo para crear otros estándares.

b) Estándar 802.11a: Permite realizar transmisiones con velocidades máximas de 54 Mbps y opera en una banda de frecuencia superior a los 5 GHz, por lo tanto no es compatible con el estándar 802.11b y el estándar 802.11g. A pesar de ser el "a" es, prácticamente, el más nuevo pues esa banda de frecuencia estaba asignada en muchos países a fuerzas públicas (bomberos, cruz roja, etc) y recién últimamente está siendo liberada. Es muy útil. Por ejemplo para separar el tráfico o para zonas con mucho ruido e interferencias. Además con el estándar 802.11a se pueden llegar a utilizar hasta 8 canales no superpuestos.

c) Estándar 802.11b: Las conexiones funcionan a una velocidad máxima de 11 Mbps y opera en una banda de 2,4 GHz. Es el más popular pues fue el primero en imponerse y existe un inventario muy grande de equipos y dispositivos que manejan esta tecnología. Además, al ser compatible con el estándar 802.11g permitió la incorporación de éste último a las redes inalámbricas wifi ya existentes. Con el estándar 802.11b, sólo se pueden utilizar 3 canales no superpuestos (de los 11 existentes) en la mayoría de los países. En Europa, según los estándares ETSI, se pueden utilizar 4 canales de los 13 existentes. No todos lo Puntos de Acceso Inalámbrico sirven para los 2 sistemas, así que es importante tenerlo en cuenta a la hora de adquirir un Puntos de acceso.

d) Estándar 802.11g: Las conexiones funcionan a una velocidad máxima de 54 Mbps y opera en una banda de 2,4 GHz. El estándar 802.11g fue aprobado a mediados del año 2003 y se popularizó rápidamente por su compatibilidad con el estándar 802.11b. Lo que muchos desconocen es que al mezclar equipos del estándar 802.11b con equipos del estándar 802.11g la velocidad la fija el equipo más lento, o sea que la instalación mixta seguirá funcionando generalmente a velocidades lentas. Respecto de los canales aquí caben las mismas observaciones que para el estándar 802.11b, o sea que con el estándar 802.11g se pueden utilizar 3 canales no superpuestos de los 11 disponibles y en Europa 4 de los 13 canales disponibles. Los canales que generalmente se utilizan con el estándar 802.11g y con el estándar 802.11b son: "1", "6" y "11" y en Europa: "1", "4", "9" y "13".

e) Estándar 802.11n: Es un estándar nuevo que aún está en elaboración. Si bien se está trabajando en él desde el año 2004, sólo se ha logrado hasta ahora un borrador, que todavía no es definitivo y que, como suele suceder, puede ser modificado hasta la aprobación final del estándar 802.11n. El objetivo es elaborar un estándar con velocidades de transmisión superiores a 100 Mbps. El proceso se está demorando pues entre los promotores del estándar se han formado dos grupos antagónicos WWiSE y TGn Sync. Ninguno de los dos tiene una mayoría suficiente para imponer su tecnología y por lo tanto están trabadas las

negociaciones. En 2005 se creó otro grupo con empresas de ambos bandos para tratar de encontrar algún punto medio. Este grupo es el "Enhanced Wireless Consortium - EWC". En lo único que están los dos grupos de acuerdo es en la utilización de una nueva tecnología conocida como MIMO que permite incrementar el ancho de banda y el alcance en WIFI utilizando Multiplexing. Según se apruebe la propuesta de un grupo u otro, las velocidades podrían variar entre 135 Mbps y 300 Mbps y las bandas de frecuencia serían 10GHz, 20GHz o 40GHz.

f) El Dilema Pre-estándar 802.11n: En las redes inalámbricas WIFI, el tema de la homologación y certificación de equipos, no es un tema menor. Conviene aclarar, desde ya, y enfatizar que la compra de equipos homologados y certificados por la WiFi Alliance (Organización que agrupa a los fabricantes de productos WiFi) es de vital importancia para garantizar un funcionamiento armónico de los diversos elementos que componen una red inalámbrica wifi. Debido a las demoras que se están produciendo con este estándar, y ante la avidez de los consumidores por instalar redes inalámbricas wifi con velocidades superiores a 54 Mbps, existen algunos fabricantes que desde hace varios meses están ofreciendo productos "supuestamente" del estándar 802.11n. Como se explicó anteriormente, el estándar 802.11n aún no existe y sólo hay un borrador que todavía puede ser modificado una o más veces. Por consiguiente la WiFi Alliance, ha comunicado que no certificará productos respecto del inexistente estándar 802.11n.

Por todo esto es importante dejar claro a todos los usuarios que cualquier producto que compren de 802.11n no es estándar y puede presentar ahora y, aún más en el futuro, problemas de compatibilidad con otros elementos de la red inalámbrica wifi.

Estándares IEEE 802.11 - WIFI, Más Relevantes

- 802.11a - Transmisión de Datos en la Banda de 5GHz
- 802.11b - Transmisión de Datos en la Banda de 2.4GHz

- 802.11e - QoS - Calidad de Servicio
- 802.11g - Transmisión de Datos Adicional Banda 2.4 GHz
- 802.11h - Espectro y Potencia en Europa - Banda 5 GHz
- 802.11i - Mejoras en Seguridad WIFI (WPA/WPA2)
- 802.11k - Mediciones y Gestión de RF en WIFI
- 802.11n - Transmisión de Datos - Altas Velocidades (MIMO)
- 802.11p - WAVE (WIFI en vehículos)
- 802.11r - Fast Roaming
- 802.11s - Redes Malla / Wifi Municipal
- 802.11u - Internetworking con otras Redes
- 802.11v - Puntos de accesos, Gestión de Clientes (MIB)
- 802.11w - Seguridad de Paquetes de Management.

Las capas de IEEE 802.2

La norma IEEE 802.2 define exclusivamente los temas relacionados con las dos primeras capas del sistema OSI: las capas física y la de enlace. De hecho, a la capa de enlace la divide en dos, por lo que el resultado son tres capas.

- PHY (Physical Layer, 'Capa física') es la capa que se ocupa de definir los métodos por los que se difunde la señal.
- MAC (Médium Access Control, 'Control de acceso al medio') es la capa que se ocupa del control de acceso al medio físico. En el caso de Wi-Fi el medio físico es el espectro radioeléctrico. La capa MAC es un conjunto de protocolos que controlan cómo los dispositivos comparten el uso de este espectro radioeléctrico.
- LLC (Logical Link Control 'Control de enlace lógico') es la capa que se ocupa del control de enlace lógico. Define cómo pueden acceder múltiples usuarios a la capa MAC.

Estándar 802.2

IEEE 802.2 es el IEEE 802 estándar que define el control de enlace lógico (LLC), que es la parte superior de la capa enlace en las redes de área local. La subcapa LLC presenta un interfaz uniforme al usuario del servicio enlace de datos, normalmente la capa de red. Bajo la subcapa LLC esta la subcapa Media Access Control (MAC), que depende de la configuración de red usada (Ethernet, token ring, FDDI, 802.11, etc.).

El estándar IEEE incluye esta subcapa que añade las etiquetas estándar de 8-bit *DSAP* (*Destination Service Access Point*) and *SSAP* (*Source Service Access Point*) a los paquetes del tipo de conexión. También hay un campo de control de 8 o 16 bits usado en funciones auxiliares como Control de flujo. Hay sitio para 64 números SAP globalmente asignados, y la IEEE no los asigna a la ligera. IP no tiene un número SAP asignado, porque solo los “estándares internacionales” pueden tener números SAP. Los protocolos que no lo son pueden usar un número SAP del espacio de SAP administrado localmente. EL Subnetwork Access Protocol (SNAP) permite valores EtherType usados para especificar el protocolo transportado encima de IEEE 802.2, y también permite a los fabricantes definir sus propios espacios de valores del protocolo.

- 1 Modos Operativos
- 2 Encabezado LLC
- 3 IEEE 802.2 palabras de control de Encabezado y formatos de paquete.

Modos Operativos

IEEE 802.2 incorpora dos modos operativos no orientados a conexión y uno orientado a conexión:

- Tipo 1 Es un modo no orientado a conexión y sin confirmación. Permite mandar frames:

- A un único destino (punto a punto o transferencia unicast),
- A múltiples destinos de la misma red (multicast),
- A todas las estaciones de la red (broadcast).

El uso de multicast y broadcast puede reducir el tráfico en la red cuando la misma información tiene que ser enviada a todas las estaciones de la red. Sin embargo el servicio tipo 1 no ofrece garantías de que los paquetes lleguen en el orden en el que se enviaron; el que envía no recibe información sobre si los paquetes llegan.

- Tipo 2 es un modo operativo orientado a conexión. La enumeración en secuencia asegura que los paquetes llegan en el orden en que han sido mandados, y ninguno se ha perdido.
- Tipo 3 es un modo no orientado a conexión con confirmación. Únicamente soporta conexión punto a punto (point to point).

Capa de enlace

La capa de enlace de datos del estándar 802.11 se compone de dos subcapas: la capa de control de enlace lógico (o LLC) y la capa de control de acceso al medio (o MAC).

La capa MAC define dos métodos de acceso diferentes:

- El método CSMA/CA usa la función de coordinación distribuida (DCCM).
- El método de función de coordinación de punto (PCCM).

El método de acceso CSMA/CA

En una red Ethernet local común los equipos utilizan el método de acceso CSMA/CD (Acceso Múltiple Sensible a la Portadora con Prevención de Colisión) por el cual cada equipo tiene la libertad de comunicarse en cualquier momento. Cada equipo que envía un mensaje verifica que no haya otro equipo enviando un mensaje al mismo tiempo. Si alguno lo está haciendo, entonces ambos equipos deben esperar un período de tiempo aleatorio antes de comenzar a enviar el mensaje de nuevo.

Con la tecnología inalámbrica este proceso no es posible ya que dos estaciones que se comunican con un receptor no pueden escucharse entre sí al mismo tiempo debido a sus diferentes rangos de transmisión. Por esta razón, el estándar 802.11 utiliza un protocolo similar llamado CSMA/CA (Acceso Múltiple Sensible a la Portadora con Prevención de Colisión).

El protocolo CSMA/CA utiliza un mecanismo de evasión de colisiones basado en mensajes recíprocos de acuse de recibo que el transmisor y receptor intercambian como se muestra en la figura 2.2:

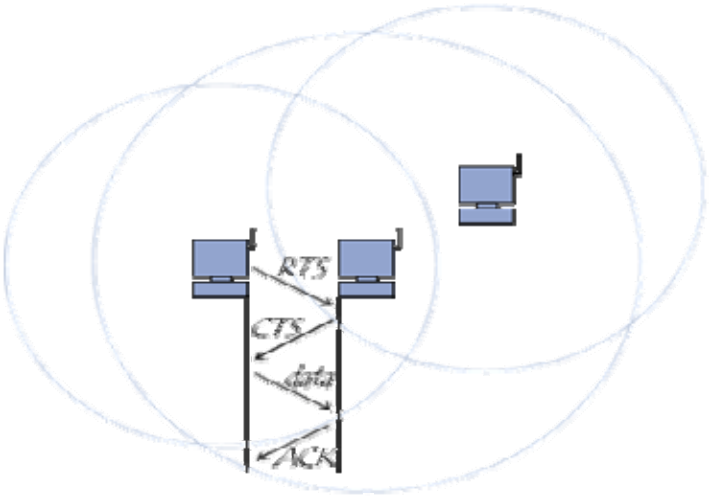


Fig. 2.2

La estación que desea transmitir escucha a la red. Si la red está ocupada, la transmisión se suspende hasta más tarde. Sin embargo, si el medio permanece libre durante un cierto período de tiempo (llamado DIFS, que es el espacio entre tramas), la estación puede transmitir la señal. La estación transmite un mensaje "Listo para enviar" (o abreviado RTS, por "Ready To Send") con información sobre la cantidad de datos que desea enviar y su velocidad de transmisión. El receptor, que por lo general es un punto de acceso, responde con un mensaje "Permitido para transmitir" (CTS por "Clear To Send") y después la estación comienza a enviar datos.

Cuando se han recibido todos los datos enviados por la estación, el receptor envía un aviso de acuse de recibo (ACK). Entonces, todas las estaciones cercanas esperan el tiempo estimado necesario para transmitir esa cantidad de información a la velocidad declarada.

CAPITULO III

PROPUESTA

CAPITULO III

SOLUCIÓN PROPUESTA

3.1 Desarrollo del proyecto.

Actualmente Comisión Federal de Electricidad, tiene una amplia gama de tecnología innovadora, incluyendo sus principales componentes como son los cuartos de comunicación para dar servicio a los usuarios, ya sea voz, datos y video (videoconferencias).

Se puede observar que dentro de los cuartos de comunicación se cuenta con diversos equipos, desde un simple rack de distribución hasta switches de la más alta tecnología.

En la resolución del proyecto se utiliza la tecnología Wi-Fi, para la instalación de radios de la marca Enterasys, ya que es por continuidad tecnológica de la empresa, puesto que es un convenio obtenido de dichas empresas.

3.1.1 Configuración del Puntos de acceso.

Los puntos de acceso necesitan disponer de puertos para poderse conectar con una red local cableada y con Internet, para seguir con este proceso, los puntos de acceso suelen traer uno o más puertos 10/100Base-T (RJ45). No obstante, las posibilidades de conectividad de los puntos de acceso no acaban aquí; dependiendo del modelo, se puede encontrar diferentes características, esto se debe a que cada marca maneja sus configuraciones y estructuración diferentes. Aunque los cambios en algunos casos son muy pequeños siempre es recomendable, ver los lineamientos y normas de cada equipo.

En este caso los puntos de acceso que se usaron llevan una configuración inicial que sirve de guía paso a paso hasta lograr su funcionamiento correcto.

Contraseña: Todos los puntos de acceso (el aparato que recibe y transmite las señales por el aire) traen una contraseña predeterminada. Cada fabricante les coloca un nombre de usuario y una contraseña a todos sus modelos. Con lo cual, lo primero que hace un hacker (Persona que se dedica a entrar ilegalmente en sistemas) es probar con esos nombres de usuarios y contraseñas. Entonces, lo mejor es cambiarlas por claves difíciles de descubrir.

Encriptación: La información que viaja por el aire en una red sin cables debe ser ininteligible para los intrusos. Más precisamente, si un hacker puede ver lo que viaja de un lugar a otro de la red, lo mejor es que lo haga sin poder leer o descifrar lo que ve. Para ello, la comunicación debe ser encriptada o cifrada.

Para redes por aire, hay 3 tipos de encriptación: La conocida como WEP es la más común. Los especialistas sostienen que alcanza un nivel de cifrado débil. WAP es un tipo de encriptación más reciente, recomendado por los que saben. El tercer tipo es el nuevo WAP 2. "Es mucho más fuerte. Tiene un nivel de codificación alto.

Para activar algún tipo de encriptación, el sistema pide que se ingresen claves, generalmente en letras y números. Luego, esas claves se deberán ingresar en las PC que se conectan a la red.

Si esas mismas computadoras lo permiten, lo mejor es usar WAP 2, pero sino lo permiten hay que usar WAP o WEP.

Tan importante es el cifrado que algunos proveedores de Internet tienen en cuenta el tema, configurando los puntos de acceso inalámbrico a sus clientes residenciales con una clave de seguridad WEP. Pero si el cliente lo desea, puede dejar su red abierta.

Lejos de ventanas: Como los puntos de acceso tienen un radio de alcance específico, para reducir la posibilidad de intrusos hay que colocarlos lejos de ventanas y paredes. Y será más difícil que ingresen desde afuera.

Sobre todo para empresas, hay un software que delimita el área de cobertura de los puntos de acceso. Esto es ideal para los que no quieren compartir el acceso a la red con la oficina de al lado. "Se llama Wireless Site Manager. Y además les da de baja a los que intentan usar la red sin su autorización y cambia automáticamente las claves de encriptación, por ejemplo WEP, que vienen predeterminadas de fábrica.

Dirección MAC: Toda tarjeta de red (lo que permite a la computadora conectarse a la red) tiene una combinación de letras y números que conforman el número de hardware o dirección MAC. En el programa de configuración de los puntos de acceso se puede configurar qué direcciones MAC podrán ingresar a la red. Así, por ejemplo, si una notebook intrusa quiere ingresar, y la red no alberga en su listado la dirección MAC de esa notebook, el sistema no dejará que ingrese.

No propagar el SSID: Es el nombre de la red inalámbrica. Se puede configurar para propagarlo o para no propagarlo. Si se lo configura en propagarlo, la red propia prácticamente se convertirá en pública. Porque así se invita a entrar a cualquiera.

3.2 Esquema de Configuración.

Servicios de Configuración Inalámbrica.

Un servicio es un concepto que representa un sistema de opciones que se configura y que despliega en la red inalámbrica; no es un artículo seleccionable en la interfaz de RASM. Los servicios se configuran para proporcionar varios niveles del acceso de red inalámbrica a los usuarios, tales como acceso seguro del

empleado, acceso del huésped, acceso multi-recibido, o acceso inalámbrico del IP de excedente de la voz (VoWIP).

Se puede configurar un servicio para ser independiente de otros servicios en la red inalámbrica, o se puede compartir componentes de la configuración entre servicios. Por ejemplo, el acceso multi-recibido se aísla completamente de otros servicios (ninguna configuración compartida), mientras que los servicios que prevén a los invitados y acceso del empleado en una sola corporación pueden compartir un perfil de radio común. De esta manera, se puede reutilizar la parte de la configuración del servicio para otros servicios que se desea proporcionar. Se podría configurar un servicio para el acceso del empleado; entonces se reutiliza la parte de la configuración para proporcionar los servicios para el acceso de invitado.

Cada servicio tiene tipos potenciales de la autentificación; por ejemplo, 802.11, página del Web, MAC address, o acceso abierto. El acceso abierto a veces se llama recurso pasado. Cada servicio también tiene tipos potenciales del cifrado, tales como 802.11i, WPA, WEP, o unencrypted.

Esta sección contiene ejemplos para ayudar a configurar los tipos siguientes de sistemas del servicio:

- Acceso del empleado (802.11).
- Acceso del invitado (portal del Web).
- IP excesivo de la voz (MAC AAA).

Configuración a los servicios del Acceso del Empleado o Usuario.

Los servicios para el acceso del usuario se configuran típicamente para proporcionar el acceso seguro, cifrado a la red inalámbrica.

La tabla 3.1 de tarea, mostrada abajo, contiene las tareas que se necesitan realizar para crear un servicio para el acceso del usuario.

Tarea	Trayectoria	Parámetros a configurar
Crear el perfil de radio	1. Opción barra de herramientas: Se selecciona La Configuración. 2. Organizador del panel: Ampliar el switch de RoamAbout. 3. Ampliar el radio 4. Click en encendido de los perfiles de radio 5. Seleccionar el perfil de radio en la lista de la tarea.	Para crear el perfil de radio Nombre del perfil de radio: incorporar un nombre Después de que se cree el perfil del servicio, se puede mapear al perfil de radio. Después de que se instale el RoamAbout APs, se pueden mapear los radios al perfil de radio. Nota: Los ejemplos en esta sección configuran el perfil de radio primero. Sin embargo, también se puede configurar el perfil de radio más adelante como parte de la configuración del perfil del servicio.
Configurar el servidor RADUIS	1. Opción barra de herramientas: Seleccionar La Configuración. 2. Organizador del panel: Ampliar el switch de RoamAbout. 3. Ampliar Sistema 4. Click RADIUS 5. Seleccionar el servidor del RADIO en la lista de la tarea.	Para la creación del servidor del RADIUS: • Nombre: Incorporar el nombre del servidor. • IP address: Incorporar el IP address del servidor. • Llave: Incorporar la llave. • Grupo del servidor: Permitir que lo cree. • En los servidores mismos del RADIUS configurar el AAA movido hacia atrás (no en RASM): • Instalar cada switch de RoamAbout como cliente del RADIO. • Definir las cualidades vendedor-especificas de Enterasys (VSAs) en el diccionario del servidor del RADIO. • Configurar cada expediente del usuario con reglas de la autorización (username y contraseña). • Configurar a cada usuario con la cualidad del Vlan-Nombre (Enterasys VSA) o la Tunel-Privado-Grupo-Identificación del RADIO para asignar a usuarios a VLANs. • Configurar las reglas de la autentificación (802.11, MAC, acceso abierto, o portal del Web).

Tarea	Trayectoria	Parámetros a configurar
Crear un perfil de servicio por 802.11	1. Opción barra de herramientas: Seleccionar La Configuración. 2. Organizador del panel: Ampliar el switch de RoamAbout. 3. Ampliar el radio 4. Click en servicios de radio 5. Seleccionar el perfil del servicio 802.11 en la lista de la tarea.	Para crear el perfil de servicio: • Se debe mantener el nombre del perfil: Corregir el nombre • Nombre de SSID: Incorporar el nombre • Modo de seguridad: Seleccionar WPA (y quite WEP dinámico) • Tipo de cifrado: Utilizar TKIP • Tipo de EAP: Utilizar el servidor externo del RADIO • Grupo del servidor del RADIO: Seleccionar uno • Por default VLAN de SSID: Incorporar el nombre • Perfil de radio: Seleccionar uno
Instalar un VLAN para VoWIP en los switches de RoamAbout	1. Opción de Barra de herramientas: Seleccionar La Configuración. 2. Organizador del panel: Ampliar el switch de RoamAbout. 3. Ampliar el sistema 4. Click en VLANs	Para crear el perfil de servicio: • VLAN nombre: introducir nombre • Nombre de SSID: Incorporar el nombre • Modo de seguridad: Seleccionar WPA (y de select WEP dinámico) • Tipo de cifrado: Utilizar TKIP • Tipo de EAP: Utilizar el servidor externo del RADIO

Tabla 3.1 asignación de tareas

Resumen.

La lista siguiente resume los campos seleccionados o los artículos de la configuración incorporados para configurar el acceso del empleado:

1. Crear un perfil de radio:

a) Para crear el perfil de radio, incorporar RadioProfile1 como el nombre del perfil de radio.

b) Click finish

2. Configurar el servidor RADUIS

a) Configurar el servidor del RADIO para el uso 802.11. el método recomendado de EAP, PEAP + MS-CHAP.

b) Instalar cada switch de RoamAbout como cliente del RADIO.

c) Definir cualquier cualidad vendedor-especifica deseada de Enterasys (VSAs).

d) Configurar cada expediente del usuario con cualquier cualidad del VLAN-Nombre o el Tunel-Privado-Grupo-Identificación del RADIO.

e) Configurar las reglas de la autentificación 802.11.

3. Configuración del RADIO en RASM:

a) Para crear RADIUS, incorporar sg1 como el nombre del servidor, la dirección IP del servidor, y la llave permiten que el wizard cree el grupo del servidor y coloque el servidor en él para usuario.

b) Click en finish

Crear un perfil del servicio para el servicio 802.11.

a) Para el 802.11 del perfil, verificar después e inscribir a Secure-802.11-Employees como el nombre del perfil del servicio y a empleados como el SSID. Click en Después.

b) Seleccionar WPA y quite WEP dinámico. Click en Después.

c) Dejar como TKIP permitido. Click en Después.

d) Asegurarse de que el servidor externo del RADIO está permitido, seleccionar el grupo del servidor del RADIO, y agregar, click en después.

e) Incorporar el vlan-mkt por default VLAN para utilizar si el VLAN no es asignado por la autorización de RADIUS. Click en Después.

f) Seleccionar RadioProfile1 y click en agregar. Seleccionar el defecto y el click en quitar.

g) Click en finish

Instalación de una VLAN en los switches RoamAbout.

a) Para crear la VLAN, incorporar el vlan-mkt como el nombre de VLAN.

b) Click en después. Seleccionar los puertos de VLAN. Se teclea agregar para compartirlos con el otros VLANs o para moverse. Para utilizarlos exclusivamente en este VLAN. Si se tecleo agrega, después se selecciona la etiqueta.

c) Click en finish

Ejemplo: Configuración de Acceso a Empleado.

Las secciones siguientes proporcionan los pasos detallados requeridos para configurar el ejemplo de los servicios del empleado.

- Crear un perfil de radio.
- Configurar Los Servidores del RADIO.
- Crear un perfil del servicio para el acceso de 802.1 X.
- Instalación de VLANs en los switches de RoamAbout.

En general, estos mismos pasos también se utilizan para configurar otros servicios. Se puede referir a esta sección, usando la lista sumaria o la tabla de la tarea, con las opciones de la configuración los servicios del acceso del huésped o configuración del servicio sin hilos del IP del excedente de la voz.

Crear un perfil de radio.

La configuración de un perfil de radio permite fijar las cualidades que se aplican a los radios múltiples. Más bien que configurando cada radio individualmente, aplicar un perfil de radio a los radios múltiples. Los perfiles del servicio traz para radiar perfiles.

El perfil de radio puede contener ajustes Auto-Tuning y IEEE del RF 802.11 ajustes que controlen cómo se reciben y se transmiten los datos.

- Necesidad del APs (y por lo tanto, radios) de ser agregado a RASM después de crear un perfil de radio.

Para crear un perfil de radio en RASM:

Entrar al programa RoamAbout y seleccionar next para dar paso a lo que será la configuración.

En la figura 3.1 se muestra la pantalla inicial del programa en el cual se configuran los radios.

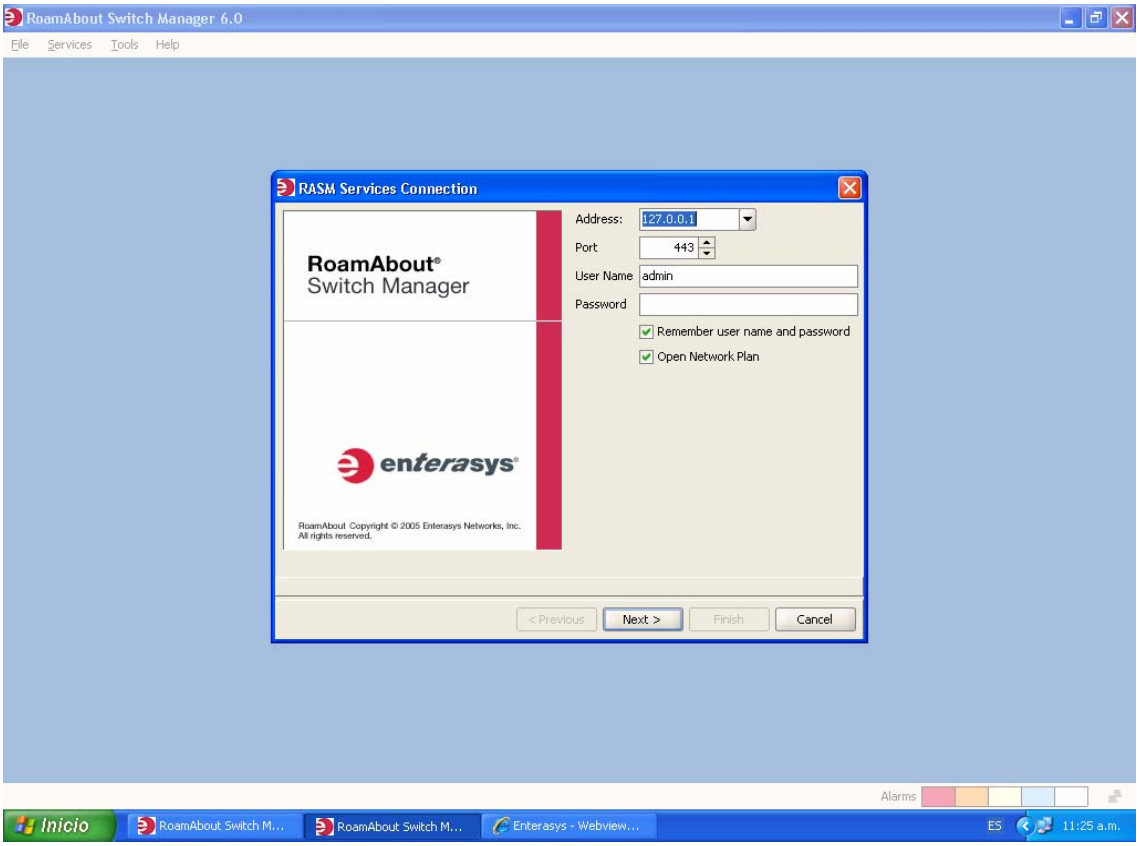


Fig. 3.1 Esquema de entrada al programa de configuración

1. Se selecciona la configuración en la barra de herramientas.

En la figura 3.2, se muestra la pantalla del primer paso que se debe dar para seguir paso a paso la configuración.

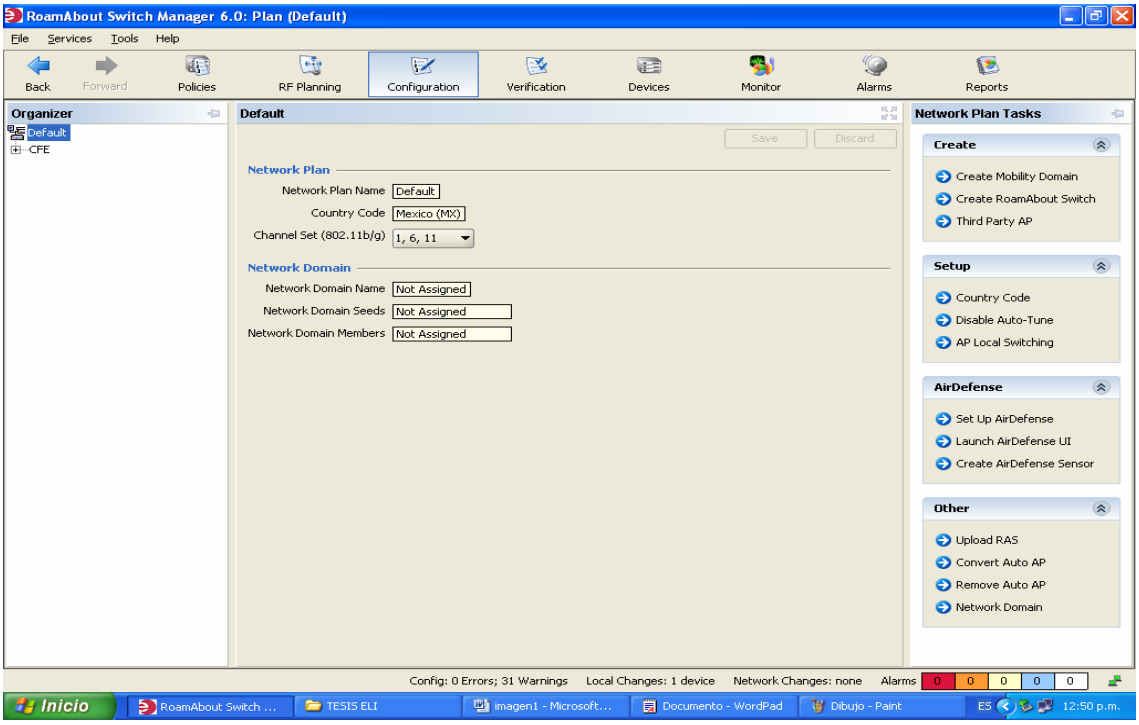


Fig. 3.2 Esquema de configuración

2. En el panel del organizador, ampliar el se RoamAbout con la selección de la instrucción Puntos de acceso. En la figura 3.3 se muestra los acces point que están conectados.

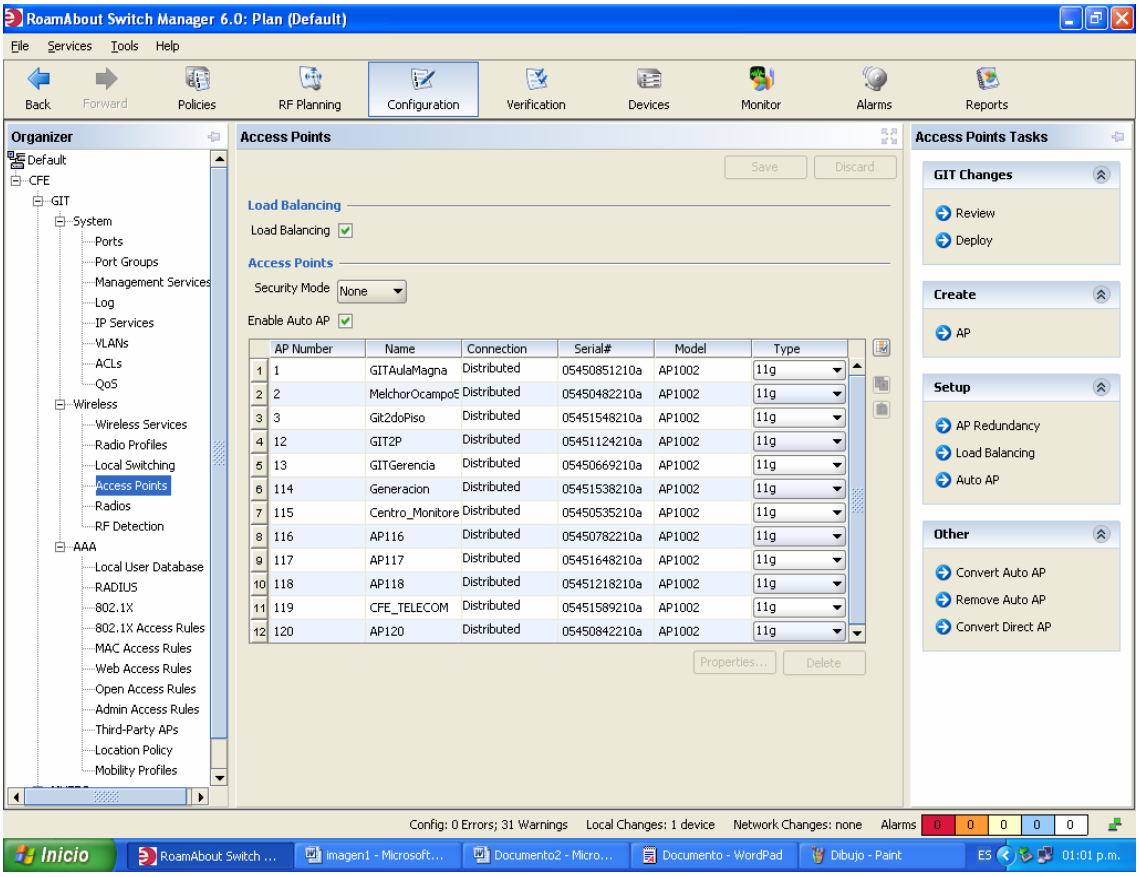


Fig. 3.3 Esquema de configuración de los Puntos de acceso

3. Se selecciona perfiles de radio.

4. En el panel de la lista de la tarea, seleccionar el perfil de radio. Exhiben el perfil del radio a crear.

5. Incorporar el nombre del perfil de radio, después click en después.

En la figura 3.4 nos despliega la pantalla en donde se debe poner la asignación de dirección IP, así como algunas descripciones requeridas.

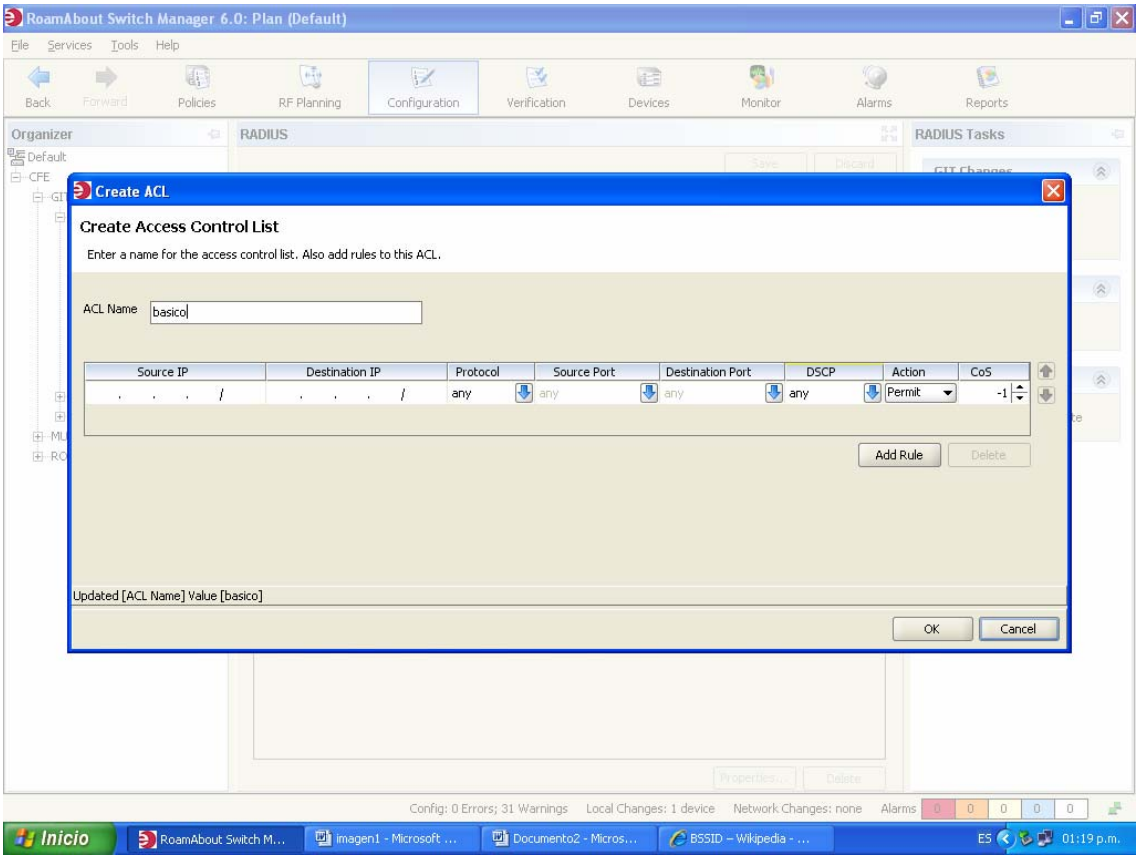


Fig. 3.4 Esquema de direccionamiento de IP

6. Si el APs se configura en ese momento, se seleccionan los radios para mapear al perfil de cada uno de ellos, entonces se puede ver el movimiento.

El encargado del switch de RoamAbout quita las radios del perfil de radio que están adentro y las coloca en el nuevo perfil.

Si no se ha configurado el APs el encargado del switch de RoamAbout todavía, no se enumera ningunas radios.

7. Click en finish para salvar los cambios y cerrar.

En la figura 3.5 muestra los radios configurados y dados de alta en cada edificio o cada switches.

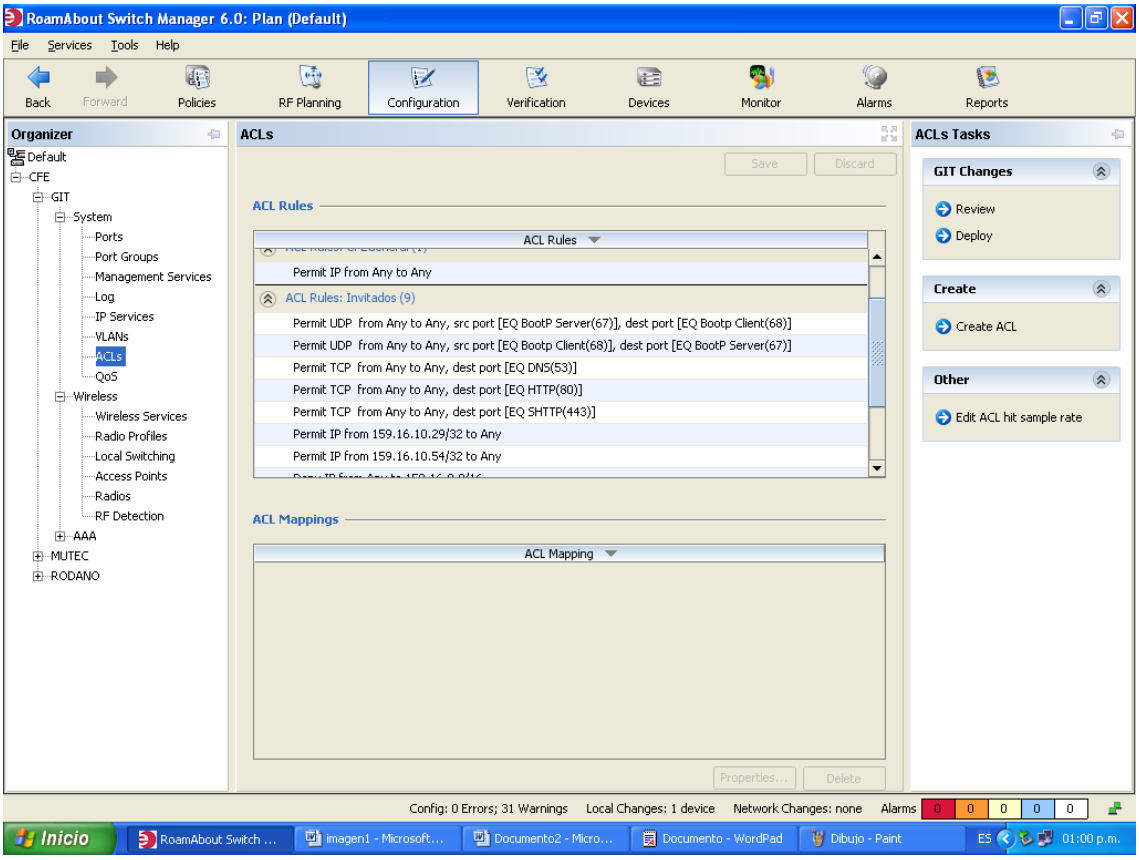


Fig. 3.5 Esquema de localización de puertos

Configuración de los Servidores del RADIO.

La autentificación alejada Dial-En el servicio del usuario (RADIO) es un protocolo de la seguridad del servidor de cliente que proporciona la autentificación, la autorización, y la contabilidad para los usuarios y los dispositivos de la red. Un servidor del RADIO almacena los perfiles de usuario, que incluyen usar nombres, contraseñas, y otras cualidades del usuario.

Se deben realizar las siguientes acciones para configurar los servidores del RADIO:

- Configure las cualidades del servidor del RADIO en RASM.
- Configure las cualidades en el servidor del RADIO.

Configuración el servidor del RADIO en RASM.

Para configurar el RADIO en RASM, se definen los grupos del servidor del RADIO (nombrados los sistemas de servidores del RADIO). Se debe crear por lo menos un grupo del servidor. Los grupos del servidor del RADIO pueden autenticar administradores y a usuarios de la red.

Para configurar el servidor del RADIO en RASM:

- Seleccionar la configuración en la barra de herramientas.
- En el panel del organizador, ampliar el switch de RoamAbout en el cual se estará configurando el servicio.
- Ampliar el AAA, después seleccionar el RADIO.
- En el panel de la lista de la tarea, seleccionar el servidor del RADIO.
- Introducir el nombre, el IP address, y la llave. Click en después.

En la figura 3.6 se ilustra la pantalla donde se da la dirección IP a cada radio y se selecciona el grupo o edificio al cual va a pertenecer

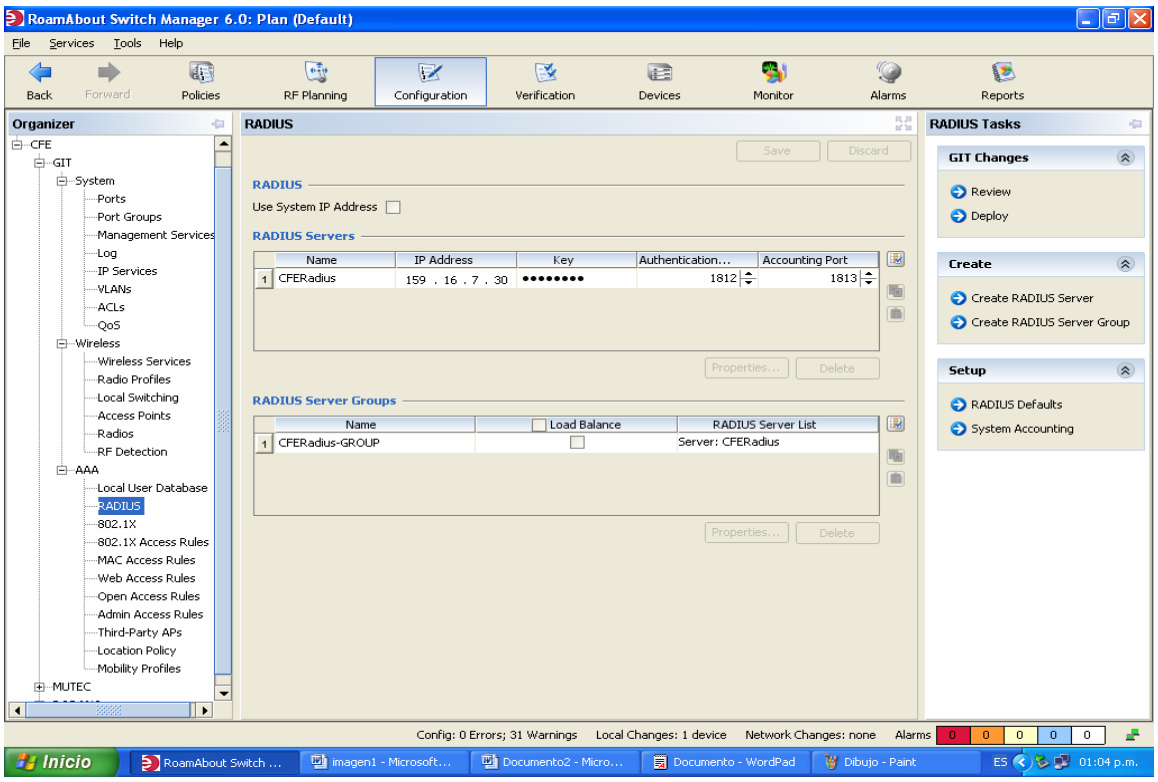


Fig. 3.6 Pantalla del direccionamiento de IP

RASM sugiere el nombre de un grupo del servidor en el cual colocar el servidor. El grupo del servidor se requiere porque las reglas del AAA refieren a grupos del servidor, no a los servidores individuales.

- Click en finish para guardar el servidor y para crear el grupo del servidor. El nuevo servidor y grupo aparecen en el panel control.

Configurar las cualidades en el servidor del RADIO.

RASM se puede autentificar a los usuarios que se configuran en la base de datos local o en los servidores del RADIO. Para configurar los servicios para este empleado tenga acceso al ejemplo, configuran el servidor del RADIO como sigue:

1.- Configurar el servidor del RADIO para realizar 802.11 usando el método recomendado de EAP PEAP + MSCHAPV2.

2.- Instalar cada switch de RoamAbout como cliente del RADIO.

3.- Definir cualquier cualidad vendedor-especifica deseada de Enterasys (VSAs) en el diccionario del servidor del RADIO.

Las cualidades creadas por Enterasys Networks se encajan según el procedimiento recomendado en RFC 2865, fijada a 14525.

4.- Configurar cada expediente del usuario con reglas de la autorización (username y contraseña) y con la cualidad del Vlan-Nombre (Enterasys VSA) o la Tunel-Privado-Grupo-Identificación del RADIO para asignar a usuarios a VLANs. Otras cualidades son opcionales.

Creación de un perfil del servicio para el acceso de 802.11.

Un perfil del servicio contiene la configuración para el servicio que se desea ofrecer, por ejemplo el acceso del empleado, el acceso del huésped, o VoWIP.

Para crear un perfil del servicio 802.11:

1. Seleccionar la configuración en la barra de herramientas.
2. En el panel del organizador, ampliar el interruptor de RoamAbout.

3. Ampliar la radio, después seleccionar los servicios sin hilos.
4. En el panel de la lista de la tarea, seleccionar el perfil del servicio 802.11.
5. Click en continuar
6. Cambie el nombre del perfil del servicio a Secure-802.11-Employees, y utilice el mismo nombre para el SSID.
7. Click en siguiente. Seleccionar WPA y de select WEP dinámico.
8. Click en siguiente.
9. Click en siguiente. Se Deja el servidor externo del RADIO seleccionado como el tipo de EAP.
10. Seleccionar el grupo del servidor del RADIO en los grupos disponibles del servidor del RADIO.
11. Click en siguiente. Introducir el vlan-mkt en la VLAN.
12. Click en siguiente. Seleccionar RadioProfile1 en la lista disponible de los perfiles del radio.
13. Click en finish.

3.3 Necesidades VLAN (red de área Local Virtual).

Una red de área local (LAN) se define como una red de computadoras localizada en un área geográfica determinada, como puede ser una escuela o empresa. Algunos de los principales problemas asociados con este tipo de red son el no contar con confidencialidad entre los usuarios de la LAN así como el hecho de no aprovechar correctamente el ancho de banda al tener a todas las estaciones de trabajo en un mismo dominio de colisión.

Una VLAN consiste en una red de computadoras que se comportan como si estuviesen conectados al mismo cable, aunque en realidad pueden estar conectados físicamente a diferentes segmentos de una red de área local. Una de las mayores ventajas de este tipo de redes, es que una computadora puede ser

trasladada físicamente permaneciendo en la misma VLAN sin ningún tipo de reconfiguración.

La red virtual, permite separar la visión lógica de la red de su estructura física; esto es, que si un departamento se desplaza a un edificio a través del campus, este cambio físico será transparente gracias a la visión lógica de la red virtual. Del mismo modo, se reduce notablemente el tiempo y los datos asociados con los movimientos físicos, permitiendo que la red mantenga su estructura lógica y que los centros de cableado permanezcan seguros y a salvo de interrupciones

3.3.1 Características

Los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes concentradores de la misma. • Los usuarios pueden, así, "moverse" a través de la red, manteniendo su pertenencia al grupo de trabajo lógico. Al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios. • Al ubicar a los usuarios dentro de distintos segmentos de red, es posible situar puentes y routers entre ellos, separando segmentos con diferentes topologías y protocolos.

3.3.2 Instalación de VLANs en los switches RoamAbout.

Los radios de RoamAbout en un dominio de la movilidad contienen el tráfico de un usuario dentro del VLAN a el cual se asigna al usuario. Por ejemplo, si se asigna a usuario al rojo de VLAN, los interruptores de RoamAbout en el dominio de la movilidad contienen el tráfico del usuario dentro del rojo de VLAN configurado en los interruptores. Las VLANs que se configura para la radio de la ayuda de los sistemas del servicio usuario- no sirven como gerencia VLANs.

Si un interruptor de RoamAbout es conectado con la red por solamente un subnet del IP, el interruptor de RoamAbout debe tener por lo menos un VLAN configurado. Opcionalmente, cada VLAN puede tener su propio IP address. Sin embargo, ningunas dos direcciones del IP en el interruptor pueden pertenecer al mismo subnet del IP. Se deben definir a usuario VLANs en por lo menos un interruptor de RoamAbout dentro del dominio de la movilidad.

Se puede configurar el protocolo STP en un VLAN. STP se utiliza para mantener una red lazo-libre; de está manera reconocerá un lazo en la topología y bloqueará unas o más trayectorias redundantes, creando una trayectoria lazo-libre.

Para instalar un VLAN en un RoamAbout cambiar:

3. Seleccionar la configuración en la barra de herramientas.
4. En el panel del organizador, ampliar el interruptor de RoamAbout.
5. Ampliar el sistema, después seleccionar VLANs.
6. En el panel de la lista de la tarea, seleccionar VLAN.

En cualquier caso, la mayor debilidad de cualquier sistema informático no es la tecnología, sino sus usuarios. De nada sirve un sistema de cifrado completamente seguro si no se activa, si sus claves son evidentes o si se dejan con la configuración por defecto.

3.4.1 Seguridad WIFI: WEP (WIRED EQUIVALENT PRIVACY)

Desde un comienzo se conocían las debilidades en cuanto a Seguridad Informática de las Redes Inalámbricas WIFI. Por este motivo se incluyó en el

estándar 802.11b un mecanismo de seguridad que permita encriptar la comunicación entre los diversos elementos de una red inalámbrica WIFI. Esta protección se denominó WEP (Wired Equivalent Privacy). En español sería algo así como "Privacidad equivalente a la de una red cableada". El protocolo WEP se basa en el algoritmo de encriptación RC4.

La idea de los promotores del estándar 802.11b consistía en encriptar el tráfico entre Puntos de Acceso y estaciones móviles y compensar así la falta de seguridad que se obtiene al enviar la información por un medio compartido como es el aire. Es así como, todos los Puntos de Acceso y dispositivos WIFI incluyen la opción de encriptar las transmisiones con el Protocolo de Encriptación WEP.

Brevemente diremos que hay que establecer una clave secreta en el Punto de Acceso, que es compartida con los clientes WIFI. Con esta clave, con el algoritmo RC4 y con un Vector de Inicialización (IV) se realiza la encriptación de los datos transmitidos por Radio Frecuencia.

Dentro del programa de RoamAbout se selecciona en el área de configuración, se toma la opción que indica que es wíreless y en el subraya *wíreless service* donde muestra una pequeña pantalla en la cual indica cuantos y con que nombres están dados de alta las formas de acceso a la red;

En la figura 3.7 muestra la pantalla en la cual nos da la opción de elegir si queremos proteger alguna de nuestras entradas a la red por medio de un encriptación.

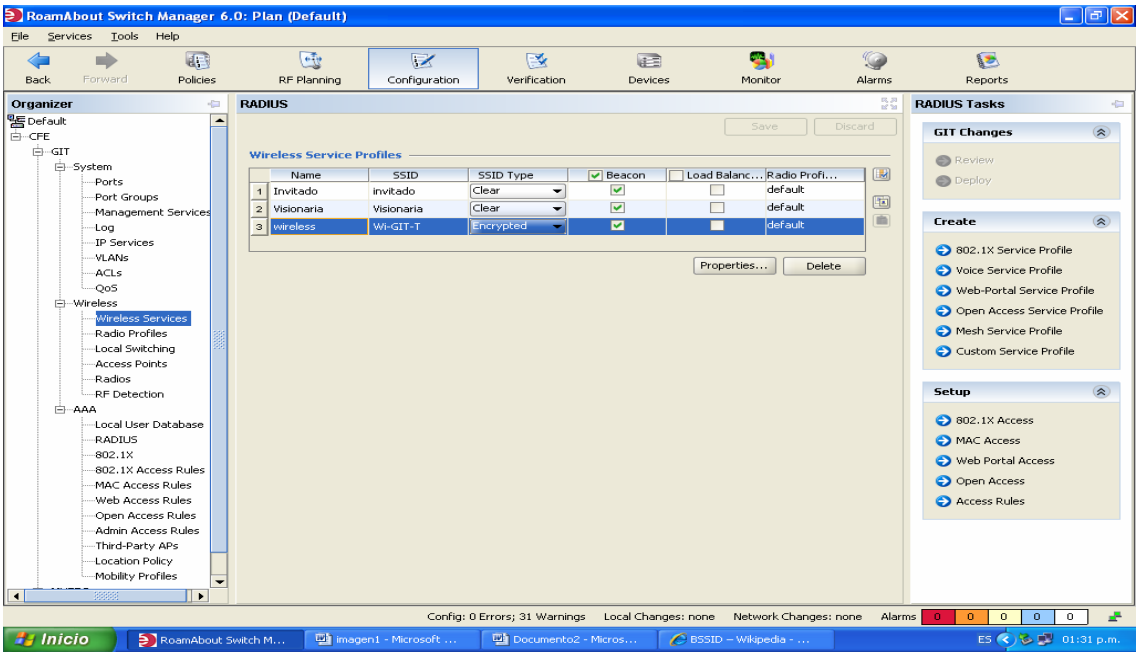


Fig. 3.7 Pantalla de selección de seguridad

En este caso muestra los tres perfiles que se definieron para el acceso a la red de CFE, las cuales fueron asignadas o nombradas de la siguiente forma: la primera es la de invitado, la segunda es la de visionario, y la tercera es la de wireless que esta ultima es por la cual podrán accesar los usuarios de CFE, pero se va a proteger de la siguiente manera:

En la figura 3.8 se despliega el menú donde vamo0s a escoger nuestro tipo de encriptación.

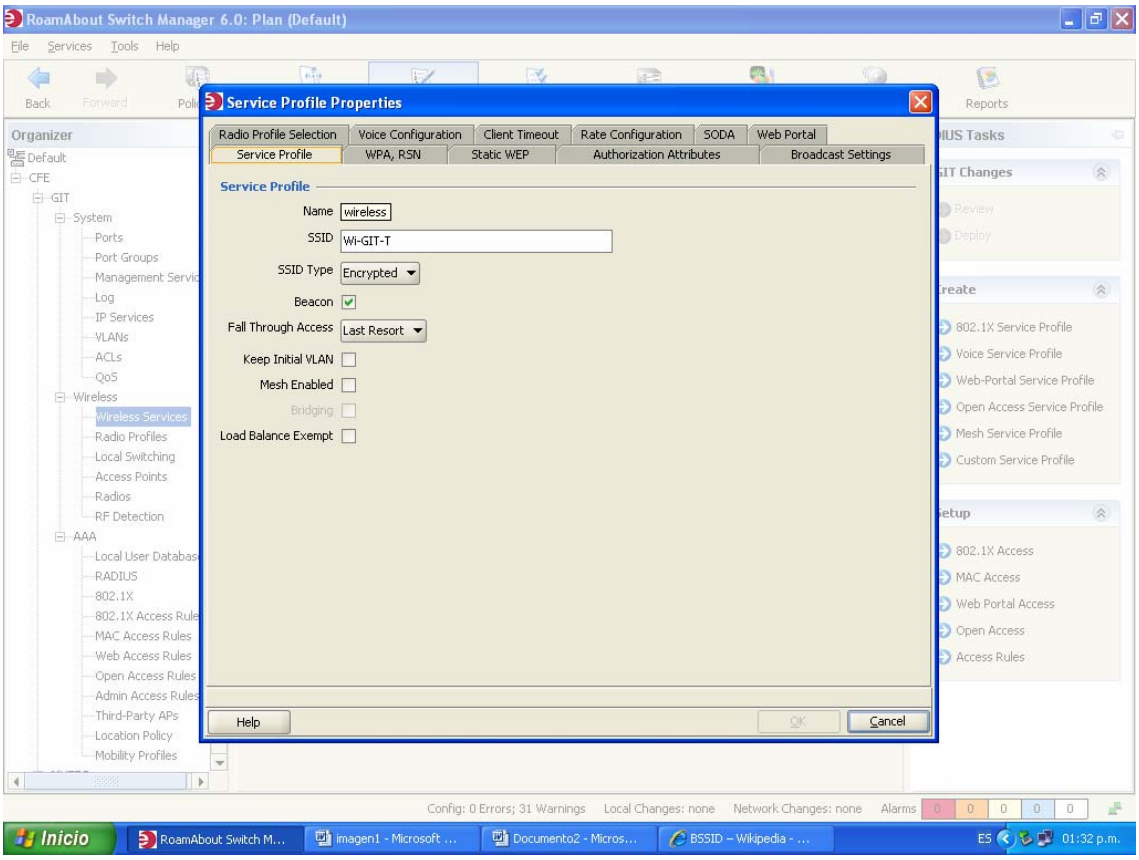


Fig. 3.8 Pantalla de encriptación.

Se selecciona wíreless de tal forma que se pueda entrar a las propiedades de esta, de esta forma da una nueva pantalla el la cual indica diferentes opciones de tipo de encryptación dependiendo la que el usuario desee es la que se selecciona, en este caso se utiliza la encriptación tipo WEP

Se selecciona la opción Static WEP, la cual despliega una serie de líneas en las que pide la clave que se agregara para tener acceso a la red llamada Wíreless.

Aquí permite agregar una clave de diez caracteres hexadecimales, con esto indica que solo las personas que sepan la clave serán las que puedan entrar a Internet e Intranet de la empresa esto para mayor seguridad de la misma.

En la fig. 3.9 se muestra el formato que se da para hacer la encriptación así como la pantalla para ingresar la clave o llave para entrar a la red.

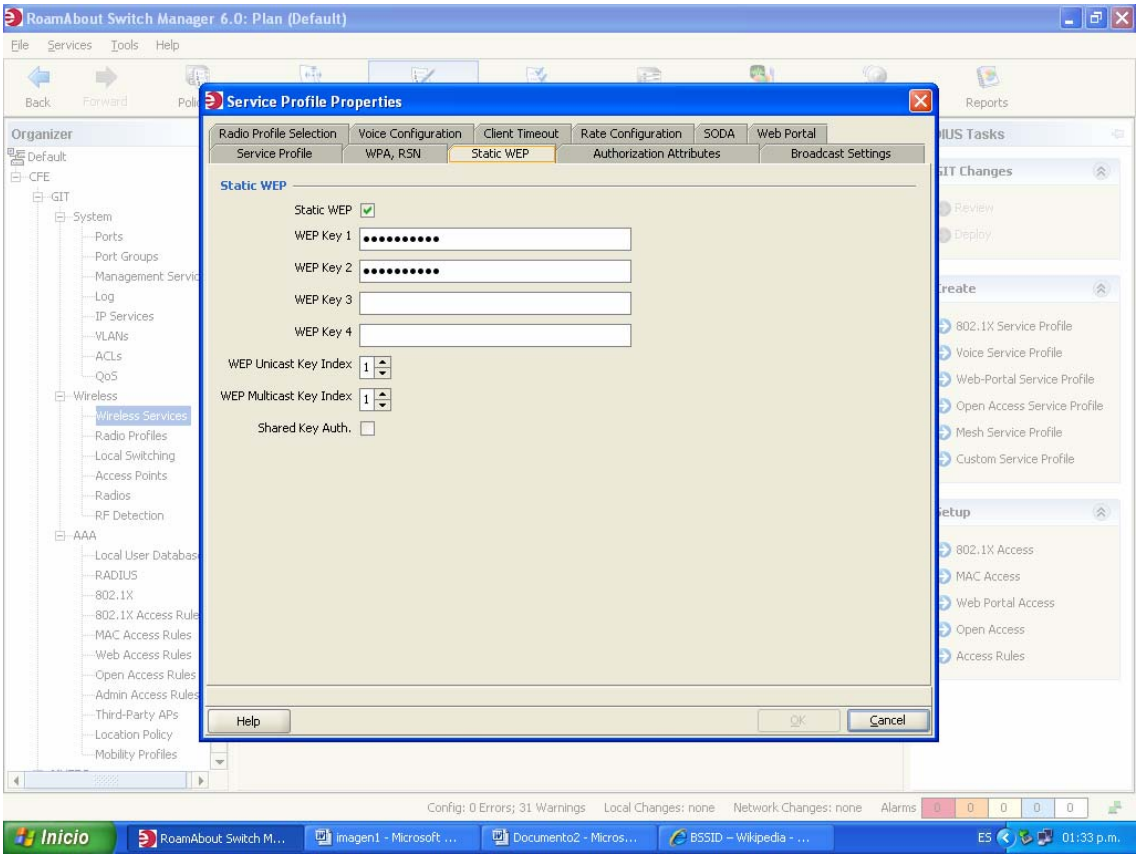


Fig. 3.9 Formato de encriptación

Con esta medida se pretende que la seguridad en la empresa sea mayor, ya que desde el punto base del registro de cada uno de los dispositivos móviles, serán monitoreados los radios en función.

A medida que fue aumentando la difusión de las Redes Inalámbricas WIFI, en Comisión Federal de Electricidad, se fueron detectando graves problemas de

seguridad informática en el Protocolo de Encryptación WEP, lo que generó hace unos años muy mala imagen a las redes inalámbricas WIFI.

Debilidades del Protocolo WEP

1. El Vector de Inicialización IV, es demasiado corto pues tiene 24 bits y esto ocasiona que en redes inalámbricas WIFI con mucho tráfico se repita cada tanto.
2. Hay algunos dispositivos clientes (tarjetas, USB) muy simples que el primer IV que generan es cero y luego 1 y así sucesivamente.
3. Las claves que se utilizan son estáticas y se deben cambiar manualmente. No es fácil modificarlas frecuentemente.

No tiene un sistema de control de secuencia de paquetes. Varios paquetes de una comunicación pueden ser robados o modificados sin que se sepa.

Esta situación generó la aparición de múltiples aplicaciones capaces de crackear la seguridad WEP en poco tiempo. Según la capacidad de los equipos utilizados y la habilidad del hacker y el tráfico de la red inalámbrica WIFI, se puede tardar desde 15 minutos a un par de horas en descifrar una clave WEP. Además del Airsnort mencionado en el artículo recomendado, están el WEPCrack, el NetStumbler.

Posteriormente de que están configurados cada uno de los radios, se procede a instalarse en las salas requeridas, con la ayuda de un cable UTP categoría 6 rematado con conectores RJ45 en cada extremo, uno va al radio y el otro extremo al Switch, esté pasa por medio de una escalerilla donde se encuentran los cables de red al closet de comunicaciones, de igual manera el radio debe estar conectado a una Terminal de energía eléctrica para poder dar el servicio de forma correcta.

CAPITULO IV

RESULTADOS

CAPITULO IV

4.1 RESPUESTA DEL EQUIPO.

Dentro de los cuartos de comunicaciones se pueden observar los equipos con que se cuenta, haciendo mención que existen problemas con el cableado de la empresa. Y los cuales no permitían identificar los puntos de red de los usuarios.

En las figuras 4.1 y 4.2 se muestran como se encuentran algunos closet de comunicaciones en los cuales se instalaron los radios.

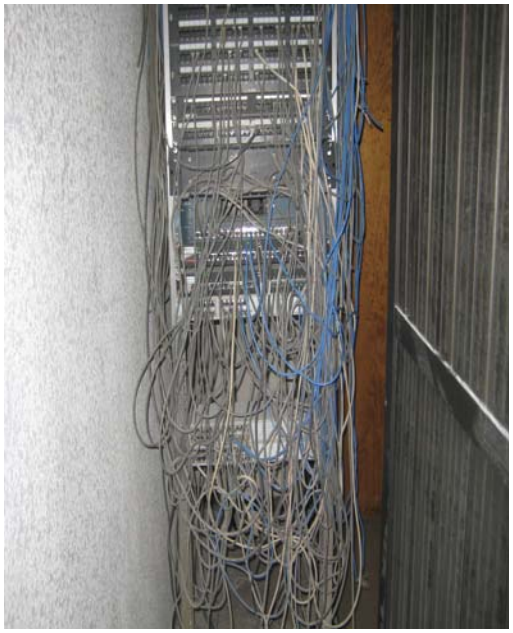


Fig. 4.1 Equipo de Comunicaciones Rodano 2º piso

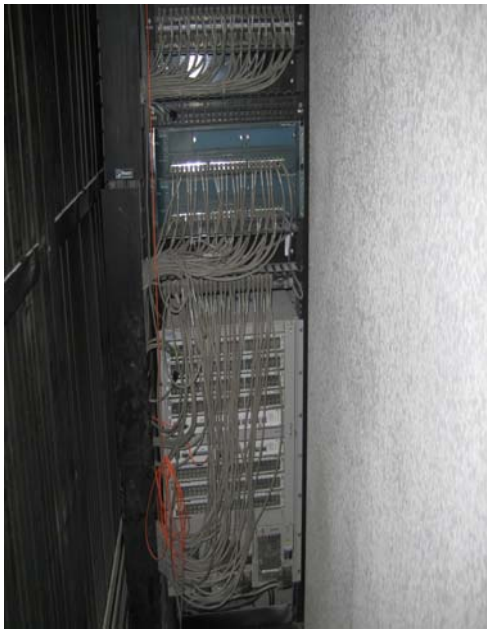


Fig. 4.2 Equipo de Comuns. Reforma PH

Así también se están dando modificaciones de equipos viejos por nuevos, se están emigrado todos los servicios que habían en Hub, Switches 3Com, Enterasys, Cisco, etc., a un equipo nuevo de la marca Nortel. Y los resultados obtenidos son favorables, ya que la finalidad de esta sustitución de equipos es para estar a la vanguardia día con día y competir a gran escala.

En las figuras 4.3 y 4.4 muestra la forma en la que quedaron algunos closet de comunicación al ser ordenado de la forma correcta para la instalación de los radios.

Fig.4.3 Equipo de Coms. Reforma 5º piso

Fig. 4.4 Equipo Nortel

Con los pequeños cambios que se han realizado en los cuartos de comunicaciones a permitido facilitar para la instalación del proyecto, así como para dar servicios requeridos en determinas áreas. Del tal forma que el proyecto, no solo va ha servir para la aplicación de la red inalámbrica, sino también, para el mejoramiento de las instalaciones.

Actualmente en Comisión Federal de Electricidad tuvo la necesidad de instalar radios de abajo alcance usando la tecnología inalámbrica WI-FI, que es un paso importante para la empresa contar con este tipo de servicio.

Ya que se requirió principalmente en las áreas de conferencias, juntas y auditorios, donde se pueden realizar algunas conexiones simultáneas y poder interactuar directamente con algún evento o servicio.

De esta manera las salas u oficias donde era requerido la instalación de los radios, realizaron un reporte de solicitud al área llamada “Mesa de ayuda”, la cual paso los reportes a la gerencia del área de comunicaciones, y en una reunión del personal de dicha área se llego a la conclusión que instalar dichos radios ayudaría a facilitar el trabajo y tener mayor calidad de servicio.

Esto consistió en hacer una junta con el personal del área de redes para plantear el problema, se hizo un proyecto piloto el cual consistía en la aplicación de la tecnología en solo tres edificios de la empresa estos son: GIT (Gerencia de Telecomunicaciones e Informática), el edificio de Ródano Nº 14 y Reforma Nº164.

En el diagrama de la empresa consiste en que, en cada uno de los tres edificios mencionados, existe una oficina de redes, donde se cuenta con equipo y herramientas para la solución de problemas resultantes, sin embargo en el edificio de la GIT, es donde se encuentra equipo capaz de poder verificar ya dar servicio, no solo a los edificios del área metropolitana, sino también puede estar comunicados con los distintos edificios o puntos centrales de cada estado de la republica mexicana.

En este edificio se controla la fibra óptica, que alimenta a los diferentes edificios, así como también es la que se encarga de llevar a cabo la transmisión de las videoconferencias, y algunos otros servicios, donde se cuenta con personal capacitado para poder manejar los equipos.

Básicamente el personal de este edificio encargado de manipular el equipo, son Ingenieros, y tienen una constante capacitación en cuanto a tecnologías nuevas e innovaciones de equipos.

Pues bien dentro de el edificio de la GIT, existe un monitor donde se puede observar los cambios que haya con los equipos, así como se puede observar, cuando se están utilizando los radios y en que edificio los utilizaron.

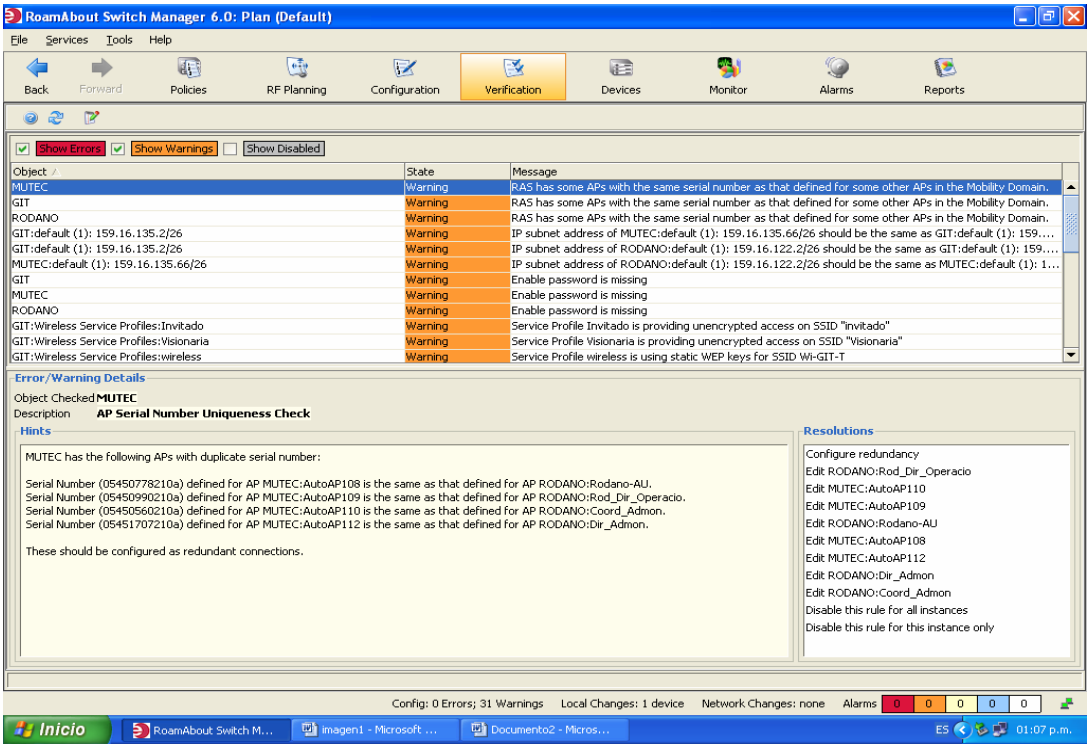
En este mismo edificio es donde se lleva a cabo la configuración de los radios y se dan de alta dentro de las direcciones IP, que la empresa tiene controladas, así se asegura el radio. Ya con la configuración, solo se dirige a los diferentes edificios a instalar el radio y verificar que funcione adecuadamente.

Las redes inalámbricas son útiles cuando los empleados necesitan acceder a la información desde distintos sitios o mantener una cierta movilidad. Éste sería el caso, por ejemplo, una reunión o conferencia en un auditorio de la empresa, donde se encuentran personal encargado de dar la conferencia, personal de la empresa, proveedores, invitados, etc., no tendrán el problema de buscar un punto de conexión sino que simplemente prenderán su maquina y se comunicaran por medio de la red inalámbrica de CFE.

Dentro de las instalaciones donde se ha colocado el equipo ha tenido una respuesta del 90% de calidad, respecto a algunas de las fallas que se han presentado, sin embargo a registrado una aceptación favorable, ya que en un principio existió un poco de incertidumbre con respecto a la respuesta de los radios, puesto que la tecnología que utiliza es nueva para muchos.

Sin embargo es grato verificar servicios de calidad para el usuario.

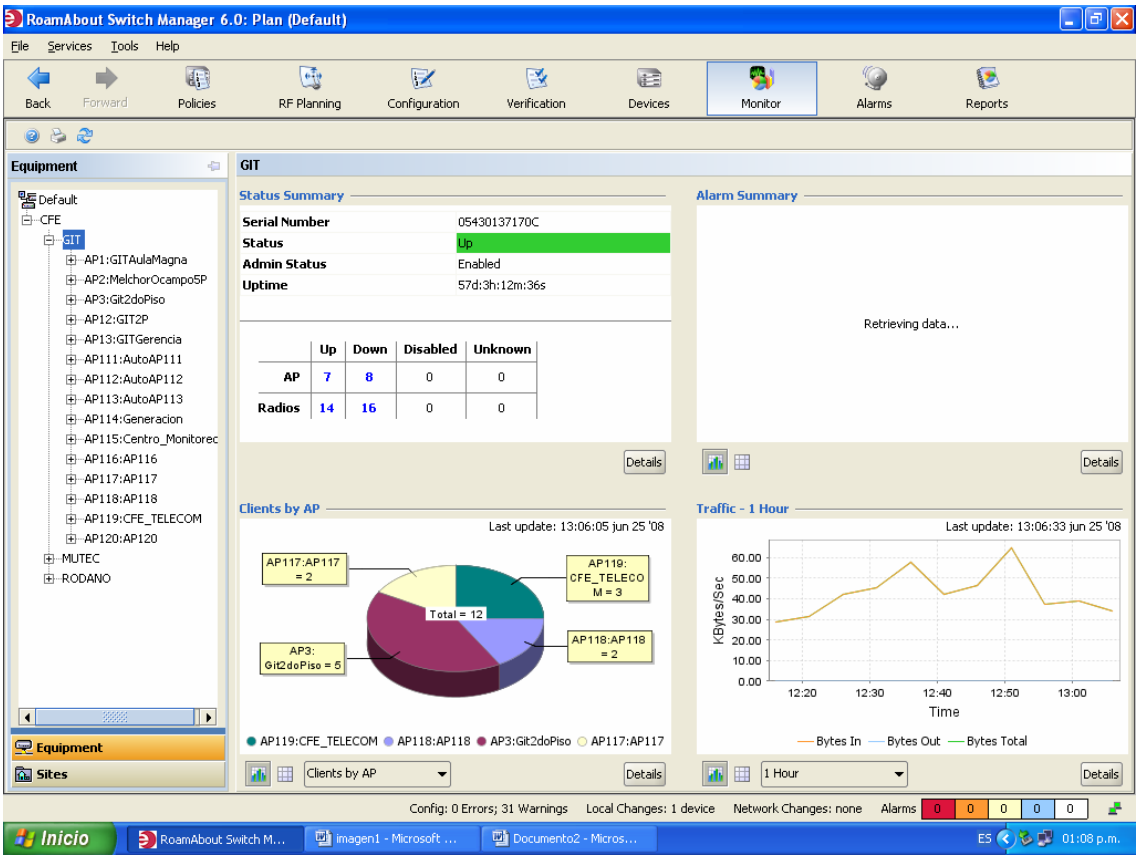
En la figura 4.5 despliega la verificación de los servicios que se están brindando.



4.5 Verificación de los servicios

Monitoreo de cada uno de los radios en la imagen se presenta cuantos usuarios están utilizando el radio dirigido en ese lugar

En la figura 4.6 muestra en una forma grafica el registro de los servicios utilizados y por cuantos usuarios.



4.6 Registros de los servicios

4.2 Respuesta de los usuarios con la tecnología implantada.

Los usuarios del edificio de Rodano opinan al respecto de la tecnología puesto que han sido instalados 12 radios en diferentes pisos.

Por ejemplo, en la sala 504 que es la Dirección de Administración donde se encuentra la Licenciada Juanita Solorio y el Licenciado Oscar Borja. Quienes comentan que no ha existido ningún problema con la red inalámbrica, que el funcionamiento que dan los radios a sido de un 100% de calidad, que solo hubo un día donde se presentaron fallas ya que la señal se cortaba y era interrumpida pero fue por un lapso de 5 a 10 minutos y todo regreso con total normalidad al funcionamiento. Esto se debió a una pequeña falla que se dio desde la oficina donde se manejan los equipos (Av. Don Manuelito GIT)

Otro de los comentarios con respecto a los radios en el piso 6 en las salas 602 y 603 que son de la Dirección de Operación, se presenta el problema de que existió un día completo fallas en la red puesto que, se interrumpía la señal fue por el mismo motivo que se presentaron las fallas.

PLANO DEL 6º PISO DE RODANO

En esta imagen (fig. 4.7) es de un plano de los pisos de CFE, el cual muestra como está diseñada la infraestructura de los pisos de Rodano donde se instalaron algunos radios

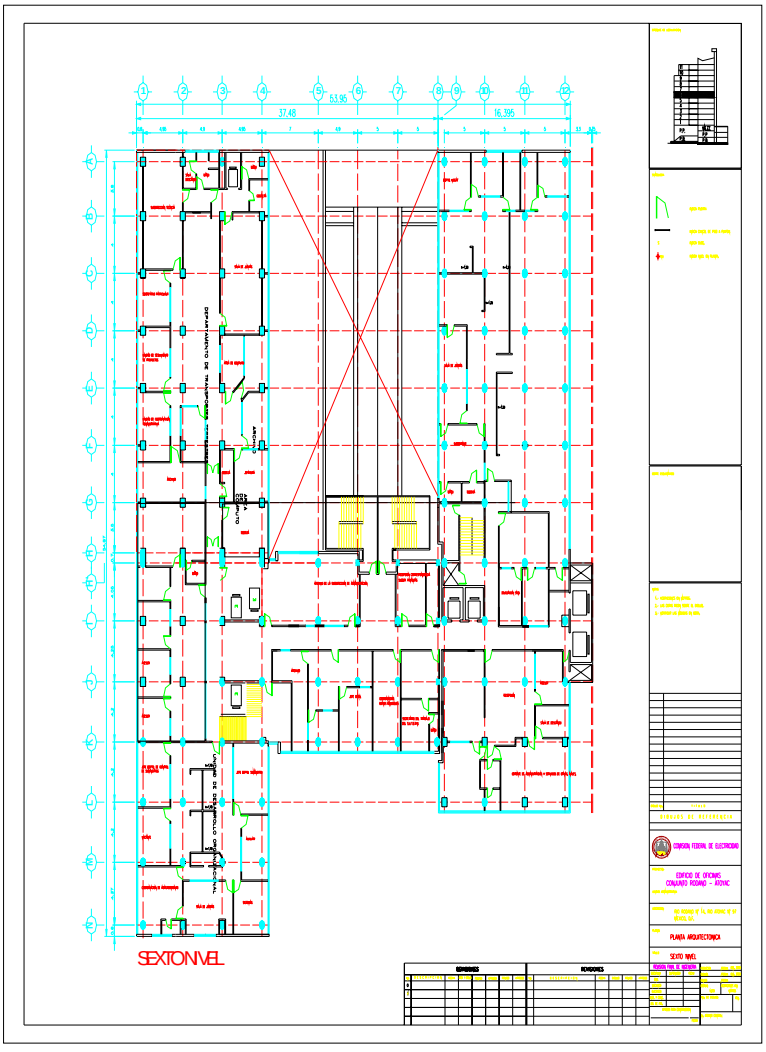


Fig. 4.7 Plano del piso 6º de Rodano

PLANO DEL 5º PISO DE REFORMA

En esta imagen (fig. 4.8) es de un plano de los pisos de CFE, el cual muestra como está diseñada la infraestructura de los pisos de Reforma donde se instalaron algunos radios.

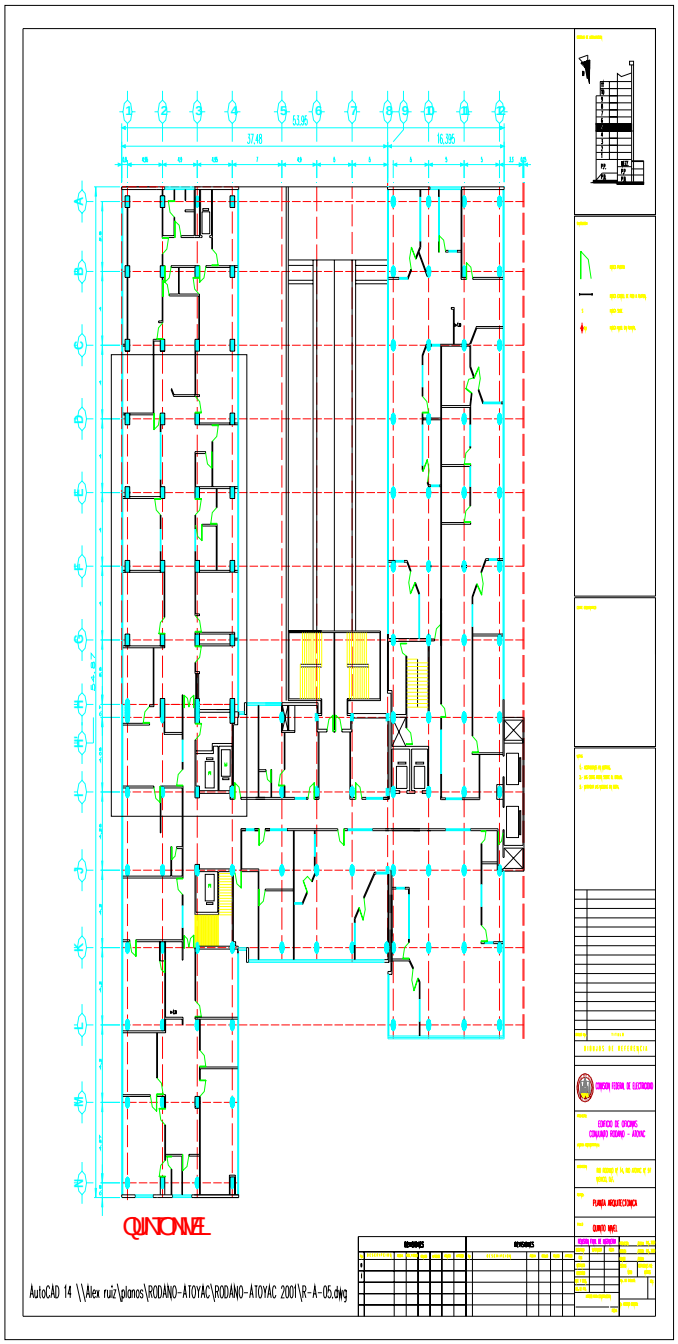


Fig. 4.8 Plano de Reforma 5º Piso

PLANO DEL 7º PISO DE RODANO

En esta imagen (fig. 4.8) es de un plano de los pisos de CFE, el cual muestra como está diseñada la infraestructura de los pisos de Rodano donde se instalaron algunos radios.

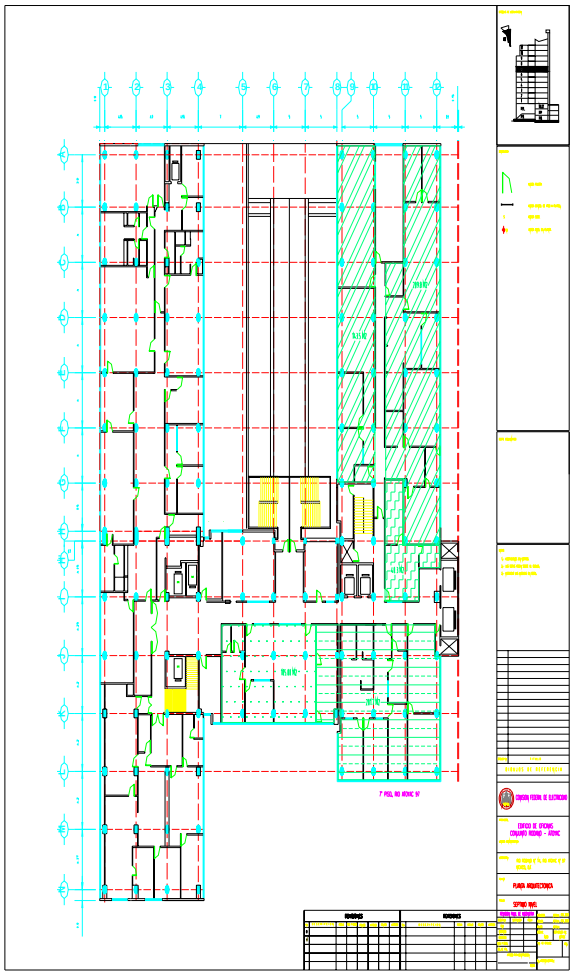


Fig. 4.9 Plano de Rodano piso 7.

4.3 Problemas resultantes

Algunos de los problemas que se han dado con respecto a los radios, se puede decir básicamente es que el personal en general usuarios de la red directa de CFE, tienen problemas para ingresar a lo que es Intranet, puesto como ya se menciono, que solo se tendrá acceso a dicha opción por medio de una clave que la misma empresa proporciona de 10 dígitos XXXXXXXXXX, el jefe de oficina o persona a cargo de determinada área no a proporcionado a todos los trabajadores dicha clave, sin embargo cada día se presenta más usuarios conectados por este medio, manifestando estar en total acuerdo y comodidad con la respuesta que da el servicio.

En el desarrollo del proyecto uno de los factores más importantes que se pudo constatar es el problema existente que había en algunos cuartos de comunicaciones, los cuales mostraban que la estructura en la que estaban era de una forma incorrecta puesto que el tendido de cables no era la adecuada y eso imposibilitaba el realizar servicios adecuadamente.

Desde el punto de vista de la empresa, las redes inalámbricas son aplicables en cualquier campo de la industria donde exista la necesidad de utilizar un dispositivo informático, tener movilidad y permanecer en contacto en tiempo real con recursos informáticos dentro o fuera de la empresa.

Una red inalámbrica cubre las mismas funciones que las que proporcionan una red cableada. Por lo tanto se ha comprobado que dentro de la empresa se requería la instalación de una red inalámbrica, que satisficiera algunas necesidades que los usuarios tenían.

Así mismo existen diferentes salas u oficinas dentro de la empresa donde usualmente el personal necesita tener un acceso a la red pero en forma directa y no conectarse a un punto de red, ya que para facilidad de algún evento o servicio

dado, se requiere este servicio. Sin embargo no en todas las oficinas o salas se cuenta con dicho servicio, puesto que esta como proyecto piloto y dependiendo del resultado de esta aplicación se podrá instalar en las diferentes salas u oficinas requeridas.

Dentro de esta red se van a manejar dos perfiles, uno donde usuarios y proveedores que tengan acceso a la red, tanto a Internet como a Intranet, desde el equipo maestro, y otro donde podrán entrar invitados restringidos, los cuales solo tendrán acceso a Internet.

Es por eso que Comisión Federal de Electricidad, tiene la obligación y el interés de estar a la vanguardia en cuanto a tecnología de punta.

El proyecto en si, es un avance dentro de la empresa, ya que a dado grandes resultados en beneficio a los usuarios e invitados de tal, que han tenido la oportunidad de comparar el servicio.

Sin embargo la tecnología avanza día a día y eso trae como resultado una mayor necesidad de estar a la vanguardia, por esta razón es importante mencionar que la tecnología utilizada en este caso de los radios modelo RoamAbout RBT-1002 Wireless Puntos de acceso de la marca enterasys, utiliza el protocolo 802.11a, 802.11b y el 802.11g, es de suma importancia el decir que estos actúan por medio de un switch denominado RBT el cual tiene la capacidad de soportar a 25 radios conectados, para un mayor servicio.

Es importante mencionar que debido a la mascara de la red que utiliza cada radio puede dar servicio a 39 usuarios en excelentes respuesta en condiciones iniciales a una velocidad de 54 Mbps, ya que pertenecen a la categoría 802.11g y la categoría 802.11n esta puede alcanzar una velocidad de 300Mbps.

Los equipos con los que se esta trabajando están diseñados y configurados para ambas tecnologías, esto es como se mociono la categoría 802.11n alcanza una mayor velocidad, está en la actualidad no se esta utilizando por la razón que las tarjetas de las maquinas no están aun diseñadas para soportar dicha velocidad, entonces seria una aplicación sin sentido puesto que la velocidad proporcionada por los radios instalados es de 54Mbps es buena en el servicio y para los requerimientos establecidos.

Se necesita aún por trabajar para mejorar los servicios, pero día a día el personal trabaja conjuntamente para que sea esto posible.

Para ver las ventajas de las redes inalámbricas, simplemente hay que pensar en la alternativa actual: utilizar formularios de papel, copiar del papel al computadora, manejar información impresa no actualizada, tener que moverse para conseguir acceder a la información de la empresa, etc. esto trae consigo la duplicación de trabajo, aumentar los tiempos de respuesta, introducir errores de interpretación de escritura manual, manejar información no actualizada, peder tiempo en desplazamientos innecesarios, etc.

Una conexión Inalámbrica puede mejorar grandemente el rendimiento y eficiencia de muchos puestos de trabajo: facilita la movilidad, elimina el papeleo, disminuye los errores, reduce los costos de gestión, elimina el estorboso e incomodo cableado, reduce costos de instalación, acerca la empresa al trabajador y aumenta su eficiencia.

CAPITULO V

CONCLUSIONES

CAPITULO V

CONCLUSIONES

El proyecto se realizó correctamente cubriendo las necesidades que presentaba la empresa Comisión Federal de Electricidad, de esta forma se logró alcanzar los objetivos establecidos e indirectamente la solución de problemas no previstos en el desarrollo del proceso.

Se realizó un ordenamiento en los cuartos de comunicación para trabajar en mejores condiciones, se cubrió la necesidad presentada en salas de juntas, auditorios, y diferentes oficinas, donde ahora ya se cuenta con el servicio de red inalámbrica, dando el servicio requerido está dando resultados excelentes.

Dentro de la aplicación del proyecto existieron diferentes problemas en el desarrollo del mismo, puesto que las condiciones que se requerían, no en todos los lugares se contaban con ellas, lo cual implica un poco más de trabajo, para acondicionar adecuadamente el lugar, otro factor fue el de que los usuarios no entendían como sería la diferencia para acceder a la red entre usuario de CFE o invitado.

De esta forma se fue preparando poco a poco esta situación de tal forma que la gran mayoría de los trabajadores de CFE han alcanzado su rendimiento de la red inalámbrica a un 95%, y los invitados que se conectan a la red están satisfechos con el resultado, puesto que tienen un servicio de calidad, en tiempo real, y sin la necesidad de molestar a otra persona para que se le asignara un punto de red.

Con esto queda claro que la tecnología avanza día con día y CFE, esta en la vanguardia dando pasos agigantados, ya que los switches ya están

configurados para la inicialización de la entrada de la tecnología 802.11n y otras aplicaciones.

El proyecto en la empresa me ha dado muchas muy buenas experiencias, tanto en el sentido académico como profesional, se que esta dando un buen resultado y me siento muy orgullosa de haber contribuido aunque fuera un poco en la realización de este gran proyecto, puesto que las nuevas tecnologías que se están implantando son cada vez más interesantes y llenas de avances, que permitirán el crecimiento y rendimiento en la empresa.

ANEXOS

ANEXOS

APENDICE A

Algunas de las normas que se toman en cuenta en cuanto a las Normas de cableado estructurado son las siguientes:

NORMAS NACIONALES

Tipo de Normas

NMX, Norma Recomendatoria

NOM, Norma Obligatoria

NMX-I-248-1998

- Norma Nacional del Cableado Estructurado
- Actualmente en revisión.

NMX,-I279-2001

- Sistema de canalización para cableado estructurado.

NOM-SEDE-001-1999

- Instalaciones eléctricas y cableado en general
- Equivalente la NFPA 250:NEC
- Artículo 770, Fibra Óptica

Otras Normas

NOM-002-STPS-1999

NOM-130-ECOL-1999

NMX-I-237-1997-NYCE

NMX-I-238-1997-NYCE

NMX-I-274-NYCE-2000

Normas para el closet de Telecomunicaciones

Difieren del cuarto de equipos y la cometida de servicios, en que estos están generalmente considerados para el servicio de pisos, proporcionado un punto de conexión entre Back Bone y el cableado horizontal.

Todo edificio debe ser atendido por al menos un closet de telecomunicaciones o cuarto de equipos por piso. No existe un número máximo de closet que puedan ser instalación dentro de un edificio.

Closet de Telecomunicaciones (Telecommunications room)

- Tamaño recomendado: altura 2.6m, 3.0 x 2.4 de área para área de servicio <500m^2.
- Espacio.
- Alimentación
- Tuberías.
- Plafones
- FireBarier^{TM}
- Control de Ambiente

Los tipos de servicio de cableado que pueden ser alojados en los closet de telecomunicaciones, incluyen:

- Cross-Connect Horizontal (HC)
- Main Cross-connect (MC)
- Intermediate Cross-connect (IC)
- Acometida de Servicios

Es un cuarto de propósito especial que proporciona y mantiene un medio ambiente comunicaciones y cómputo. Difieren d los closet de Telecomunicaciones en que están considerados para dar servicio a un edificio o campus completos.

- Requerimiento similares al TC
- Incluye accesorios de interconexión.
- Plafones no permitidos.
- Rango de temperatura de 18º a 24 ºC.

Back Bone

El back bone (también llamado “riser”), es la parte de sistema de cableado estructurado que proporciona interconexión entre cuartos de equipos, closet de telecomunicaciones y los servicios de la acometida de telecomunicaciones. Normalmente proporciona:

- Conexión intra-edificio entre los diferentes pisos.
- Conexión entre edificios en medios tipo “campus”

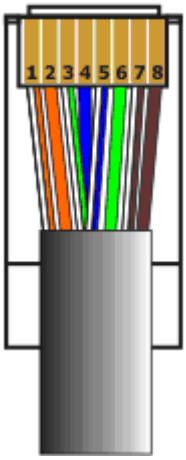
Dentro de estos closet de comunicación existen los equipos donde van conectados los servicios por medio del cable utilizado cuyas características son:

Se trabaja con cable UTP categoría 6, su forro puede ser de PVC o LS0H

- Marcaje 3M telecomunications Cat 6
- Cumple con las Normas ISO 1180, EIA-TIA 568, IEC332-I y NFC32070 2.1
- Con cruceta de separación de pares.
- Cinta de cubierta entre cubierta y pares.

Con este tipo de cable se emplea el conector RJ45, el cual tiene como característica que puede trabajarse en dos normas de uso las cuales definen como será su funcionamiento estas son:

Conector RJ45
Norma "568-B"
("Patilla" hacia abajo)

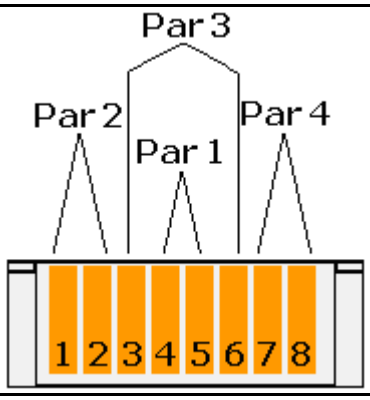


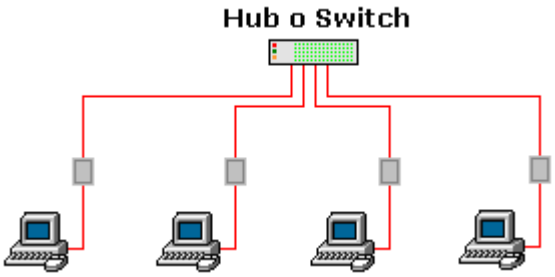
Norma de cableado "568-B" (Cable normal o paralelo)

Esta norma o estándar establece el siguiente y mismo código de colores en ambos extremos del cable:

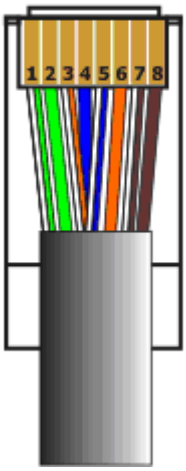
Conector 1	Nº Pin←→Nº Pin	Conector 2
Blanco/Naranja	Pin 1 a Pin 1	Blanco/Naranja
Naranja	Pin 2 a Pin 2	Naranja
Blanco/Verde	Pin 3 a Pin 3	Blanco/Verde
Azul	Pin 4 a Pin 4	Azul
Blanco/Azul	Pin 5 a Pin 5	Blanco/Azul
Verde	Pin 6 a Pin 6	Verde
Blanco/Marrón	Pin 7 a Pin 7	Blanco/Marrón
Marrón	Pin 8 a Pin 8	Marrón

Este cable lo usaremos para redes que tengan "Hub" o "Switch", es decir, para unir los Pc´s con las rosetas y éstas con el Hub o Switch.
NOTA: Siempre la "patilla" del conector RJ45 hacia abajo y de izqda. (pin 1) a dcha. (pin 8)





Conector RJ45
Norma "568-A"
("Patilla" hacia abajo)

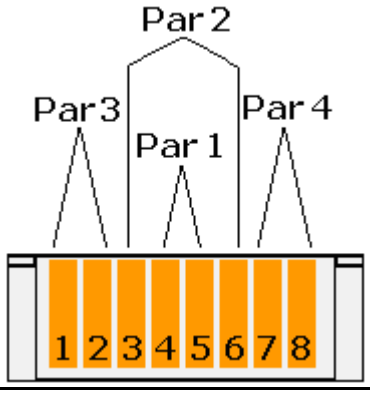


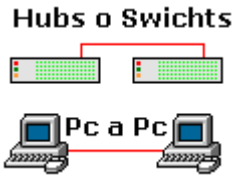
Norma de cableado "568-A" (Cable "Cruzado")

Esta norma o estándar establece el siguiente código de colores en cada extremo del cable:

Conector 1 (568-B)	Nº Pin	Nº Pin	Conector 2 (568-A)
Blanco/Naranja	Pin 1	Pin 1	Blanco/Verde
Naranja	Pin 2	Pin 2	Verde
Blanco/Verde	Pin 3	Pin 3	Blanco/Naranja
Azul	Pin 4	Pin 4	Azul
Blanco/Azul	Pin 5	Pin 5	Blanco/Azul
Verde	Pin 6	Pin 6	Naranja
Blanco/Marrón	Pin 7	Pin 7	Blanco/Marrón
Marrón	Pin 8	Pin 8	Marrón

Este cable lo usaremos para redes entre 2 Pc´s o para interconexionar Hubs o Switchs entre sí.
NOTA: Siempre la "patilla" del conector RJ45 hacia abajo y de izqda. (pin 1) a dcha. (pin 8)





APENDICE B

Configuración del router.

Un router es un equipo que sirve de intermediario entre las redes. Su funcionamiento es la enlutar correctamente el tráfico que se intercambian entre ellas. Los usuarios de Wi-Fi nos encontramos habitualmente con dos tipos de routers: un punto de acceso, que hace d intermediario entre una red inalámbrica y una red cableada, y un módem router ADLS/cable, que hace de intermediario entre la red local del uso de Internet.

Como los router se encuentran entre dos redes necesitan disponer de dos configuraciones: una para cada red. Las numeraciones IP de la red local del router las gestiones del propio router, mientras que desde el punto de vista de la externa, el router es un usuario más. Por ejemplo, la red local de un punto de acceso es las inalámbricas, mientras que la red externa es la red cableada a la que se conecta. En el caso de los módem router ADLS/cable la red local es la de sus usuarios, mientras que la externa es Internet.

Cuando el router está conectado a Internet necesita conocer la dirección IP del router de Internet al que tiene que enviar los paquetes dirigidos a esta red. Esta dirección será la del router del proveedor de acceso y suele conocerse como IP del router remoto.

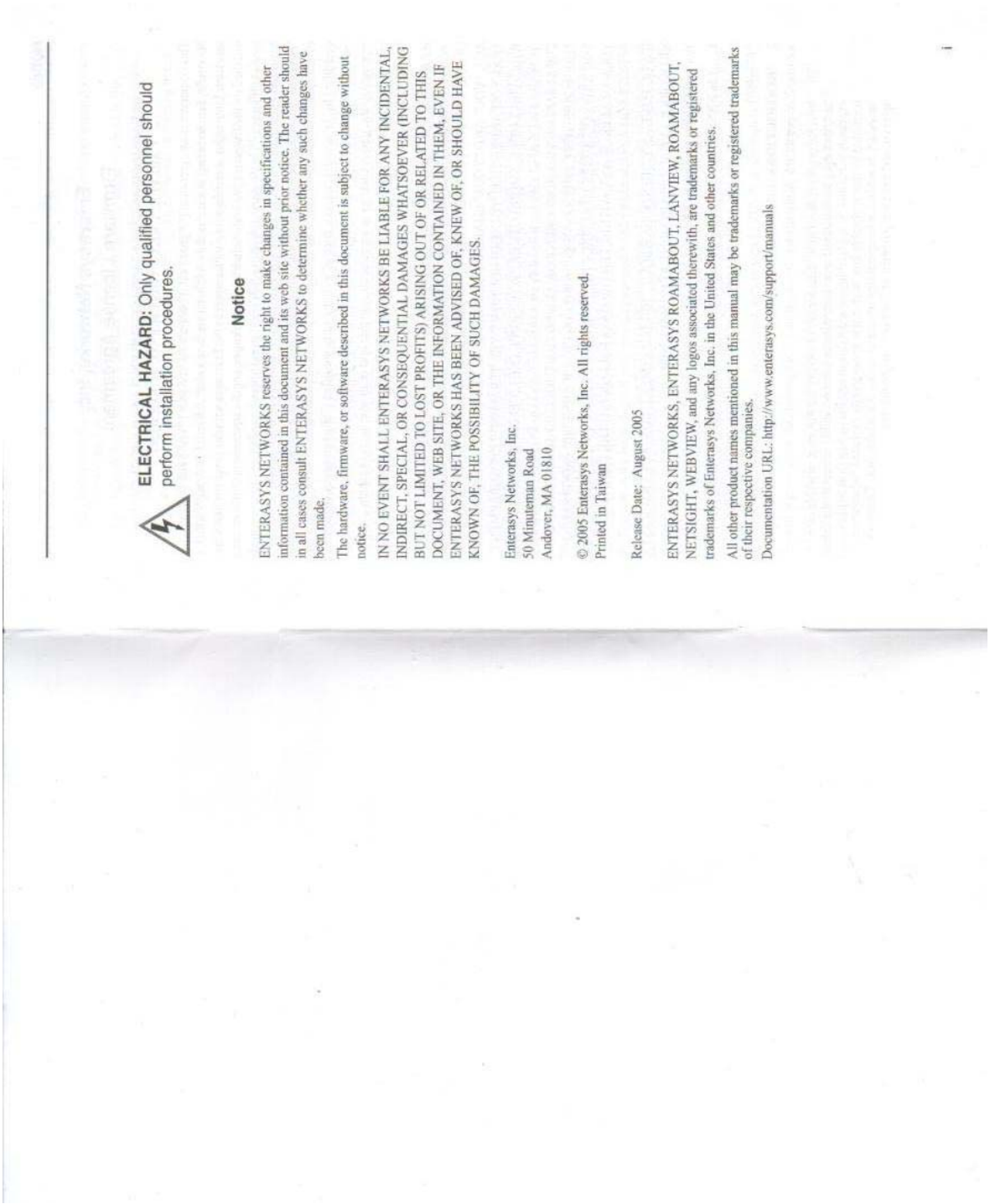
- IP interna del router, también conocida como dirección privada del router o IP LAN. Es la dirección IP que identifica al router dentro de la red local. Desde el punto de vista de las computadoras de la red, la dirección IP interna del router es su parte de enlace con Internet. Generalmente, la dirección interna del router suele ser la primera dirección IP del rango de direcciones privadas. Por ejemplo, 172.26.0.1 ó 192.168.0.1.

- IP externa del router, también conocida como dirección IP pública del router o dirección IP WAN. Esta dirección la facilita el proveedor del acceso a Internet (proveedor del servicio ADLS/cable).
- IP router remoto. Es la dirección del router de la red del proveedor de acceso a Internet (ISP). Por defecto, este valor puede asignarse automáticamente.

Adicionalmente, el router utiliza su servidor DHCP para gestionar la asignación automática de direcciones IP a sus usuarios locales y su servicio NAT para que todos sus usuarios locales pueden compartir su única dirección IP externa.

APENDICE 3

Esquema del manual que se utilizó en el desarrollo del proyecto, otorgado por la marca enterasys



ELECTRICAL HAZARD: Only qualified personnel should perform installation procedures.

Notice

ENTERASYS NETWORKS reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult ENTERASYS NETWORKS to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810

Printed in Taiwan

Release Date: August 2005

Documentation URL: http://www.enterasys.com/support/manuals

Enterasys Networks, Inc.
Firmware License Agreement

BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement ("Agreement") between the end user ("You") and Enterasys Networks, Inc. on behalf of itself and its Affiliates (as hereinafter defined) ("Enterasys") that sets forth Your rights and obligations with respect to the Enterasys software program/firmware installed on the Enterasys product (including any accompanying documentation, hardware or media) ("Program") in the package and prevails over any additional, conflicting or inconsistent terms and conditions appearing on any purchase order or other document submitted by You. "Affiliate" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. This Agreement constitutes the entire understanding between the parties, and supersedes all prior discussions, representations, understandings or agreements, whether oral or in writing, between the parties with respect to the subject matter of this Agreement. The Program may be contained in firmware, chips or other media.

BY INSTALLING OR OTHERWISE USING THE PROGRAM, YOU REPRESENT THAT YOU ARE AUTHORIZED TO ACCEPT THESE TERMS ON BEHALF OF THE END USER (IF THE END USER IS AN ENTITY ON WHOSE BEHALF YOU ARE AUTHORIZED TO ACT, "YOU" AND "YOUR" SHALL BE DEEMED TO REFER TO SUCH ENTITY) AND THAT YOU AGREE THAT YOU ARE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES, AMONG OTHER PROVISIONS, THE LICENSE, THE DISCLAIMER OF WARRANTY AND THE LIMITATION OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO ENTER INTO THIS AGREEMENT, ENTERASYS IS UNWILLING TO LICENSE THE PROGRAM TO YOU AND YOU AGREE TO RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS, LEGAL DEPARTMENT AT (978) 684-1000.

You and Enterasys agree as follows:

1. LICENSE. You have the non-exclusive and non-transferable right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this Agreement.

2. RESTRICTIONS. Except as otherwise authorized in writing by Enterasys, You may not, nor may You permit any third party to:

(i) Reverse engineer, decompile, disassemble or modify the Program, in whole or in part, including for reasons of error correction or interoperability, except to the extent expressly permitted by applicable law and to the extent the parties shall not be permitted by that applicable law, such rights are expressly excluded. Information necessary to achieve interoperability or correct errors is available from Enterasys upon request and upon payment of Enterasys' applicable fee.

(ii) Incorporate the Program, in whole or in part, in any other product or create derivative works based on the Program, in whole or in part.

(iii) Publish, disclose, copy, reproduce or transmit the Program, in whole or in part.

(iv) Assign, sell, license, sublicense, rent, lease, encumber by way of security interest, pledge or otherwise transfer the Program, in whole or in part.

(v) Remove any copyright, trademark, proprietary rights, disclaimer or warning notice included on or embedded in any part of the Program.

3. APPLICABLE LAW. This Agreement shall be interpreted and governed under the laws and in the state and federal courts of the Commonwealth of Massachusetts without regard to its conflicts of laws provisions. You accept the personal jurisdiction and venue of the Commonwealth of Massachusetts courts. None of the 1980 United Nations Convention on Contracts for the International Sale of Goods, the United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

4. EXPORT RESTRICTIONS. You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the Program is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Sections 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People's Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The enclosed Program (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Program is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

6. **DISCLAIMER OF WARRANTY.** EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED TO YOU IN WRITING BY ENTERASYS, ENTERASYS DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT WITH RESPECT TO THE PROGRAM. IF IMPLIED WARRANTIES MAY NOT BE DISCLAIMED BY APPLICABLE LAW, THEN ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THIRTY (30) DAYS AFTER DELIVERY OF THE PROGRAM TO YOU.

7. **LIMITATION OF LIABILITY.** IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS FOREGOING LIMITATION SHALL APPLY REGARDLESS OF THE CAUSE OF ACTION UNDER WHICH DAMAGES ARE SOUGHT.

THE CUMULATIVE LIABILITY OF ENTERASYS TO YOU FOR ALL CLAIMS RELATING TO THE PROGRAM, IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE TOTAL AMOUNT OF FEES PAID TO ENTERASYS BY YOU FOR THE RIGHTS GRANTED HEREIN.

8. **AUDIT RIGHTS.** You hereby acknowledge that the intellectual property rights associated with the Program are of critical value to Enterasys and, accordingly, You hereby agree to maintain complete books, records and accounts showing (i) license fees due and paid, and (ii) the use, copying and deployment of the Program. You also grant to Enterasys and its authorized representatives, upon reasonable notice, the right to audit and examine during Your normal business hours, Your books, records, accounts and hardware devices upon which the Program may be deployed to verify compliance with this Agreement, including the verification of the license fees due and paid Enterasys and the use, copying and deployment of the Program. Enterasys' right of examination shall be exercised reasonably, in good faith and in a manner calculated to not unreasonably interfere with Your business. In the event such audit discovers non-compliance with this Agreement, including copies of the Program made, used or deployed in breach of this Agreement, You shall promptly pay to Enterasys the appropriate license fees. Enterasys reserves the right, to be exercised in its sole discretion and without prior notice, to terminate this license, effective immediately, for failure to comply with this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

9. **OWNERSHIP.** This is a license agreement and not an agreement for sale. You acknowledge and agree that the Program constitutes trade secrets and/or copyrighted material of Enterasys and/or its suppliers. You agree to implement reasonable security measures to protect such trade secrets and copyrighted material. All right, title and interest in and to the Program shall remain with Enterasys and/or its suppliers. All rights not specifically granted to You shall be reserved to Enterasys.

10. **ENFORCEMENT.** You acknowledge and agree that any breach of Sections 2, 4, or 9 of this Agreement by You may cause Enterasys irreparable damage for which recovery of money damages would be inadequate, and that Enterasys may be entitled to seek timely injunctive relief to protect Enterasys' rights under this Agreement in addition to any and all remedies available at law.

11. **ASSIGNMENT.** You may not assign, transfer or sublicense this Agreement or any of Your rights or obligations under this Agreement, except that You may assign this Agreement to any person or entity which acquires substantially all of Your stock or assets. Enterasys may assign this Agreement in its sole discretion. This Agreement shall be binding upon and inure to the benefit of the parties, their legal representatives, permitted transferees, successors and assigns as permitted by this Agreement. Any attempted assignment, transfer or sublicense in violation of the terms of this Agreement shall be void and a breach of this Agreement.

12. **WAIVER.** A waiver by Enterasys of a breach of any of the terms and conditions of this Agreement must be in writing and will not be construed as a waiver of any subsequent breach of such term or condition. Enterasys' failure to enforce a term upon Your breach of such term shall not be construed as a waiver of Your breach or prevent enforcement on any other occasion.

13. **SEVERABILITY.** In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired thereby, and that provision shall be reformed, construed and enforced to the maximum extent permissible. Any such invalidity, illegality or unenforceability in any jurisdiction shall not invalidate or render illegal or unenforceable such provision in any other jurisdiction.

14. **TERMINATION.** Enterasys may terminate this Agreement immediately upon Your breach of any of the terms and conditions of this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

COMPLIANCES

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:
FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Wireless 5 GHz Band Statements:

As the Access Point can operate in the 5150-5250 MHz frequency band it is limited by the FCC, Industry Canada and some other countries to indoor use only so as to reduce the potential for harmful interference to co-channel Mobile Satellite systems.

High power radars are allocated as primary users (meaning they have priority) of the 5250-5350 MHz and 5725-5850 MHz bands. These radars could cause interference and /or damage to the access point when used in Canada.

The term "IC:" before the radio certification number only signifies that Industry Canada technical specifications were met.

Operating Frequencies

The user must use the configuration utility provided with this product to ensure the channels of operation are in conformance with the spectrum usage rules for country in which it is being operated.

Industry Canada - Class B

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of Industry Canada.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matérial brouilleur: "Appareils Numériques," NMB-003 édictée par l'Industrie.

TABLE OF CONTENTS

Chapter 1
Introduction

The RoamAbout RBT-1002 Wireless Access Point is an IEEE 802.11a/g access point that provides transparent, wireless high-speed data communications between a wired LAN and fixed, portable or mobile devices equipped with an 802.11a, 802.11b or 802.11g wireless adapter.

This solution offers fast, reliable wireless connectivity with considerable cost savings over wired LANs (which include long-term maintenance overhead for cabling). Using 802.11a and 802.11g technology, this access point can easily replace a 10 Mbps Ethernet connection or seamlessly integrate into a 10/100 Mbps Ethernet LAN.

Radio Characteristics – The IEEE 802.11a/g standard uses a radio modulation technique known as Orthogonal Frequency Division Multiplexing (OFDM), and a shared collision domain (CSMA/CA). It operates at the 5 GHz Unlicensed National Information Infrastructure (UNII) band for connections to 802.11a clients, and at 2.4 GHz for connections to 802.11g clients.

IEEE 802.11g includes backward compatibility with the IEEE 802.11b standard. IEEE 802.11b also operates at 2.4 GHz, but uses Direct Sequence Spread Spectrum (DSSS) and Complementary Code Keying (CCK) modulation technology to achieve a communication rate of up to 11 Mbps.

The access point supports a 54 Mbps half-duplex connection to Ethernet networks for each active channel.

Package Checklist

The RoamAbout RBT-1002 Wireless Access Point package includes:

- One RoamAbout 1002 Wireless Access Point
- One AC power adapter and power cord
- Four rubber feet
- Four wall-mounting screws
- Bezel
- This Installation Guide

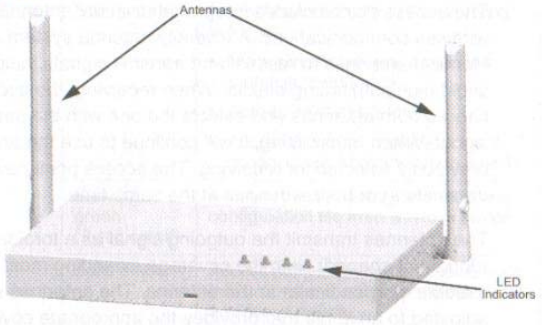
Optional Wireless Access Point Equipment:

- Wall-mounting bracket

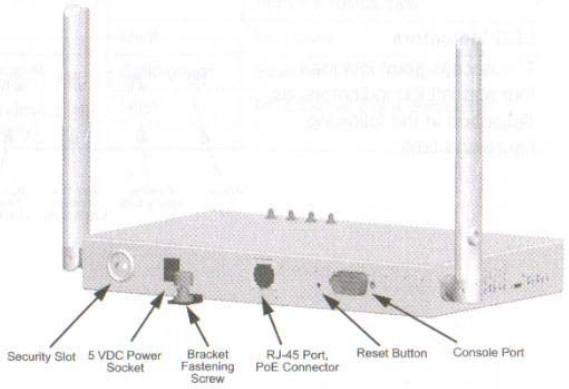
Inform your dealer if there are any incorrect, missing or damaged parts. If possible, retain the carton, including the original packing materials. Use them again to repack the product in case there is a need to return it.

Hardware Description

Top Panel



Rear Panel



Component Description

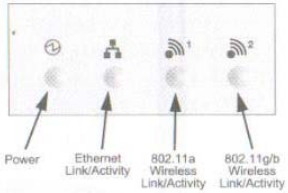
Antennas

The access point includes integrated diversity antennas for wireless communications. A diversity antenna system uses two identical antennas to receive and transmit signals, helping to avoid multipath fading effects. When receiving, the access point checks both antennas and selects the one with the strongest signal. When transmitting, it will continue to use the antenna previously selected for receiving. The access point never transmits from both antennas at the same time.

The antennas transmit the outgoing signal as a toroidal sphere (doughnut shaped), with the coverage extending most in a direction perpendicular to the antenna. The antennas should be adjusted to an angle that provides the appropriate coverage for the service area. For further information, see "Positioning the Antennas" on page 2-5.

LED Indicators

The access point includes four status LED indicators, as described in the following figure and table.



LED	Status	Description
Power	Solid green	Normal operation. All of the following are true: • Management link with a wireless switch is operational • Access point has booted • Access point has received a valid configuration from a wireless switch
	Slow blink green (2 sec on/off)	Access point is booting and receiving configuration file from wireless switch.
	Solid amber	Access point is waiting to receive boot instructions and a configuration file from a wireless switch.
	Quick blink green	Access point has successfully booted but received an invalid configuration from a wireless switch.
	Unlit	No power.
Ethernet Link (Ethernet Link/ Activity)	Solid green	Ethernet link is detected.
	Unlit	No Ethernet link is detected.

LED	Status	Description
11a and 11b/g (Wireless Link/ Activity)	Solid green	A client is associated with the radio, or the radio is in Sweep/Sentry mode.
	Slow blink green (2 sec on/off)	Radio is unable to transmit. This state can indicate inability to send a beacon or radio failure.
	Fast blink green	Associated client is sending or receiving traffic.
	Unlit	Indicates one of the following: • The radio is disabled • No clients are associated with the radio and there is no traffic activity

Security Slot

The access point includes a Kensington security slot on the rear panel. You can prevent unauthorized removal of the access point by wrapping the Kensington security cable (not provided) around an unmovable object, inserting the lock into the slot, and turning the key.

Console Port

The console port is not used on the RBT-1002.

Ethernet Port

The access point has one 10BASE-T/100BASE-TX RJ-45 port that can be attached directly to 10BASE-T/100BASE-TX LAN segments. These segments must conform to the IEEE 802.3 or 802.3u specifications.

This port uses an MDI (i.e., internal straight-through) pin configuration. You can therefore use straight-through twisted-pair cable to connect this port to most network interconnection devices such as a switch or router that provide MDI-X ports.

However, when connecting the access point to a workstation or other device that does not have MDI-X ports, you must use crossover twisted-pair cable.

The access point appears as an Ethernet node and performs a bridging function by moving packets from the wired LAN to remote workstations on the wireless infrastructure.

Note: The RJ-45 port also supports Power over Ethernet (PoE) based on the IEEE 802.3af standard. Refer to the description for the "Power Connector" for information on supplying power to the access point's network port from a network device, such as a switch, that provides Power over Ethernet (PoE).

Reset Button

The reset button has no affect on the RBT-1002.

Power Connector

The access point does not have a power switch. It is powered on when connected to the AC power adapter, and the power adapter is connected to a power source. The access point automatically adjusts to any voltage between 100-240 volts at 50 or 60 Hz. No voltage range settings are required.

The access point may also receive Power over Ethernet (PoE) from a switch or other network device that supplies power over the network cable based on the IEEE 802.3af standard.

Note that if the access point is connected to a PoE source device and also connected to a local power source through the AC power adapter, PoE will be disabled.

Features and Benefits

- Local network connection via 10/100 Mbps Ethernet ports or 54 Mbps wireless interface (supporting up to 127 mobile users)
- IEEE 802.11a, 802.11b and 802.11g compliant
- Interoperable with multiple vendors based on the IEEE 802.11f protocol
- Advanced security through 64/128-bit Wired Equivalent Protection (WEP) encryption, IEEE 802.1x authentication via a central RADIUS server, Wi-Fi Protected Access (WPA), and MAC address filtering features to protect your sensitive data and authenticate only authorized users to your network
- Provides seamless roaming within the IEEE 802.11a, 802.11b and 802.11g WLAN environment
- Scans all available channels and selects the best channel for each client based on the signal-to-noise ratio

System Defaults

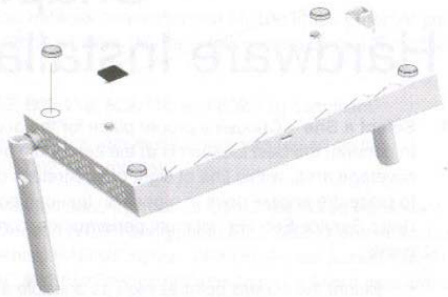
There are no system defaults on the RBT-1002 because a new image is loaded on the access point with every power cycle.

Chapter 2 Hardware Installation

1. **Select a Site** – Choose a proper place for the access point. In general, the best location is at the center of your wireless coverage area, within line of sight of all wireless devices. Try to place the access point in a position that can best cover its Basic Service Set. For optimum performance, consider these points:
   - Mount the access point as high as possible above any obstructions in the coverage area.
   - Avoid mounting next to or near building support columns or other obstructions that may cause reduced signal or null zones in parts of the coverage area.
   - Mount away from any signal absorbing or reflecting structures (such as those containing metal)

   Note: The supplied bezel should not be used when mounting on a plenum ceiling.
2. **Mount the Access Point** – The access point can be mounted on any horizontal surface or a wall.

   Mounting on a horizontal surface – To keep the access point from sliding on the surface, attach the four rubber feet provided in the accessory kit to the marked circles on the bottom of the access point.



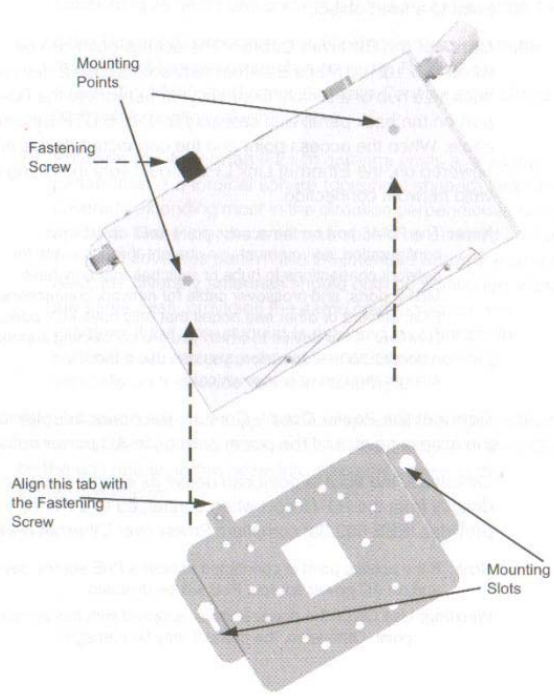
Mounting on a wall – The access point should be mounted only to a wall or wood surface that is at least 1/2-inch plywood or its equivalent. To mount the access point on a wall, always use its wall-mounting bracket.

a. Using the mounting bracket, mark the position of the four screw holes on the wall. For concrete or brick walls, you will need to drill holes and insert wall plugs for the screws.

b. Position the mounting bracket over the wall screw holes, then insert the included screws and tighten them down to secure the bracket firmly to the wall.

c. Attach the access point to the mounting bracket. Line up the two mounting points on the bracket with the two mounting slots on the bottom of the access point (see the following figure). Place the mounting points of the bracket into the mounting slots of the bracket, slide it into position so that the bracket fastening screw on the access point

lines up with the tab on the bracket. Then screw down the fastening screw to secure the access point to the bracket.



Bracket

3. **Lock the Access Point in Place** – To prevent unauthorized removal of the access point, you can use a Kensington Slim MicroSaver security cable (not included) to attach the access point to a fixed object.

4. **Connect the Ethernet Cable** – The access point can be wired to a 10/100 Mbps Ethernet network through a device such as a hub or a switch. Connect your network to the RJ-45 port on the back panel with category 3, 4, or 5 UTP Ethernet cable. When the access point and the connected device are powered on, the Ethernet Link LED should light indicating a valid network connection.

   Note: The RJ-45 port on the access point uses an MDI pin configuration, so you must use straight-through cable for network connections to hubs or switches that only have MDI-X ports, and crossover cable for network connections to PCs, servers or other end nodes that only have MDI ports. However, if the device to which you are connecting supports auto-MDI/MDI-X operation, you can use either straight-through or crossover cable.

5. **Connect the Power Cord** – Connect the power adapter to the access point, and the power cord to an AC power outlet.

   Otherwise, the access point can derive its operating power directly from the RJ-45 port when connected to a device that provides IEEE 802.3af compliant Power over Ethernet (PoE).

   Note: If the access point is connected to both a PoE source device and an AC power source, PoE will be disabled.

   Warning: Use ONLY the power adapter supplied with this access point. Otherwise, the product may be damaged.

6. **Observe the Self Test** – When you power on the access point, verify that the Power indicator stops blinking and remains on green, and that the other indicators start functioning as described under "LED Indicators" on page 1-4.

   If the Power LED does not stop blinking or turns on yellow, the self test has not completed correctly. Refer to the *RoamAbout Mobility System Software Configuration Guide* for troubleshooting information.

7. **Position the Antennas** – Each antenna emits a radiation pattern that is a toroidal sphere (doughnut shaped), with the coverage extending most in the direction perpendicular to the antenna. Therefore, the antennas should be oriented so that the radio coverage pattern fills the intended horizontal space. Also, the diversity antennas should both be positioned along the same axes, providing the same coverage area. For example, if the access point is mounted on a horizontal surface, both antennas should be positioned pointing vertically up to provide optimum coverage.

If you choose to use the supplied bezel, position the bezel directly over the access point so that the LED holes line up with the LEDs on the unit and snap the bezel into place, as shown in the following diagram:

To remove the bezel, grasp both sides and gently pry away from the fastening slots located on each antenna side. Pull the bezel clear of the access point.

Chapter 3 Configuration

All configuration of the RBT-1002 is done from the RoamAbout wireless switch and the RoamAbout Switch Manager interface.

Refer to the *RoamAbout Switch Manager User Guide* and the *RoamAbout Mobility System Software Configuration Guide* for configuration information.

Appendix A
Troubleshooting

For troubleshooting information, refer to the *RoamAbout Mobility System Software Configuration Guide*.

Appendix B
Cables and Pinouts

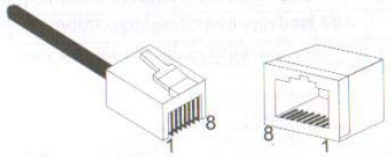
Twisted-Pair Cable Assignments

For 10/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

Caution: DO NOT plug a phone jack connector into the RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

Caution: Each wire pair must be attached to the RJ-45 connectors in a specific orientation. (See "Straight-Through Wiring" on page B-3 and "Crossover Wiring" on page B-3 for an explanation.)

The following figure illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.



10/100BASE-TX Pin Assignments

Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3 or better cable for 10 Mbps connections, or 100-ohm Category 5 or better cable for 100 Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

The RJ-45 port on the access point is wired with MDI pinouts. This means that you must use crossover cables for connections to PCs or servers, and straight-through cable for connections to switches or hubs. However, when connecting to devices that support automatic MDI/MDI-X pinout configuration, you can use either straight-through or crossover cable.

10/100BASE-TX MDI Port Pinouts	
Pin	**MDI Signal Name**
1	Transmit Data plus (TD+)
2	Transmit Data minus (TD-)
3	Receive Data plus (RD+)
4	GND (Positive Vport)
5	GND (Positive Vport)
6	Receive Data minus (RD-)
7	-48V feeding power (Negative- Vport)
8	-48V feeding power (Negative- Vport)

Note: The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

Straight-Through Wiring

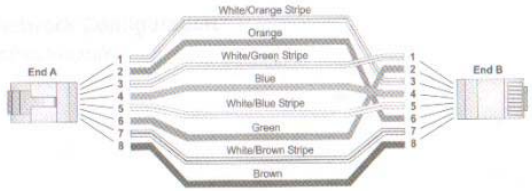
Because the 10/100 Mbps port on the access point uses an MDI pin configuration, you must use "straight-through" cable for network connections to hubs or switches that only have MDI-X ports. However, if the device to which you are connecting supports auto-MDIX operation, you can use either "straight-through" or "crossover" cable.

EIA/TIA 568B RJ-45 Wiring Standard
10/100BASE-TX Straight-through Cable

Crossover Wiring

Because the 10/100 Mbps port on the access point uses an MDI pin configuration, you must use "crossover" cable for network connections to PCs, servers or other end nodes that only have MDI ports. However, if the device to which you are connecting supports auto-MDIX operation, you can use either "straight-through" or "crossover" cable.

EIA/TIA 568B RJ-45 Wiring Standard
10/100BASE-TX Crossover Cable



Appendix C Specifications

General Specifications

Maximum Channels

802.11a:
US & Canada: 12
802.11b/g:
FCC/IC: 1-11
Maximum Clients
127 total clients for the AP

Operating Range

Refer to the *RoamAbout Switch Manager User Guide*

Data Rate

802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel
802.11g: 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps per channel
802.11b: 1, 2, 5.5, 11 Mbps per channel

Modulation Type

802.11a: BPSK, QPSK, 16-QAM, 64-QAM
802.11g: CCK, BPSK, QPSK, OFDM
802.11b: CCK, BPSK, QPSK

Network Configuration

Infrastructure

Operating Frequency
802.11a:
5.150 ~ 5.250 GHz (lower band) US/Canada
5.250 ~ 5.350 GHz (middle band) US/Canada
5.725 ~ 5.850 GHz (upper band) US/Canada
802.11b:
2.4 ~ 2.4835 GHz (US, Canada)

AC Power Adapters
Input: 100-240 AC, 50-60 Hz
Output: 5 VDC, 3 A or 2 A
Maximum Power: 13.2 W

Unit Power Supply
DC Input: 5 VDC, 2 A
PoE input: 48 VDC, 0.2 A maximum
Power consumption: 9.6 W maximum

Note: Power can also be provided to the access point through the Ethernet port based on IEEE 802.3af Power over Ethernet (PoE) specifications. When both PoE is provided and the adapter is plugged in, PoE will be turned off.

Physical Size
20.9 x 12.5 x 2.6 cm (8.23 x 4.92 x 1.02 in)

Weight
0.65 kg (1.43 lbs)

LED Indicators
Power, Ethernet Link/Activity, Wireless Link/Activity

Network Management
Via RoamAbout wireless switches, RoamAbout Switch Manager

Temperature
Operating: 0 to 40 °C (32 to 104 °F)
Storage: 0 to 70 °C (32 to 158 °F)

Humidity
15% to 95% (non-condensing)

Compliances
FCC Class B (US)
ICES-003 (Canada)

Radio Signal Certification
FCC Part 15.247 (2.4 GHz)
FCC part 15 15.407(b)
RSS-210 (Canada)

Safety
CSA/NTRL (CSA 22.2 No. 950 & UL 60950)
EN60950 (TÜV/GS), IEC60950 (CB)

Standards
IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX,
IEEE 802.11a, b, g

Sensitivity

IEEE 802.11a	Sensitivity (GHz - dBm)		
Modulation/Rates	5.150-5.250	5.250-5.350	5.725-5.850
BPSK (6 Mbps)	-88	-88	-88
BPSK (9 Mbps)	-87	-87	-87
QPSK (12 Mbps)	-86	-86	-86
QPSK (18 Mbps)	-84	-84	-84
16 QAM (24 Mbps)	-81	-81	-81
16 QAM (36 Mbps)	-77	-77	-78
64 QAM (48 Mbps)	-73	-73	-73
64QAM(54 Mbps)	-69	-70	-67

IEEE 802.11g	
Data Rate	Sensitivity (dBm)
6 Mbps	-88
9 Mbps	-87
12 Mbps	-86
17 Mbps	-85
24 Mbps	-81
36 Mbps	-77
48 Mbps	-72
54 Mbps	-70

IEEE 802.11b	
Data Rate	Sensitivity (dBm)
1 Mbps	-93
2 Mbps	-90
5.5 Mbps	-90
11 Mbps	-87

Transmit Power

IEEE 802.11a	Maximum Output Power (GHz - dBm)		
Data Rate	5.15-5.250	5.25-5.350	5.725-5.850
6 Mbps	17	17	17
9 Mbps	17	17	17
12 Mbps	17	17	17
8 Mbps	17	17	17
24 Mbps	17	17	17
36 Mbps	17	17	17
48 Mbps	17	17	17
54 Mbps	12	17	16

IEEE 802.11g	Maximum Output Power (GHz - dBm)	
Data Rate	2.412	2.417~2.462
6 Mbps	20	20
9 Mbps	20	20
12 Mbps	20	20
18 Mbps	20	20
24 Mbps	20	20
36 Mbps	20	19
48 Mbps	17	16
54 Mbps	15	14

IEEE 802.11b	Maximum Output Power (GHz - dBm)	
Data Rate	2.412	2.417~2.462
1 Mbps	15	16
2 Mbps	15	16
5.5 Mbps	15	16
11 Mbps	15	16

GLOSARIO DE TERMINOS

Glosario:

A

AAA. Autentificación, autorización, y contabilidad. Un marco para los servicios de configuración que proporcionan una conexión de red segura y un expediente de la actividad del usuario, identificando a quién es el usuario, a lo que puede tener acceso el usuario, y qué servicios y recursos está consumiendo el usuario. En un sistema de la movilidad de las redes de Enterasys, el interruptor de RoamAbout puede utilizar un servidor del RADIO o su propia base de datos local para los servicios del AAA.

ACE. Una regla en un Access Control List de la seguridad (ACL) ese las concesiones o niega un sistema de las derechas de acceso de red basadas en unos o más criterios. Criterios del uso de ACEs tales como un protocolo y una fuente o un IP address de la destinación para determinarse si permitir o negar los paquetes que emparejan los criterios. ACEs se procesan en la orden en la cual aparecen en la seguridad ACL. Vea también la seguridad ACL.

ADLS. Asymmetric Digital Suscriber Line, “Línea de abonado digital asimétrica”. Tecnología pensada para poder transmitir datos a alta velocidad a través del bucle de abonado de la línea telefónica. El bucle de abonado es el cable de cobre.

AES. . Estándar Avanzado Del Cifrado. Uno de los estándares federales de la tratamiento de la información (PAA). El AES, documentado en la publicación 197 de los PAA, especifica un algoritmo simétrico del cifrado para el uso por organizaciones de proteger la información sensible. Vea 802.11i; CCMP.

ANCHO DE BANDA. Cantidad de datos que pueden circular en un medio por unidad e tiempo. Generalmente se mide en bits por segundos. También puede hacer referencia a un rango de frecuencia.

AP. Vea El Punto De Acceso.

API. Aplication Program Interface, “Interfaz entre programas”. Interfaz que permite la comunicación entre programa, redes y base de datos.

ÁREA DE COBERTURA. En encargado del interruptor de Enterasys RoamAbout, la unidad más pequeña del espacio dentro de la cual para planear la cobertura del punto de acceso (AP) para un LAN sin hilos (WLAN). El número de los puntos de acceso requeridos para un área de la cobertura depende del tipo de transmisión de IEEE 802.11 usada, y de las características del área y de la densidad físicas del usuario.

ASCII. American Standard Code for Information Exchange, “Código normalizado americano para el intercambio de información”. Código que le asigna a cada letra, número o signo empleado por las computadoras una determinada combinación de ceros y unos. Éste es el código más utilizado por todas las computadoras a escala internacional.

ASOCIACION. El proceso definido en IEEE 802.11 por el cual una estación (sin hilos) móvil authenticada establece una relación con un punto de acceso sin hilos (AP) para tener el acceso completo de red. El punto de acceso asigna a estación móvil un identificador de la asociación (AYUDA), que el LAN sin hilos (WLAN) utiliza seguir la estación móvil mientras que vaga.

AUTENTIFICADO. Un dispositivo que autentica a cliente. En un sistema de la movilidad de las redes de Enterasys, el autenticado es un interruptor de RoamAbout.

B

BANDA ANCHA. Comunicaciones que transmiten datos a alta velocidad. Éste es un término relativo cuyo valor ha ido cambiando con el tiempo; aunque antiguamente se aplicaba a las velocidades superiores a 64 Kbps, hoy el límite va por 1 Mbps.

BANDA DE FRECUENCIA. Rango de frecuencia del espectro radioeléctrico. El espectro radioeléctrico está dividido en bandas de frecuencias que regulatoriamente son utilizadas para distintas finalidades.

BARRIDO DE LA DETECCIÓN DEL RF. Una búsqueda comprensiva para la radiofrecuencia (RF) señala dentro de un dominio de la movilidad agrupe, para localizar clientes del rogué, los puntos de acceso del rogue (APs), y a usuarios hoc del anuncio. Un barrido puede ser cualquiera al barrido programar o un SentrySweep continúo búsqueda. Durante un barrido programar, cada radio incluida del punto de acceso barre todos los canales en el espectro 802.11b/g y 802.11a de IEEE. En contraste, SentrySweep funciona solamente en las radios lisiadas en un dominio de la movilidad y no interrumpe servicio.

BIT. Unidad más pequeña de información. Un bit puede tomar el valor de 0 ó 1. Las computadoras internamente, sólo pueden manejar este tipo de información.

BLUETOOTH. Tecnología inalámbrica que permite intercomunicar equipos a una distancia de varios metros (menos de 10 metros). Al contrario con otras tecnologías como Wi-Fi, la tecnología Bluetooth no está pensada para soportar redes de computadoras, sino, más bien, comunicar una computadora o cualquier otro dispositivo con sus periféricos: un teléfono móvil con su auricular, una PDA con su computadora, una computadora con su impresora, etc.

BRIDGE. Puente. Dispositivo que interconecta dos redes que utilizan el mismo protocolo haciéndolas funcionar como si se tratara de una sola red. Los puntos de acceso hacen la función del bridge.

BSS. Basic service Set. “Conjunto de Servicios Básicos”. Una de las modalidades de comunicación en las que se puede configurar las terminales de una red Wi-Fi. En este caso la red inalámbrica dispone de un equipo (punto de acceso) que se encarga de gestionar las comunicaciones (internas y externas) de todos los dispositivos que forman la red. Este modo de conexión también es conocido como modo infraestructura.

BSSID. Basic Service Set Identifier, “Identificador Básico del Conjunto de Servicios”, parámetro que identifica a cada computadora que forma parte de la red Wi-Fi. Este identificador se genera de forma de manera automática y aleatoria.

BYTE. Unidad de información formada por 8 bits.

C

CCI. Interferencia del co-channel. Obstrucción que ocurre cuando una señal en una frecuencia particular impone en una célula que esté utilizando que la misma frecuencia para la transmisión. En redes del multicell, los sistemas se diseñan para reducir al mínimo el CCI con energía de la transmisión y la selección de canal apropiadas.

CCPM. Contador-Modo con protocolo del código de la autentificación del mensaje de encadenamiento del bloque de la cifra. Un protocolo sin hilos del cifrado basado en el cifrado avanzado estándar (AES) y definido en la especificación de IEEE 802.11i. CCMP utiliza un modo dominante simétrico de la cifra del bloque que proporcione aislamiento por medio de la autenticidad contraria del origen del modo y de datos por medio del código de la autentificación del mensaje de encadenamiento del bloque de la cifra (CBC-MAC). Vea también 802.11i; AES; TKIP; WPA. Compare WEP.

CDMA Code divison Multiple Access) Acceso Múltiple de División de Código. Norma de transferencia de información por teléfonos inalámbricos.

CELL. El área geográfica cubierta por un transmisor sin hilos.

CERTIFICATE AUTHORITY (CA). Software de red que publica y maneja las credenciales de la seguridad y las llaves públicas para la autentificación y el cifrado del mensaje. Como parte de una infraestructura del público-llave (PKI), que permite intercambios de la información seguros sobre una red, los cheques de un Certificate Authority con una autoridad del registro (RA) para verificar la información proporcionaron por el solicitante de un certificado digital. Si la autoridad del registro verifica la información del solicitante, el Certificate Authority puede publicar un certificado. De acuerdo con la puesta en práctica de PKI, el contenido del certificado puede incluir la fecha de vencimiento del certificado, la llave pública del dueño, el nombre del dueño, y la otra información sobre el dueño del publickey. Vea también la autoridad del registro (RA).

CHAP. Protocolo De la Autentificación Del Apretón de manos Del Desafío. Un protocolo de la autentificación que define un apretón de manos de tres vías para authenticar a un usuario (cliente). La GRIETA utiliza el algoritmo del picadillo MD5 para generar una respuesta a un desafío que se pueda comprobar por el authenticator. Para las conexiones sin hilos, la GRIETA no es segura y se debe proteger por la criptografía en los métodos tales de la autentificación que el protocolo extensible protegido de la autentificación (PEAP) y la seguridad de la capa de transporte de Tunneled (TTL).

CIFRADO. Cualquier procedimiento usado en criptografía para traducir datos a una forma que se puede leer por solamente su receptor previsto. Una señal cifrada se debe descifrar para ser leído. Vea también la criptografía.

CLIENTE. El programa o el dispositivo de petición en una relación del servidor de cliente. En un LAN sin hilos (WLAN), el cliente (o el supplicant) solicita el acceso a los servicios proporcionados por el authenticator. Vea también supplicant.

CONTRASEÑA. Palabra secreta o secuencia de caracteres que se utilizan para confirmar la identidad de un usuario. Para que sea eficaz, la contraseña debe ser conocida exclusivamente por el usuario y por el proveedor del servicio.

CPC. Cable del pleno de las comunicaciones. Vea el cable pleno-clasificado.

CRC. Control por redundancia cíclico. Un cheque primitivo de la integridad del mensaje.

CRYPTO. Vea la criptografía.

CRIPTOGRAFÍA. La ciencia de la seguridad de la información. La criptografía moderna se refiere típicamente a los procesos de revolver el texto ordinario (conocido como claramente el texto o texto claro) en el texto cifrado en el extremo del remitente de una conexión, y de descifrar el texto cifrado nuevamente dentro del texto claro en el extremo del receptor. Porque su seguridad es independiente de los canales a través de los cuales el texto pasa, la criptografía es la única manera de proteger comunicaciones sobre los canales que no están bajo control del usuario. Las metas de la criptografía son secreto, integridad, nonrepudiation, y autentificación. La información cifrada no se puede entender por cualquier persona para quién no se piensa, ni se altera en almacenaje o la transmisión sin la alteración que es detectada. El remitente no puede negar más adelante la creación o la transmisión de la información, y el remitente y el receptor pueden confirmarse identidad y el origen y la destinación de la información.

CSMA/CA. Carrier Sense Multiple Access whit Collision Avoidance, “Acceso Multiple por Detección de portadora con evitación de colisión” sistema que emplea Wi-Fi para negociar las comunicaciones entre los distintos dispositivos. Este sistema evita que dos dispositivos puedan intentar hacer uso del medio simultáneamente (evita colisión).

CSMA/CD. Carrier Sense Multiple Access whit Collision Detection, “Acceso Multiple por Detección de portadora con detección de colisión” sistema que emplea las redes Ethernet para negociar las comunicaciones entre los distintos dispositivos. Este sistema evita que dos dispositivos han intentado hacer uso del medio simultáneamente (detecta colisión) y hace que cada uno de lo intente de nuevo en tiempos distintos.

CSR. Petición De Firma Del Certificado. Un mensaje enviado por un administrador para solicitar un Security Certificate de un Certificate Authority (CA). Un CSR es una secuencia de texto ajustada a formato por protocolo Aislamiento-Realzado del correo (PEM) según el estándar dominante público de la criptografía (PKCS) # 10. El CSR contiene la información necesitada por el Certificate Authority para generar el certificado.

CSV. Archivo Coma-separado de los valores. Un archivo de texto que exhibe datos tabulares en un formato coma-delimitado, como lista de las filas en las cuales el valor de cada columna es separado del siguiente por una coma. Un archivo de CSV es útil para transferir datos entre los usos de la base de datos.

CUALIDAD. En la autentificación, la autorización, y la contabilidad (AAA), una característica identificar (authenticar) a un usuario o configurar (autorizar) o registraba (explicar) un usuario administrativo o la sesión de la red. Las cualidades del AAA de un usuario se almacenan en un perfil de usuario en la base de datos local en un interruptor

de RoamAbout, o en un servidor del RADIO. Los nombres de la cualidad son caso-sensibles. Vea también el RADIO; VSA.

D

DAEMON. Software que está siempre funcionando en segundo plano esperando a que una aplicación cliente solicite sus servicios. En los sistemas UNIX, se le da este nombre del *software* servidor.

DECT (Digital Enhanced Cordless Telecommunications) Tecnología digital inalámbrica originada en Europa, pero que actualmente se usa en todo el mundo.

DES. Estándar De Cifrado De Datos. Un algoritmo simétrico federal aprobado del cifrado en el uso por muchos años y substituido por el estándar avanzado del cifrado (AES). Vea también 3DES.

DHCP. Protocolo Dinámico De la Configuración Del Anfitrión. Un protocolo que asigna dinámicamente direcciones del IP a las estaciones, de un servidor centralizado. DHCP es el sucesor al protocolo del elástico de bota (BOOTP).

DIAGINAL. La prioridad de un interruptor de RoamAbout sobre el otro RoamAbout cambia para el booting, configurando, y proporcionando la transferencia de datos para un punto de acceso (AP). El diagonal se puede fijar a bajo o a alto en cada interruptor de RoamAbout y es alto por defecto. El diagonal se aplica solamente a los interruptores de RoamAbout que se unen indirectamente al AP a través de una red de la capa intermedia 2 o de la capa 3. Un AP procura siempre patear en el puerto 1 del AP primero

DIRECCIÓN. Cada computadora conectada a Internet dispone de una dirección que lo identifica. Esta dirección puede estar dada en forma numérica (dirección IP) o alfanumérica (nombre de dominio)

DIRECCIÓN IP. Cadena numérica que identifica a las computadoras conectados a Internet. Un ejemplo de dirección IP es 128.56.78.2.

DIRECCIÓN MAC. Número único que asignan los fabricantes a los dispositivos de red (adaptadores de red y puntos de acceso). Este número es permanente y viene grabado en el propio dispositivo para permitir identificarlo de manera inequívoca. Las direcciones MAC están formadas por 12 caracteres alfanuméricos (por ejemplo, 12-AB-56-78-90-FE).

DNS. *Domain Name System*, “Sistema de nombres de dominio”. Sistema encargado de traducir los nombres de dominio de las computadoras conectados a Internet de direcciones IP.

DOMINIO. En el Internet, un sistema de las direcciones de red que se organizan en niveles. (2) en Windows NT y Windows 2000 de Microsoft, un sistema de los recursos de la red (usos, impresoras, y así sucesivamente) para un grupo de los usuarios (clientes). Los clientes registran en el dominio para tener acceso a los recursos, que se pueden situar en un número de diversos servidores en la red.

DOMINIO DE COLISION. Un solo acceso múltiple de sentido de portador half-duplex de IEEE 802.3 con la red de la detección de colisión (CSMACD). Una colisión ocurre cuando dos o más los dispositivos de la capa 2 en la red transmiten en el mismo tiempo. Los segmentos de Ethernet se separaron por un interruptor de la capa 2 están dentro de diversos dominios de la colisión

Dominio De la Movilidad. Una colección de RoamAbout cambia el trabajo junta para apoyar a un usuario que vaga (cliente

DSA. Algoritmo De la Firma De Digital. El algoritmo de la publico-llave firmaba los certificados X.509.

DSL. Digital Subscriber Line, “línea digital de abonado”. Término genérico que hace referencia a la familia de tecnologías que utilizan las líneas telefónicas para transmitir datos a alta velocidad. ADLS, SDSL o HDLS son algunas de estas tecnologías. También se utiliza el termino xDSL para hacer referencia a esta familia de tecnologías.

DSSS. Separar-espectro de la Dirigir-secuencia. Uno de dos tipos de tecnología de la radio del separar-espectro usada en transmisiones sin hilos del LAN (WLAN). Para aumentar los datos señalaron resistencia a interferencia, la señal en la estación que enviaba se combinan con una secuencia del pedacito de la alto-tarifa que separa los datos del usuario en frecuencia por un factor igual al cociente que se separa. Compare FHSS.

DTIM. Mapa de la indicación del tráfico de la entrega. Un tipo especial de elemento del mapa de la indicación del tráfico (TIM) en un marco del faro que ocurre solamente cuando una estación en un sistema del servicio básico (BSS) está en el modo economizador. Un DTIM indica que cualquier difusión protegida o los marcos del multicast es transmitida inmediatamente por un punto de acceso (AP).

Formato DXF.
Una representación de datos marcada con etiqueta, en formato del ASCII, de la información contenida en un archivo de dibujo de AutoCAD.

E

EAP. Protocolo Extensible De la Autentificación. Un punto general al protocolo de punto que apoya mecanismos múltiples de la autentificación. Definido en RFC 2284, EAP ha sido adoptado por IEEE 802.11 en una forma encapsulada para los mensajes de la autentificación que llevaban en un intercambio estándar del mensaje entre un usuario (cliente) y un authenticator. El EAP encapsulado, también conocido como EAP sobre radio del excedente del LAN (EAPoL) y de EAP (EAPoW), permite al servidor de los authenticator authenticar al cliente con un protocolo de la autentificación convenido en por ambas partes. Vea también el tipo de EAP.
EAPA. Protocolo del acceso del punto de acceso de Enterasys. Un punto para señalar el protocolo del datagrama, desarrollado por Enterasys Networks, que define la manera cada punto de acceso (AP) se comunica con un interruptor de RoamAbout en un sistema de la movilidad de las redes de Enterasys. Por medio de EAPA, el APs anuncia su presencia al interruptor de RoamAbout, acepte la configuración de ella, retransmita el tráfico a y desde

él, anuncie la llegada y la salida de los usuarios (clientes), y proporcione la estadística al interruptor de RoamAbout en comando.

EAPoL. Lan excesivo de EAP. Una forma encapsulada del protocolo extensible de la autentificación (EAP), definida en el estándar de IEEE 802.11, que permite que los mensajes de EAP sean llevados directamente por un servicio del Media Access Control del LAN (MAC) entre un cliente sin hilos (o supplicant) y un authenticator. EAPoL también se conoce como radio del excedente de EAP (EAPoW). Vea también EAP.

EAP-TLS. Protocolo extensible de la autentificación con seguridad de la capa de transporte. Un subprotocol de EAP para la autentificación 802.11. EAP-TLS apoya la autentificación mutua y utiliza certificados digitales para satisfacer el desafío mutuo. Cuando un usuario (cliente) solicita el acceso, el servidor de la autentificación responde con un certificado del servidor. El cliente contestó con su propio certificado y también valida el certificado del servidor. De los valores del certificado, el algoritmo de EAP-TLS puede derivar llaves del cifrado de la sesión. Después de validar la certificación del cliente, el servidor de la autentificación envía las llaves del cifrado de la sesión para una sesión particular al cliente. Compare PEAP.

ENLACE. Ruta de comunicación entre dos nodos de una red.

ESTACIÓN BASE. Nombre general que reciben los equipos de una red inalámbrica que se encarga de gestionar las comunicaciones de los dispositivos que forman la red.

Ethernet. La especificación original de Ethernet produjo por Digital, Intel, y Xerox (DIX) que sirvió como la base del estándar de IEEE 802.3. Tipo particular de red de área local. Tiene la particularidad de utilizar el mismo protocolo de comunicaciones que Internet (TCP/IP).

ETSI. Instituto Europeo De los Estándares De las Telecomunicaciones. Una organización no lucrativa que establece telecomunicaciones y los estándares de la radio para Europa.

ESS. Sistema extendido del servicio. Una conexión lógica de los sistemas múltiples del servicio básico (BSSs) conectó con la misma red. El vagar dentro de un ESS es garantizado por el sistema de la movilidad de las redes de Enterasys.

F

FAQ. Frequently-Asked Question, “Preguntas frecuentes”. Lista de preguntas más frecuentes sobre un tema y sus respuestas correspondientes.

FAST ETHERNET. Estándar de la red Ethernet que permite velocidades de transmisión de 100 Mbps. A este estandar se le conoce como 100BaseT y se basa en la norma IEEE 802.3u.

FCC. Comisión Federal De las Comunicaciones. El cuerpo que gobierna de los Estados Unidos para las telecomunicaciones, la radio, la televisión, el cable, y las comunicaciones basadas en los satélites.

FHSS. Separar-espectro de la Frecuencia-Impulzación. Uno de dos tipos de tecnología de la radio del separar-espectro usada en transmisiones sin hilos del LAN (WLAN). La

técnica de FHSS modula la señal de los datos con una señal de portador de banda estrecha que los "saltos" en una secuencia fiable de la frecuencia a la frecuencia en función del tiempo sobre una venda ancha de frecuencias. Se reduce interferencia, porque un interferir de banda estrecha afecta la señal del separar-espectro solamente si ambos están transmitiendo en la misma frecuencia en el mismo tiempo. Las frecuencias de la transmisión son determinadas por un código (de la lupulización que se separa). El receptor se debe fijar al mismo código de la lupulización y debe escuchar la señal entrante en la época y la frecuencia apropiadas de recibir la señal. Compare DSSS.

FTP. *File Transfer Protocol*, “Protocolo de transferencia de archivos”. Protocolo de Internet que permite transferir archivos de una computadora a otro.

G

GATEWAY. Pasarela. Sistema informático que transfiere datos entre dos aplicaciones o redes incompatibles entre sí. El *gateway* adapta el formato de los datos de una aplicación a otra o de una red a otra. Se utiliza generalmente para interconectar dos redes distintas o para hacer que una aplicación entienda los datos generados por otra aplicación distinta.

GBIC. Convertidor de interfaz del gigabit. Un dispositivo caliente-intercambiable de la entrada-salida que tapa en un puerto de Ethernet del gigabit, ligar el puerto a una red fiber-optic o de cobre. La tarifa de transferencia de datos es 1 gigabit por el segundo (Gbps) o más. Empleado típicamente como interfaces de alta velocidad, GBICs permite que usted configure y que aumente fácilmente redes de comunicaciones.
GMK. Llave principal del grupo. Una llave criptográfica derivaba una llave transitoria del grupo (GTK) para el protocolo dominante temporal de la integridad (TKIP) y avanzó el estándar del cifrado (AES).

GPS. *Global Positioning System*, “Sistema de posicionamiento global”. Sistema de satélites que permite identificar la posición exacta de un dispositivo localizado en cualquier punto de la superficie terrestre.

H

H.323. Un sistema de los estándares internacionales del sector de la estandardización de la telecomunicación de la unión de telecomunicaciones (ITU-T) que definen un marco para la transmisión de la voz en tiempo real señala redes packet-switched excesivas del IP.

HACKER. Persona que se dedica a entrar ilegalmente en sistemas y redes de computadoras para robar, modificar o borrar información.

HASH. Un algoritmo unidireccional que de salida la entrada es de cómputo infeasible determinarse. Con un buen algoritmo de cálculo usted puede producir salida idéntica a partir de dos entradas idénticas, pero encontrar dos diversas entradas que produzcan la misma salida es de cómputo infeasible. Las funciones del picadillo se utilizan extensamente en algoritmos de la autentificación y para los procedimientos dominantes de la derivación.

HiperLAN. Red de área local de radio de alto rendimiento. Un sistema de estándares sin hilos de la comunicación del LAN (WLAN) usados sobre todo en países europeos y adoptados por el instituto europeo de los estándares de las telecomunicaciones (ETSI).

HIT. Sistema para medir la carga de trabajo en un servidor. Se le llama *hit* a la transmisión de cada elemento de una página *web*.

HMAC. Código hashed de la autentificación del mensaje. Una función, definida en RFC 2104, para el hashing afinado para la autentificación del mensaje. HMAC se utiliza con MD5 y el algoritmo seguro del picadillo (SHA).

HOMERF. Es una solución de redes inalámbricas para hogares "inteligentes"

HOMOLOGACIÓN. El proceso de certificar un producto o una especificación para verificar que resuelve estándares reguladores

HOST. Cualquier computadora o dispositivo conectado a una red TCP/IP.

HTML. HyperText Markup Language, “Lenguaje de diseño de hipertextos”. Formato especial de archivos sobre el que está basada la estructura del servicio WWW (World Wide Web).

HPOV. Opinión Abierta De Hewlett-Packard. La familia del sistema de la dirección de la red del paraguas (nanómetros) de productos de Hewlett-Packard. La habitación de la herramienta del encargado del interruptor del sistema RoamAbout de la movilidad de las redes de Enterasys obra recíprocamente con el encargado del nodo de red de HPOV (NNM).

HTTPS. El excedente del protocolo de transferencia de hypertext asegura capa de los zócalos. Un Internet Protocol se convirtió por Netscape para cifrar y para descifrar conexiones de red a los servidores del Web. Construido en todos los browsers seguros, HTTPS utiliza el protocolo seguro de la capa de los zócalos (SSL) como subcapa bajo capa de uso regular del HTTP, y las aplicaciones viran 443 hacia el lado de babor en vez del puerto 80 en sus interacciones con la capa más baja, TCP/IP del HTTP. Vea también el SSL.

I

IAB. Internet Basic Borrad, “Consejo de la arquitectura Internet”. Organización existente dentro de la Sociedad Internet (ISOC) que se encarga, entre otras cosas, de aprobar las normas de Internet.

IAS. Servicio De la Autentificación Del Internet. Servidor del RADIO de Microsoft.

IBSS. *Independent Basic Service Set*, “Conjunto de servicios básicos independientes”. Una de las modalidades de comunicación en las que se puede configurar los terminales de una red Wi-Fi. En este caso, la red inalámbrica no dispone de punto de acceso, llevándose a cabo las comunicaciones de forma directa entre las distintas terminales que forman la red. Este modo de conexión también es conocido como *ad hoc*, modo dependiente o de igual a igual (peer-to-peer).

IC. Industria Canadá. El cuerpo que gobierna canadiense para las telecomunicaciones.

ICV. Valor del cheque de la integridad. La salida de un cheque de la integridad del mensaje.

IDENTIDAD AUTENTICADA. En un sistema de la movilidad de las redes de Enterasys, la correspondencia establecida entre un usuario y sus o sus cualidades de la autentificación. Las cualidades de la autentificación del usuario se ligan al usuario, más bien que a un puerto o a un dispositivo físico, sin importar la localización del usuario o el tipo de conexión de red. Porque la identidad autenficada sigue a usuario, él o ella no requieren ningún reautentificaciòn al vagar.

IDS. Intrusión Detección System, “Sistema de detección de intrusos”. Sistema utilizado para detectar los intentos de acceso no autorizados a una computadora o una red.

IEEE. Instituto de ingenieros eléctricos y electrónicos. Una sociedad profesional americana que estándares para la industria de la computadora y de electrónica se convierten en a menudo estándares nacionales o internacionales. En detalle, el IEEE 802 estándares para LANs se sigue extensamente.

IGMP. Protocolo De la Gerencia Del Grupo Del Internet. Un Internet Protocol, definido en el RFC 2236, que permite a una computadora del Internet divulgar su calidad de miembro de grupo del multicast a las rebajadoras vecinas del multicast. El multicasting permite que una computadora en el Internet envíe el contenido a otras computadoras que se han identificado según lo interesado en la recepción de él.

IGMP snooping. Una característica que previene el flujo de los paquetes de la corriente del multicast dentro de un LAN virtual (VLAN) y remite el tráfico del multicast a través de una trayectoria solamente a los clientes que desean recibirla. Un intercambio de la movilidad (interruptor de RoamAbout) utiliza IGMP snooping para supervisar la conversación del protocolo de la gerencia del grupo del Internet (IGMP) entre los anfitriones y las rebajadoras. Cuando el interruptor de RoamAbout detecta un informe de IGMP de un anfitrión para un grupo dado del multicast, agrega el número de acceso del anfitrión a la lista para ese grupo. Cuando detecta un anfitrión de IGMP el dejar de un grupo, el interruptor de RoamAbout quita el número de acceso de la lista del grupo.

INTERNET. Conjunto de redes, de ámbito mundial, conectadas entre si mediante el protocolo IP (*Internet Protocol*). A través de Internet se puede acceder a servicios como WWW, transferencia de archivos, accesos remotos, correo electrónico, entre otros.

INTERFAZ. Un lugar en el cual los sistemas independientes satisfacen y actúan en o se comunican con uno a, o los medios por los cuales la interacción o la comunicación es lograda.

INTRANET. Redes corporativas que realizan el mismo protocolo de Internet. Estas redes conectan a las computadoras de la empresa y ofrecen a sus usuarios (empleados de la empresa) acceder a servicios *web* (o de otro tipo) con información corporativa, documentación, bases de datos, accesos remotos, etc.

IP. *Internet Protocol*, “Protocolo Internet”. Protocolo de nivel de red utilizado tanto por Internet como la mayoría de las redes de área local cableadas e inalámbricas. Mediante el protocolo IP, cualquier paquete puede viajar a través de las distintas redes de Internet hasta llegar a su destino final. IP es la clave del funcionamiento de Internet.

IrDA. (Infrared Data Association) Organización con el fin de crear normas internacionales para el hardware y el software empleados en comunicaciones por infrarrojo, muy importante en comunicaciones inalámbricas

ISL. Acoplamiento De Interswitch. Un protocolo propietario del Cisco para interconectar los interruptores múltiples y mantener la información virtual del LAN (VLAN) como tráfico viaja entre los interruptores. Trabajando de una manera similar al trunking de VLAN, descrito en el estándar de IEEE 802.1Q, el ISL proporciona capacidades de VLAN mientras que el funcionamiento completo de la alambre-velocidad que mantiene en Ethernet se liga en modo full-duplex o half-duplex. El ISL funciona en un punto para señalar el ambiente y apoya VLANs hasta 1000.

ISM. *Industrial, Scientific and Medicine*, “Industrial, científica y médica”. Banda de frecuencias radioeléctricas reservadas a aplicaciones de este tipo. Ésta es la banda de frecuencia en las que actúa Wi-Fi.

ISO. *International Organization for Standardization*. Una organización internacional de los cuerpos nacionales de los estándares de muchos países. La ISO ha definido un número de estándares de la computadora, incluyendo la arquitectura estandardizada del Open Systems Interconnection (OSI) para el diseño de red.

ISP. *Internet Service Provider,”*Proveedor de acceso a Internet”. Cualquier empresa que facilite el acceso a Internet a sus clientes o usuarios. Estos usuarios pueden ser personas particulares u otras empresas.

IV (Vector de la inicialización). En el cifrado, los datos al azar hacían un mensaje único

K

KBPS. Kilobits por segundo. Es la unidad de velocidad de transferencia de datos. Un kilobit por segundo significa que se transfieren 1.024 bits cada segundo.

L

L2TP. *Layer 2 Tunnelling Protocol*, “Protocolo de tunelado de capa 2”. Protocolo del IETF utilizado para crear redes privadas virtuales.

LAN. *Local Area Network*, “Red de área local”.

LINK. Enlace.

M

MAC. Media Access Control. Código de la autentificación del mensaje. Un picadillo afinado verificaba integridad del mensaje. En un picadillo afinado, la llave y el mensaje son entradas al algoritmo del picadillo.

MAC Ardes. Dirección del Media Access Control. Una dirección hexadecimal 6-byte que un fabricante asigna al regulador de Ethernet para un puerto. Los protocolos de la Alto-capa utilizan el MAC address en la subcapa del MAC de la capa de transmisión de datos (capa 2) para tener acceso a los medios físicos. La función del MAC determina el uso de la capacidad de la red y las estaciones que se permiten utilizar el medio para la transmisión.

MAC Addrees glob. Una convención de las redes de Enterasys para las direcciones del Media Access Control (MAC) o los sistemas que emparejan de direcciones del MAC por medio de caracteres sabidos más un carácter "del asterisco del" comodín (*) que está parado para a partir 1 octeto a 5 octetos de la dirección.

MASCARA DE SURED. Número de 32 bits utilizado para identificar la parte de la dirección IP que identifica a la red y la parte que identifica la computadora o equipo de red.

MBPS. Megabits por segundo. Unidad de medida de la velocidad de transferencia de datos. Un megabit por segundo significa que la transfieren 1.048.576 (1.024x1.024) bits cada segundo.

MIC. Código de la integridad del mensaje. El término de IEEE para un código de la autentificación del mensaje (MAC). Vea el MAC.

MODEM. Equipo que se conecta a la computadora para poder transmitir datos por medio de transmisión analógica. En el caso de las líneas telefónicas, el módem convierte las señales digitales propias de la computadora en señales analógicas, aptas para ser transmitidas por una línea telefónica.

MODO AD HOC. Red inalámbrica Wi-Fi que no dispone de un punto de acceso. En este caso, las comunicaciones se llevan a cabo directamente entre las distintas terminales que forman la red. Este modo de conexión también es conocido como modo IBSS, modo independiente o de igual a igual (peer-to-peer).

MODO INFRAESTRUCTURA. Redes inalámbricas Wi-Fi que disponen de un equipo central, conocido como punto de acceso, que se encarga de gestionar las comunicaciones (internas y externas) de todos los dispositivos que forman la red. Este modo de conexión también es conocido como BSS.

MODULACIÓN. Hecho de distorsionar una señal eléctrica o radioeléctrica para que contenga la información a transmitir. Al proceso contrario, extrae la información de una señal modulada, se le llama modulación.

MPDU. Unidad de datos de protocolo del MAC. En IEEE 802.11 comunicaciones, la unidad de datos (o marco) que dos puntos de acceso de servicio del Media Access Control del par (MAC) (savias) intercambian con los servicios de la capa física (PHY). Un MPDU consiste en los jefes y una unidad de datos de servicio del MAC (MSDU) del MAC.

MS-CHAP-V2. Del protocolo de la autentificación del apretón de manos del desafío de Microsoft. Extensión de Microsoft A AGRIETAR. MS-CHAP-V2 es un protocolo mutuo de

la autentificación, definido en el RFC 2759, que también permite una sola conexión en un ambiente de la red de Microsoft.

MSDU. Unidad de datos de servicio del MAC. En IEEE 802.11 comunicaciones, la carga útil de los datos encapsulada dentro de una unidad de datos de protocolo del MAC (MPDU).
MSS. Software del sistema De la Movilidad. El sistema operativo de Enterasys, accesible a través de una comando-línea interfaz (CLI) o la habitación de la herramienta del encargado del interruptor de RoamAbout, que permite a productos del sistema de la movilidad de las redes de Enterasys funcionar como solo sistema. El software del sistema de la movilidad (MSS) realiza la autentificación, la autorización, y funciones de la contabilidad (AAA); maneja los interruptores y los puntos de acceso (APs) de RoamAbout.

MTU. *Maximum Transmission Unit*. El tamaño del paquete más grande que se puede transmitir sobre un medio particular. Los paquetes que exceden el valor del MTU de tamaño se hacen fragmentos o se dividen en segmentos, y después se vuelven a montar en el extremo de recepción. Si la fragmentación es no apoyada o posible, se cae un paquete que excede el valor del MTU.

MULTIMEDIA. Sistema que integra sonido, textos e imágenes, en único soporte.

N

NAT.Conversión de dirección de red. La capacidad, definida en RFC 3022, de usar un sistema de las direcciones reutilizables del IP para el tráfico interno en un LAN, y un segundo sistema de las direcciones global únicas del IP para el tráfico externo.

NAVEGADOR. Programa que permite acceder a los recursos web de Internet. Adicionalmente, un navegador puede utilizarse también para acceder a otros recursos, como correo electrónico, Internet explorer y Netscape son los dos navegadores más comunes.

NIC. *Network Interface Card*, Tarjeta interfaz de red". Tarjeta de red que necesita cualquier equipo para conectarse a una red de área local (cableada o inalámbrica).

NODO. Cualquier computadora conectada a una red.

O

OFDM. Multiplexación de división de frecuencia ortogonal. Una técnica de la modulación que envía datos a través de un número de subcarriers estrechos dentro de una banda de frecuencia especificada. Los estándares sin hilos IEEE 802.11a y IEEE 802.11g del establecimiento de una red se basan en OFDM.

OFF-LINE. Estar desconectado. Trabajar *off-line* en Internet quiere decir que se esta trabajando desconectado de la red. Lo opuesto sería trabajar *on-line*, o trabajar conectado a la red.

ON-LINE. Estar conectado. Trabajar *on-line* en Internet quiere decir que se esta trabajando estando conectado a la red. Lo opuesto sería trabajar *off-line*, o trabajar mientras se esta desconectado a la red.

P

PAT. Conversión de dirección portuaria. Un tipo de conversión de dirección de red (NACIONAL) en que cada computadora en un LAN se asigna el mismo IP address, solamente un diverso número de acceso.

PAQUETE. Cada uno de las trazas en los que un protocolo de comunicaciones divide el flujo de información para transmitirlo por la red.

PASSWORD. Contraseña.

PCI. Interconexión de componentes periódicos. Especificaciones creadas por Intel y que definen un sistema de bus local que permiten conectar al PC hasta 10 tarjetas de periféricos. El estándar PCI ha venido a reemplazar al antiguo estándar (*Industry Standard Srchiteture*).

PDA. Personal Digital Assistant - Asistente Personal Digital.

PEAP. Protocolo Extensible Protegido De la Autentificación. Una extensión del bosquejo al protocolo extensible de la autentificación con la seguridad de la capa de transporte (EAP-TLS), desarrollada por Microsoft Corporation, Cisco Systems, y RSA Data Security, Inc. TLS se utiliza en la parte 1 de PEAP para autenticar el servidor solamente, y evita así de tener que distribuir certificados del usuario a cada cliente. La parte 2 de PEAP realiza la autentificación mutua entre el cliente de EAP y el servidor. Compare EAP-TLS.

PEM. Correo Aislamiento-Realzado. Un protocolo, definido en RFC 1422 a RFC 1424, porque transporte de certificados digitales y de peticiones de firma del certificado sobre el Internet. El formato del PEM codifica los certificados en base de una jerarquía X.509 de las autoridades del certificado (CAs). La codificación Base64 se utiliza para convertir los certificados al texto del ASCII, y el texto codificado es incluido en medio COMIENZA EL CERTIFICADO y delimitadores del CERTIFICADO del EXTREMO.

PIM. Protocolo Independiente del multicast del protocolo. Un protocolo del encaminamiento del multicast de protocol-independiente que apoya millares de grupos, una variedad de usos del multicast, y tecnologías existentes del subnetwork de la capa 2. PIM se puede funcionar en dos modos: denso y escaso. En el modo denso de PIM (PIM-DM), los paquetes se inundan en todos los interfaces salientes a muchos receptores. El modo escaso de PIM (PIM-SM) limita la distribución de los datos a un número mínimo de rebajadoras extensamente distribuidas. Se envían los paquetes de PIM-SM solamente si se solicitan explícitamente en un punto rendezvous (RP).

PKI. Infraestructura Publico-llave. Software que permite a usuarios de una red pública insegura tales como el Internet intercambiar la información con seguridad y privado. El PKI utiliza la criptografía de la público-llave (también conocida como criptografía asimétrica) para autenticar el remitente del mensaje y para cifrar el mensaje por medio de un par de llaves criptográficas, un público y uno privados. Un Certificate Authority confiado en (CA) crea ambas llaves simultáneamente con el mismo algoritmo. Una autoridad del registro (RA) debe verificar el Certificate Authority antes de que un certificado digital se publique a un solicitante.

PPTP. *Point to Point Tunnelling Protocol*, “Protocolo de tunelado punto a punto”. Protocolo de red privada virtual incluidos en los sistemas operativos Windows.

PROTOLO. Conjunto de normas que indican como deben de actuar los computadoras para comunicarse entre sí. Los protocolos definen desde para que se va a usar cada hilo de un conector hasta el formato de los mensajes que se intercambian los computadoras.

PUERTO. Puede tener dos significados: por un lado, puede tratarse de un número que identifica una aplicación particular de Internet. Cuando una computadora envía un paquete a otro, el paquete contiene la información de la aplicación que está intentando comunicarse con la computadora remota. Esta identificación se hace mediante un número de puerto (port number). Por otro lado, también se conoce como puerto al conector físico que utilizan las computadoras para comunicarse con el exterior.

R

ROAMING. La capacidad de un usuario sin hilos (cliente) de mantener el acceso de red al moverse entre los puntos de acceso (APs).

RSA. Un algoritmo publico-llave se convirtió en 1977 por RSA Data Security, Inc., usado para el cifrado, firmas digitales, e intercambio dominante.

RSN. Red robusta de la seguridad. Un LAN seguro de la radio (WLAN) basado en el estándar de IEEE que se convierte 802.11i.

RSSI. Indicación recibida de la fuerza de la señal. La fuerza recibida de una señal entrante de la radiofrecuencia (RF), medida típicamente en decibelios refirió a 1 milivatio (dBm).

S

SEGURIDAD ACL. Access Control List de la seguridad. Una lista pedida de las reglas para controlar el acceso a y desde una red determinándose si remitir o filtrar los paquetes que son que la incorporan o que salen. Asociando una seguridad ACL a un usuario particular, el puerto, el LAN virtual (VLAN), o el puerto virtual en un interruptor de RoamAbout controla el tráfico de la red a o desde el usuario, el puerto, el VLAN, o el puerto virtual.

SENTRYSWEEP^{TM} . Un barrido de la detección de la radiofrecuencia (RF) que funciona continuamente en las radios lisiadas en un dominio de la movilidad grupo. Vea también el barrido de la detección del RF.

SESIÓN. Un sistema relacionado de transacciones de la comunicación entre un usuario autenticado (cliente) y la estación específica a quienes el cliente está limitado.

SHA. Asegure el algoritmo de cálculo. Un algoritmo de cálculo unidireccional usado en muchos algoritmos de la autentificación y también para la derivación dominante en muchos algoritmos. Un SHA produce un picadillo 160-bit.

SECRETO COMPARTIDO. Una llave estática distribuida por un mecanismo out-of-band al remitente y al receptor. También conocido como llave compartida o preshared la llave (PSK), un secreto compartido se utiliza como entrada a un algoritmo unidireccional del picadillo. Cuando un secreto compartido se utiliza para la autentificación, si la salida del picadillo del remitente y del receptor es igual, comparten el mismo secreto y se authentican. Un secreto compartido se puede también utilizar para la generación de la llave del cifrado y la derivación de la llave.

SIP. Protocolo De la Inicialización De la Sesión. Un protocolo que señala que establece llamadas en tiempo real y redes excesivas del IP de las conferencias.

SSH. Asegure el protocolo de la cáscara. A Telnet-como el protocolo que establece una sesión cifrada.

SSID. Mantenga el identificador determinado. El nombre único compartido entre todas las computadoras y otros dispositivos en un LAN sin hilos (WLAN).

SSL. Asegure el protocolo de capa de los zócalos. Un protocolo desarrollado por Netscape para manejar la seguridad de la transmisión del mensaje sobre el Internet. El SSL ha sido tenido éxito por el protocolo de la seguridad de la capa de transporte (TLS), que se basa en el SSL. Los zócalos parte del término refieren al método de los zócalos de pasar datos hacia adelante y hacia atrás entre un cliente y un programa del servidor en una red o entre las capas del programa en la misma computadora. El SSL utiliza el sistema dominante público-y-privado del cifrado de RSA Data Security, Inc., que también incluye el uso de un certificado digital. Vea también HTTPS; TLS.

.

STP. Atravesar Protocolo Del Árbol. Un protocolo de la gerencia del acoplamiento, definido en el estándar de IEEE 802.1D, que proporciona redundancia de la trayectoria mientras que previene lazos indeseables en una red. STP también se conoce como atravesar protocolo del puente del árbol.

T

TCP/IP. Protocolo de control de transmisión/Protocolo Internet. Normas técnicas de actuación que fijan el interfuncionamiento de las redes que forman parte de Internet.

TDMA (time division multiple access) TDMA divide un canal de frecuencia de radio en varias ranuras de tiempo

TELNET. Aplicación de Internet que permite el acceso remoto a otros computadoras de la red y trabajar como si se fuese un usuario local. Mediante Telnet se puede tener acceso a todas las facilidades de la computadora remoto.

TKIP. Protocolo Dominante Temporal De la Integridad. Un protocolo sin hilos del cifrado que fija los problemas sabidos en el protocolo Atar con alambre-Equivalente de la aislamiento (WEP) para IEEE existente 802.11 productos. Como WEP, las aplicaciones RC4 de TKIP que cifran, pero agregan funciones tales como una llave del cifrado 128-bit, un vector de la inicialización 48-bit, un nuevo código de la integridad del mensaje (MIC), y

el vector de la inicialización (iv) que ordena reglas para proporcionar una protección mejor. Vea también 802.11i; CCMP.

TLS. Protocolo de la seguridad de la capa de transporte. Una autentificación y un cifrado protocolan que es el sucesor a los zócalos seguros acoda el protocolo (SSL) para la transmisión privada sobre el Internet. Definido en RFC 2246, TLS provee de la autentificación mutua el nonrepudiation, el cifrado, la negociación del algoritmo, la derivación dominante segura, y la comprobación de la integridad del mensaje. TLS se ha adaptado para el uso en LANs sin hilos (WLANs) y se utiliza extensamente en la autentificación de IEEE 802.11. Vea también EAP-TLS; PEAP; TTL.

TLV. Tipo, longitud, y valor. Una metodología para los parámetros de la codificación dentro de un marco. El tipo indica el tipo de un parámetro, longitud indica la longitud de su valor, y del valor indica el valor de parámetro.

TTLS. Seguridad De la Capa De Transporte De Tunneled. Un método extensible del protocolo de la autentificación (EAP) se convirtió por el canguelo Software, Inc., y Crético para la autentificación 802.11. Las TTL utilizan una combinación de certificados y desafío y respuesta de la contraseña para la autentificación. El intercambio entero del subprotocol de EAP de los pares del atribuir-valor ocurre interior un túnel cifrado de la seguridad de la capa de transporte (TLS).

U

UIT. Unión Internacional de Telecomunicaciones.

UNIX. Sistema operativo multitarea y multiprogramación.

UPLINK. Enlace de subida. Suele hacer referencia al puerto donde se pueden conectar otros hubs o switches para extender la red.

URL. Localizador universal de recursos. Forma particular que se tiene en Internet de especificar las direcciones de sus distintos recursos. Un URT es una dirección.
USB. Interfaz serie de la computadora que permite conectar hasta 127 dispositivos a una velocidad de 1,5 ó 12 Mbps. Además, tiene la particularidad de que no es necesario apagar el computadora para conectar o desconectar los dispositivos.

USUARIO. Una persona que utiliza a cliente. En un sistema de la movilidad de las redes de Enterasys, el username pone e un índice y se asocian a los usuarios a cualidades de la autorización tales como calidad de miembro de grupo de usuario.

V

VIRUS. Programa que tiene la característica de auto reproducirse. Los virus pueden ser malignos si causan efectos destructivos en las computadoras que va contaminando, o benignos, si no van causando daños.

VLAN. LAN Virtual. Un sistema de los puertos que comparten una sola red de la capa 2. Porque los puertos que constituyen un VLAN pueden estar en un solo dispositivo de la red o dispositivos múltiples, VLANs le permite repartir una red física en las redes lógicas que resuelven las necesidades de su organización.

VLAN glob. Una convención de nombramiento para aplicar la autentificación, la autorización, y las cualidades de la contabilidad (AAA) en la política de la localización en un RoamAbout cambian a unos o más usuarios, basados en una cualidad virtual del LAN (VLAN). Para especificar todo el VLANs, utilice los caracteres del comodín del doble-asterisco (* *). Emparejar cualquier número de caracteres hasta, pero no incluyendo un carácter del delimitador en el glob, utiliza el comodín del solo-asterisco. Los caracteres válidos del delimitador del glob de VLAN son en (@) la muestra y el punto (.). Ve también la política de la localización; Glob del MAC address; glob del usuario.

VoIP. IP excesivo de la voz. La capacidad de una red del IP de llevar voz del teléfono señala como paquetes del IP en conformidad con la especificación internacional H.323. VoIP del sector de la estandardización de la telecomunicación de la unión de telecomunicaciones (ITU-T) permite a una rebajadora transmitir llamadas telefónicas y faxes sobre el Internet sin pérdida en funcionalidad, confiabilidad, o calidad de la voz.

VPN. Red Privada Virtual. Sistema de cifrado que permite crear redes completamente privadas en cuanto a seguridad y confidencialidad en un entorno no seguro.

VSA. Cualidad Vendedor-especifica. Un tipo de cualidad del RADIO que permite a un vendedor ampliar operaciones del RADIO para caber sus propios productos, sin estar en conflicto con cualidades existentes del RADIO o el VSAs de otras compañías. Las compañías pueden crear nuevas cualidades de la autentificación y de la contabilidad como VSAs.

W

WAN. Red de área extensa. Red formada por la interconexión de distintas redes de área local sustituidas en distintos edificios. También recibe este nombre el puerto del punto de acceso donde se deben conectar la conexión con la red de área local.

WAP. Protocolo de Aplicaciones Inalámbricas. Protocolo utilizado para que los terminales móviles puedan acceder a servicios y aplicaciones de Internet.

WECA. Alianza Sin hilos De la Compatibilidad De Ethernet. Vea La Alianza Wi-Fi.

WEP. Protocolo Atar con alambre-Equivalente del aislamiento. Un protocolo de la seguridad, especificado en el estándar de IEEE 802.11, que procura proveer de un LAN sin hilos (WLAN) un nivel mínimo de la seguridad y de la aislamiento comparables a un LAN atado con alambre típico. WEP cifra los datos transmitidos sobre el WLAN para proteger la conexión sin hilos vulnerables entre los usuarios (clientes) y los puntos de acceso (APs). Aunque es apropiado para la mayoría del uso casero, WEP es débil y fundamental dañado para el uso de la empresa. Compare AES; CCMP; TKIP.

Wi-Fi. Una organización formó conduciendo el equipo y abastecedores de software sin hilos, para certificar todo el IEEE 802.11 productos sin hilos del LAN (WLAN) para la interoperabilidad y promover el término Wi-Wi-Fi como su marca global. Solamente los productos que pasan la prueba de la alianza Wi-Wi-Fi pueden ser certificados. Los productos certificados se requieren para llevar un sello que identifica en su empaquetado indicando que el producto es Wi-Wi-Fi certificado e indicando la venda de la

radiofrecuencia usada (2.4 gigahertz para 802.11b y 5 gigahertz para 802.11a, por ejemplo). La alianza Wi-Wi-Fi era conocida antes como la alianza sin hilos de la compatibilidad de Ethernet (WECA).

WISP. Internet Service Provider sin hilos. Una compañía que proporciona LAN público de la radio (WLAN) mantiene.

WLAN. Lan Sin hilos. Un LAN a el cual los usuarios móviles (clientes) pueden conectar y comunicarse por medio de ondas de radio de alta frecuencia más bien que de alambres. WLANs se define en el estándar de IEEE 802.11.

WPA. Acceso Protegido Wi-Wi-Fi. La versión de la alianza Wi-Wi-Fi del protocolo dominante temporal de la integridad (TKIP) que también incluye un código de la integridad del mensaje (MIC) conocido como Michael. Aunque WPA proporciona mayor seguridad sin hilos que el protocolo Atar con alambre-Equivalente de la aislamiento (WEP), WPA no es tan seguro como IEEE 802.11i, que incluye ambo el cifrado RC4 usado en WEP y el cifrado estándar avanzado del cifrado (AES), pero todavía no es ratificado por IEEE. Vea también AES; RC4; TKIP.

WPA IE. Un sistema de los campos adicionales en un marco sin hilos que contienen el Wi-Wi-Fi protegió la información del acceso (WPA) para el punto de acceso (AP) o el cliente. Por ejemplo, un punto de acceso utiliza el IE de WPA en un marco del faro para anunciar las habitaciones de la cifra y los métodos de la autentificación que el punto de acceso apoya para su SSID cifrado.

2.5G. También conocido como GPRS (General Packet Radio Service), es una tecnología digital de telefonía móvil. Es considerada la generación 2.5, entre la segunda generación

3G FORMATO contenedor de multimedia definido por Third Generation Partnership Project (3GPP) para ser usado en teléfonos celulares de tercera generación (3G).

BIBLIOGRAFIA

BIBLIOGRAFIA

(Carballar, 1996)	José A. Caballar, "Instalación, Seguridad y Aplicaciones" Ed. Alfa-Omega
(Caballar)	José A. Caballar, ""WI-FI, Cómo construir una red inalámbrica" Ed. Ra-Ma 2ª Edición
(Flickenger)	Rob Flickenger, "Wireless los mejores trucos" Ed. Anaya multimedia.
(Raya)	J.L Raya, L. Raya "Redes Locales" Ed. Ra-Ma 3ª Edición.
(F.J)	F.J. • "Instalación y mantenimiento de servicios de redes locales" Ed. Ra-Ma
(Sanchez)	Jesús Sánchez Allende, Joaquín López Lérida, • "Redes, iniciación y referencia" Ed. McGraw-Hill
(Derfler)	Frank Derfler, • "Redes Lan y Wan" Ed. Plentice Hall
(Rábago)	J. Félix Rábago, • "Redes locales" Ed. Anaya.
	Manual de instalación RoamAbout.
(enterasys)	http://www.enterasys.com/support/manuals.html
(aulaclic)	http://www.aulaclic.es/articulos/wifi.html
(munodgeej)	http://www.munodgeej.net/archivos/asegurar-una-red-wifi/
(tenowifi)	http://www.tecnowifi.com/category/redes-wifi/
(trucoswindows)	http://www.trucoswindowa.net/redes-wifi.html
(wi-fi)	www.Wi-Fi.org
(wi-fiplanet)	www.Wi-Fiplanet.com

(links)	www.linksys.com
(ciudadwireless)	www.ciudadwireless.com
(ecommwireless)	www.ecommwireless.com/calculations
(decibleproducts)	www.decibleproducts.com/software
(lawebdelprogramador)	www.lawebdelprogramador.com