UNIVERSIDAD POLITÉCNICA SALESIANA

FACULTAD DE INGENIERÍAS

SEDE QUITO – CAMPUS SUR

CARRERA DE INGENIERÍA DE SISTEMAS

MENCIÓN TELEMÁTICA

"ANÁLISIS Y DISEÑO DE LA RED INALÁMBRICA Y DEL SISTEMA DE CONTROL DE ACCESO EN EL EDIFICIO MATRIZ DE LA COMPAÑÍA XEROX DEL ECUADOR UTILIZANDO TECNOLOGÍA Wi-Fi (802.11) CON SEGURIDAD EN PLATAFORMAS WINDOWS"

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

BLANCA ELIZABETH ZHUNIO SALINAS

MARCO VINICIO SOCASI SANGOQUIZA

DIRECTOR: ING. JAIME GALLARDO

Quito, Marzo 2010

DECLARACIÓN

Nosotros, Blanca Elizabeth Zhunio Salinas y Marco Vinicio Socasi Sangoquiza, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y la normatividad institucional vigente.

_____ _____

Blanca Elizabeth Zhunio Salinas Marco Vinicio Socasi Sangoquiza

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Blanca Elizabeth Zhunio Salinas y Marco Vinicio Socasi Sangoquiza, bajo mi dirección.

_____

Ing. Jaime Gallardo
Director de Tesis

AGRADECIMIENTO

Al término de esta etapa de nuestras vidas, quisiéramos expresar un profundo agradecimiento a quienes de una u otra manera nos alentaron a lograr esta hermosa realidad.

En primer lugar quisiéramos agradecer al, Ing. Jaime Gallardo, por su incondicional ayuda como tutor a través de todo este proceso; sin su paciencia, conocimiento, y apoyo el desarrollo de este proyecto no habría tenido éxito.

Asimismo, al personal de Xerox gracias por su colaboración y en especial al personal del departamento de sistemas, no sólo por permitirnos observar tan de cerca el desempeño de la red, sino por todos sus acertados comentarios, gracias.

Finalmente, lo más importante: agradecer profundamente a nuestras familias por su eterno apoyo moral y su incondicional amor.

A todos Mil Gracias.

Este trabajo lo dedico a mis padres, mis hermanos Roberto, Cris por todo su esfuerzo y apoyo que han fortalecido mi espíritu para lograr este objetivo y nuevos retos en mi vida profesional y a todas y cada una de las personas que aportaron a que este proyecto llegue a su fin.

Marco

A mis hijos Nicole y Mateo quienes me han impulsado a luchar y a seguir adelante, a mi esposo Juan Carlos por su amor y comprensión, a mis hermanas y en especial a mi madre por estar siempre a mi lado en los buenos y malos momentos de mi vida y por último a mi querida abuelita a quien jamás olvidaré. A todos ustedes les dedico este trabajo y todos los logros de mi vida. ! Los amo y los amaré por siempre!

Eli

CONTENIDO

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

CAPÍTULO V

CAPÍTULO VI

CAPÍTULO VII

RESUMEN

Esta Tesis se enfoca en el análisis y diseño de una red inalámbrica basada en el estándar 802.11 b y el análisis y diseño de un Sistema de Control de Accesos para Xerox, para luego acoplarlos en un solo sistema y finalizando con un estudio de costos y rentabilidad del proyecto en caso de implementación; para lo cual se desarrollaron los siguientes capítulos:

Capítulo I. Situación Inicial del proyecto.-El primer capítulo de esta tesis busca dar una visión general sobre la problemática de la red actual de Xerox, partiendo de su situación inicial ; además expone las dificultades que existen para el manejo del control de accesos dentro del edificio donde laboran los empleados de Xerox , de esta forma motivando a los autores de esta tesis a establecer objetivos y requerimientos tanto de la red inalámbrica y el Sistema de Control de Accesos; dando así inicio al desarrollo de esta tesis

Capítulo II.-Redes inalámbricas 802.11.- En esta sección de la tesis se describe el aspecto teórico de las redes inalámbricas, donde se contemplan sus estándares, componentes físicos, topologías, tecnologías, seguridades etc.

Capítulo III.-Hardware de la red inalámbrica.-Describe los componentes físicos de una red inalámbrica a manera general tales como tarjetas inalámbricas, antenas, puntos de acceso, amplificadores de radio frecuencia, etc., incluyendo también una descripción a detalle de cada uno de estos elementos de hardware existentes en el mercado.

Capítulo IV.-Sistemas de Control de Acceso.-El capítulo comienza con una pequeña introducción sobre la importancia de los Sistemas de Control de acceso, luego contempla el tema de las tecnologías aplicadas al control de accesos entre las que citamos algunas como código de barras, banda magnética, proximidad, etc. Luego se describen los componentes y funcionamiento de un sistema de control a nivel general, dirigiéndose de esta forma a lo que es el diseño del sistema de Control de Accesos donde como primer punto se selecciona el tipo de

tecnología a usarse en el diseño del sistema tomando en cuenta las ventajas y desventajas de cada una de las tecnologías expuestas al principio de este capítulo, en base a esta selección se proponen dos diseños, de los cuales se escogió uno y por último se presenta un resumen del software a emplearse en este sistema de Control de Accesos.

Capitulo V. Diseño de la Red Inalámbrica local 802.11.-En este capítulo primero se determina el modo de configuración de la red inalámbrica tomando en cuenta primero las políticas de telecomunicaciones establecidas en nuestro país para las redes inalámbricas y luego el número de puntos de acceso a emplearse, segundo se selecciona el equipo inalámbrico a usarse haciendo una comparación entre los equipos existentes en el mercado citados en el capítulo II llegando así a escoger el equipo adecuado, ya en el diseño de la red se realiza un estudio de parámetros técnicos de la red como son la cobertura, alcance, canales de comunicación, cálculo del número y ubicación de los puntos de acceso a través de cálculos matemáticos a continuación el direccionamiento IP para todos los equipos de la red inalámbrica y el sistema de control y por último la integración del sistema de Control de Accesos a la red inalámbrica.

Capítulo VI. Análisis de Costos y rentabilidad del proyecto.- Este capítulo presenta la inversión que Xerox del Ecuador tendría que realizar, y la reducción de gastos que obtendría en caso de implementar el proyecto, finalmente se establece la rentabilidad del proyecto a través de una relación entre la inversión y la reducción de costos

Capítulo VII. Conclusiones y Recomendaciones.- Presenta todos los logros obtenidos durante el desarrollo de esta tesis; además finaliza con recomendaciones que los autores de este proyecto sugieren con el propósito de manejar y mejorar el diseño de la red inalámbrica y el Sistema de Control de Accesos

CONTENIDO DE FIGURAS

Pág.

CONTENIDO DE TABLAS

Pág.

PRESENTACIÓN

La elaboración de este proyecto nace con la necesidad que tienen los usuarios de la red actual de Xerox de acceder a la información y recursos en tiempo real sin estar físicamente conectados a un determinado lugar, gracias a la tecnología de distribución de banda ancha Wi-Fi (Wireless Fidelity), es posible dar solución a este problema.

Por otro lado se analiza la falta de control que existe en el momento del ingreso de personas al edificio de Xerox, por eso se propone el diseño de un sistema de control de acceso electrónico que mejore este proceso.

Como una solución final se propone el acoplamiento del sistema de control de acceso electrónico a la red inalámbrica

Esperamos que el contenido de este documento llene toda expectativa con respecto al tema planteado en este proyecto de tesis

CAPÍTULO I

SITUACIÓN INICIAL DEL PROYECTO

1.1 INTRODUCCIÓN

Las tecnologías Inalámbricas, basadas principalmente en los estándares 802.11, también comúnmente conocidas como redes Wi-Fi[1] se están convirtiendo en una alternativa económica y funcional al acceso tradicional a los servicios de datos e Internet. Dichas tecnologías han ganado mucha popularidad en los últimos tiempos, esta popularidad ha crecido hasta tal punto en que las podemos encontrar en casi cualquier ámbito de nuestra vida cotidiana, teléfonos inalámbricos, ordenadores, teléfonos móviles son algunos de los ejemplos más evidentes; es por eso que estas tecnologías están teniendo una gran difusión, sobre todo por grupos de usuarios que desean crear pequeñas redes independientes.

Gracias a las ventajas que ofrecen este tipo de redes, se está desarrollando un mercado con gran potencial y futuro. Las aplicaciones son múltiples, por lo que la incorporación en las empresas, hogares, dependencias públicas y privadas (universidades, bibliotecas, colegios, hoteles..., etc.), medios de transporte etc. está garantizado.

La bondad de las tecnologías inalámbricas para cubrir y dar acceso a redes y servicios como Internet en entornos donde los usuarios se desplazan de unas oficinas a otras, las hace merecedoras de una atención especial para el desarrollo de este proyecto de tesis, debido a que Xerox del Ecuador busca brindar a los usuarios ahorro de tiempo y sin complicaciones si disponen de un acceso transparente a la red de área local (LAN). La conexión es prácticamente instantánea y está disponible desde cualquier lugar con cobertura inalámbrica;

[1] Wi-Fi: (Wireless Fidelity) Conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11

además la información en línea está siempre disponible, la integración de nuevos dispositivos y aplicaciones en el entorno de la tecnología inalámbrica también mejora considerablemente y por último el tamaño de la red se puede modificar con gran facilidad, en respuesta a los distintos niveles de demanda conforme la compañía cambia, incluso a diario si es preciso. Es mucho más sencillo implementar una mayor concentración de puntos de acceso inalámbrico en una ubicación concreta que aumentar el número de puertos de red con cable.

Este proyecto de tesis además de cumplir con las expectativas de Xerox, en cuanto a la red LAN del edificio Matriz plantea también el diseño de un Sistema del control de acceso operado y administrado a través de la red inalámbrica, mantendrá el control desde una locación central y proveerá los reportes sobre los movimientos de los empleados y visitantes a través del edificio.

En este trabajo se centrarán todos los esfuerzos en establecer una comunicación en las mejores condiciones posibles dentro de la red del edificio de Xerox.

1.2 ANTECEDENTES

El presente proyecto en un principio busca analizar la situación de la red interna en el edificio matriz de la Compañía Xerox del Ecuador que actualmente está en funcionamiento, con el fin de diseñar una solución inalámbrica óptima que sirva de apoyo o reemplazo de la red actual en el edificio matriz de la compañía, y al mismo tiempo brindar alternativas tecnológicas acerca de los equipos para la red que permitirán cumplir con los requerimientos de Xerox, especialmente en lo que se refiere a la seguridad dentro de la red , haciendo que el flujo de información sea más ágil y oportuno para el mejor desenvolvimiento del personal que utilizan los servicios de dicha red.

La falta de control de acceso del personal que ingresa y sale del edificio no es registrada lo que hace necesario el diseño de un sistema de control de acceso que sea administrado a través de la red.

1.3 OBJETIVOS

1.3.1 GENERAL

Diseñar la red inalámbrica e integrar un sistema de control de acceso usando la tecnología Wi-Fi (Estándar 802.11) con seguridad en plataformas Windows.

1.3.2 ESPECÍFICOS

- ✓ Realizar un análisis de la red que actualmente funciona en el edificio matriz de la Compañía Xerox del Ecuador.
- ✓ Comprender el comportamiento de las redes inalámbricas
- ✓ Definir los parámetros técnicos, económicos y de servicio para la futura Implementación de la red inalámbrica.
- ✓ Investigar acerca de la tecnología inalámbrica para el control de acceso en edificaciones.
- ✓ Analizar las especificaciones recogidas para proceder a la elaboración de los pasos exigidos para el diseño del sistema de control.
- ✓ Brindar alternativas de hardware para la red inalámbrica y para el sistema de control de acceso.
- ✓ Buscar la mejor opción que permita mantener la seguridad de la información en la red.
- ✓ Analizar los costos y beneficios que brindará una red inalámbrica en el edificio matriz de la Compañía Xerox del Ecuador.

1.4 JUSTIFICACIÓN

La elaboración de este proyecto se justifica en base a la necesidad de los usuarios del edificio matriz de la Compañía Xerox del Ecuador para acceder a la información y recursos en tiempo real sin estar físicamente conectados a un determinado lugar. Mediante la implementación a futuro de la red y gracias a la

tecnología Wi-Fi (802.11 Wireless Fidelity), tanto el personal del edificio como sus visitantes autorizados podrán manipular de mejor manera la información. Además Wi-Fi ofrece la posibilidad de conectarse a velocidades entre 1 Mbps y más de 50 Mbps mediante el uso de las ondas de radio.

Por otra parte el edificio matriz de la Compañía Xerox del Ecuador posee deficiencias en el manejo del personal propio y visitantes al igual que en el aspecto de vigilancia dentro de las instalaciones del edificio, por tal razón se ha considerado imprescindible buscar mecanismos tales como los sistemas de control de acceso que nos permita solucionar dichas deficiencias.

Siempre que exista información a ser compartida requiere que se garantice la fiabilidad, integridad y confidencialidad de la misma; motivo por el cual Xerox está interesado en que la red inalámbrica brinde mecanismos de seguridad para la información.

También es importante mencionar que al no contar en el edificio con un cableado estructurado bien definido una red inalámbrica sería una buena opción para solucionar este problema ya que en este tipo de redes no se usa cables

Los factores expuestos anteriormente han sido determinantes y suficientes para que se ejecute el presente proyecto.

1.5 MOTIVACIÓN DEL PROYECTO

Los autores de este proyecto se motivaron a la realización del mismo, basándose en los requerimientos de movilidad de los usuarios de la red del edificio Xerox; es por eso que este proyecto a través del diseño de una red inalámbrica buscará satisfacer dichos requerimientos, tomando en cuenta también el aspecto de seguridad en plataformas Windows; por otra parte a más del diseño de la red inalámbrica se pretende controlar el acceso no autorizado al edificio a través del diseño de un sistema de control de accesos , acoplándolo a la red.

1.5.1 LOCALIZACIÓN

El presente proyecto se lo realizará en el edificio matriz de la Compañía Xerox del Ecuador, ubicado en la provincia de Pichincha, ciudad Quito Av. Amazonas N35-17 y Juan Pablo Sanz, como se observa en la figura 1.1

Figura 1.1 Edificio Matriz Xerox del Ecuador

1.5.2 ÁREA DE ESTUDIO

El área donde se realizará el presente estudio comprende el décimo piso, mezanine y planta baja del edificio Xerox. A continuación se detalla la estructura del edificio matriz de Xerox, por pisos con sus respectivos departamentos.

a) Décimo Piso

- ✓ Gerencia
- ✓ Departamento de Recursos Humanos
- ✓ Departamento de Post-Venta
- ✓ Departamento de Cobranzas

b) Mezanine

- ✓ Oficina
- ✓ PSG
- ✓ Departamento de Sistemas
- ✓ Cuarto de Comunicaciones
- ✓ Departamento de Sistema Global de Xerox (XGS)
- ✓ Departamento de Contabilidad
- ✓ Departamento de Servicio Técnico
- ✓ Departamento de Analistas
- ✓ Otros

c) Planta Baja

- ✓ Recepción
- ✓ Sala de muestras de equipos

1.6 ESTRUCTURA ACTUAL DE LA RED LAN DEL EDIFICIO MATRIZ DE XEROX DEL ECUADOR

El diseño actual de la red LAN del edificio matriz de Xerox se ilustra en la figura 1.2. A continuación se describe la red de Xerox

1.6.1 SERVIDORES DE LA RED LAN DE XEROX

En el Edificio Matriz existen seis servidores principales de datos detallados en la tabla 1.1, que se encuentran en el centro de cómputo, estos reciben consultas desde todos los departamentos del edificio matriz.

NOMBRE DEL SERVIDOR	FUNCIÓN	PROCESADOR	MODELO	RENUDAS DE EXPANSIÓN
XDORQSQL	Servidor de Base de Datos SQL primario	Pentium III	X Series 232	2(2) x PCI 64 / 66 MHz-de longitud larga. 2(2) x PCI 64 / 33 MHz-de longitud larga. 1(1) x PCI-de longitud larga.
XDORINET	Servidor de la Intranet	Pentium III	Netfinity 5000	3(3) x PCI-de longitud larga. 2(2) x PCI / ISA compartido - de media longitud.
XEROXMZ	Servidor de Base de Datos de Producción	Pentium III	X Series 232	2(2) x PCI 64 / 66 MHz-de longitud larga. 2(2) x PCI 64 / 33 MHz-de longitud larga. 1(1) x PCI-de longitud larga.
ECUQUIMDWH Data Warehouse Goldmine Docucentros	Servidor de Base de Datos Integral	Pentium III	X Series 232	2(2) x PCI 64 / 66 MHz-de longitud larga. 2(2) x PCI 64 / 33 MHz-de longitud larga. 1(1) x PCI-de longitud larga.
XEROX10 WS1-F Formas Fuentes Sistemas	Desarrollo y Pruebas	Pentium II	PC Server 330	2(2) x PCI 64 / 66 MHz-de longitud larga.
AS/400			AS/400e Series 4/8 GB SLRS QIC-4GB-DC	

Tabla 1.1 Características de los servidores del centro de cómputo del edificio Xerox

1.6.2 EQUIPOS PORTÁTILES Y DE ESCRITORIO DE LA RED LAN DE XEROX

El número de equipos portátiles y de escritorio por departamento de la compañía dentro del edificio están distribuidos tal y como se muestra en la tabla 1.2. Cabe mencionar que todos los equipos son de marca DELL y con sistema operativo Windows XP.

PISO	DEPARTAMENTOS	No. PCS	No. PORTÁTILES	SUBTOTAL
Décimo	Gerencia	1	1	2
	Gerente Técnico y Financiero	1	2	3
	Dpto. de RRHH	2	2	4
	Posventas	3	0	3
	Atención al Cliente	11	0	11
	Sala de Reuniones	4	0	4
			TOTAL X PISO	**27**
Mezanine	Marketing	1	1	2
	Sistemas	10	2	12
	Servicios Globales Xerox (XGS)	8	3	11
	PSG	4	7	11
	Contabilidad	6	0	6
	Servicio Técnico	0	4	4
	Oficinas	1	7	8
	Analistas	3	2	5
	Otros	2	1	3
			TOTAL X PISO	**62**
Planta Baja	Recepción	1	0	1
			TOTAL DE EQUIPOS	**90**

Tabla 1.2 Número de Portátiles y Pc's por departamento

1.6.3 DISPOSITIVOS ACTIVOS Y PASIVOS DE LA RED LAN DE XEROX

A continuación se describen los dispositivos pasivos y activos de la red LAN de Xerox que actualmente están en funcionamiento:

Dispositivo	N° de puertos	Cantidad existentes
Router Cisco 1700	24	1
Switch 3COM 4226T	24	7
Switch Cisco 1700	24	1
Switch D-Link DES-1024R	24	1
TOTAL DE EQUIPOS		10

Tabla 1.3 Dispositivos Activos

En cuanto a los dispositivos pasivos la red actual de Xerox cuenta con 4 patch panel, un tendido de cable UTP 5e y uno de fibra óptica para el décimo piso.

1.6.4 ESTRUCTURA FÍSICA DE LA RED LAN DE XEROX

La red LAN de Xerox está completamente interconectada por switches, hubs y routers por medio de fibra óptica (enlace mezanine – décimo piso) y cable UTP categoría 5e. Los servidores se conectan a los switches mediante interfaces 10/100 Mbps Ethernet y éstos a su vez al nivel superior a través de múltiples enlaces Ethernet excepto el décimo piso.

En el cuarto de maquinas ubicado en el mezanine existen cuatro switches y un router todos organizados en el Rack “A” y en el Rack “E” como se muestra en las figuras 1.2 y 1.3 respectivamente

Figura 1.2 Rack “A”

Figura 1.3 Rack “E”

En un extremo del ascensor en el mezanine está ubicado el rack “B” en el cual se encuentran tres switches enlazados en cascada, tal y como se muestra en la figura 1.4, los mismos que permiten la comunicación con el décimo piso y además abastecen a la mayor parte de los puntos de red que están en dicho piso

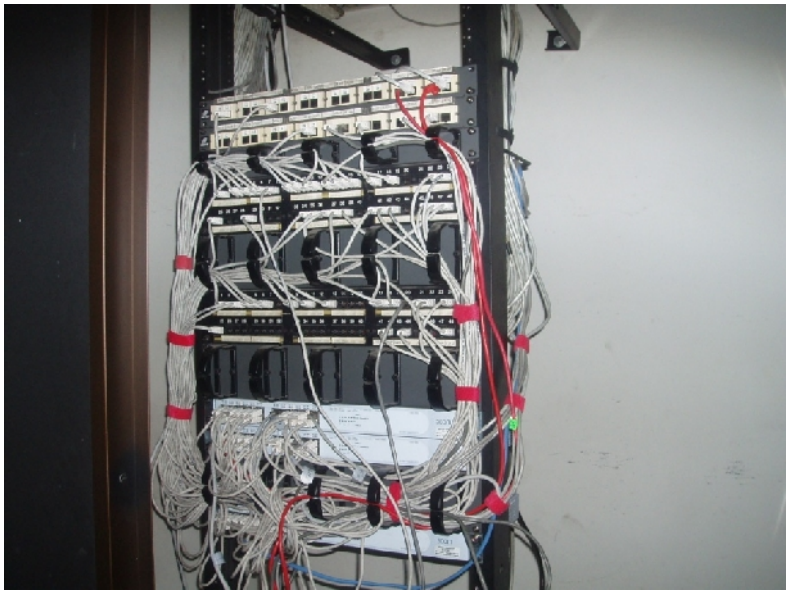


Figura 1.4 Rack “B”

A continuación se detalla de forma grafica la distribución de los elementos anteriormente mencionados dentro de la estructura física de la red LAN actual tanto en la planta baja como el mezanine del Edificio Xerox, tal como se muestra en la figura 1.5.

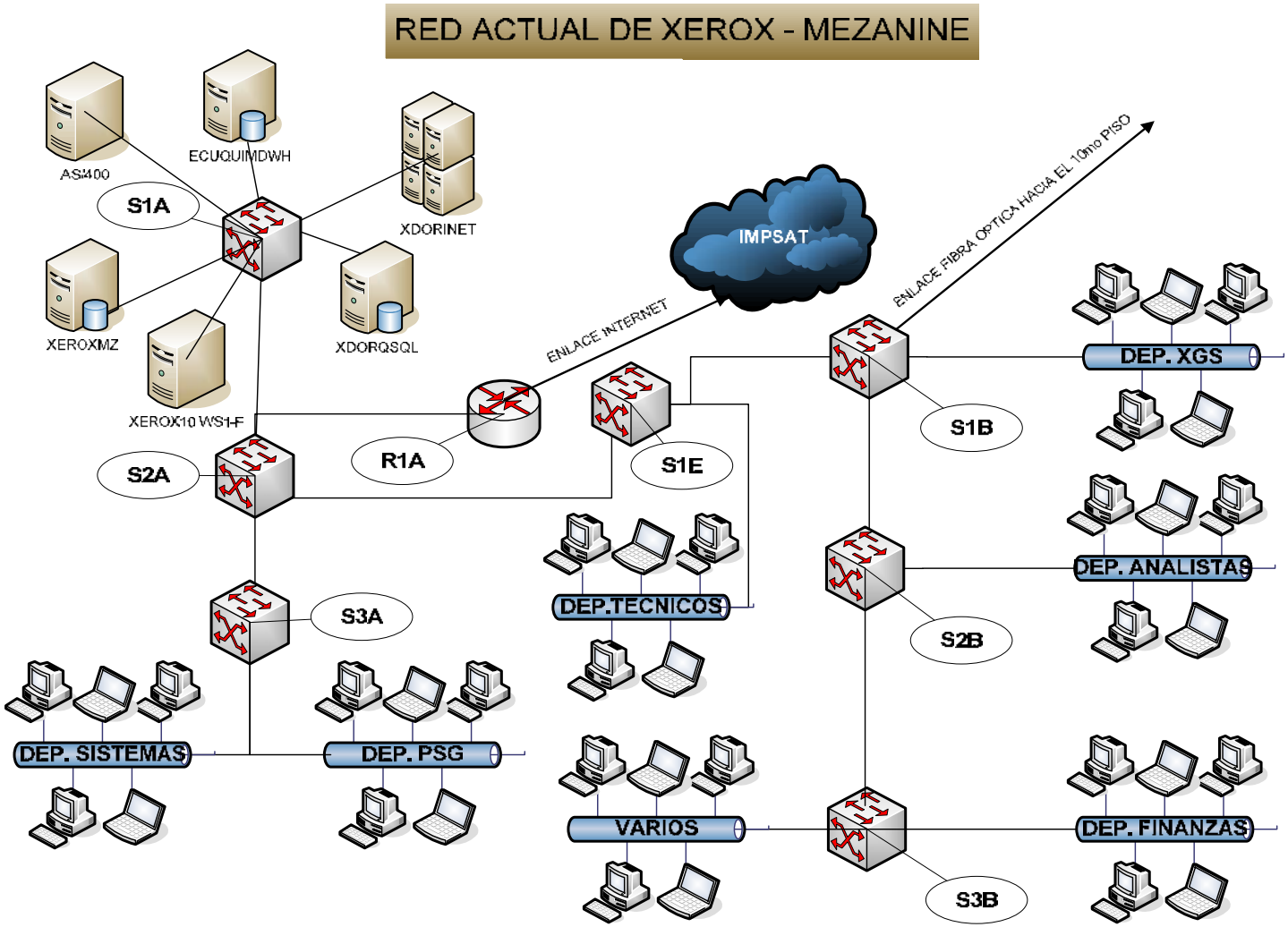


Figura 1.5 Estructura de la red LAN del piso mezanine del edificio Xerox

En el décimo piso se encuentra ubicado el Rack “C” como se muestra en la figura 1.6 en el que están dos switches enlazados en cascada los mismos que prestan servicios de red al décimo piso. En la figura 1.7 se observa un segmento de la estructura física de la red LAN actual de Xerox, correspondiente al 10mo piso.

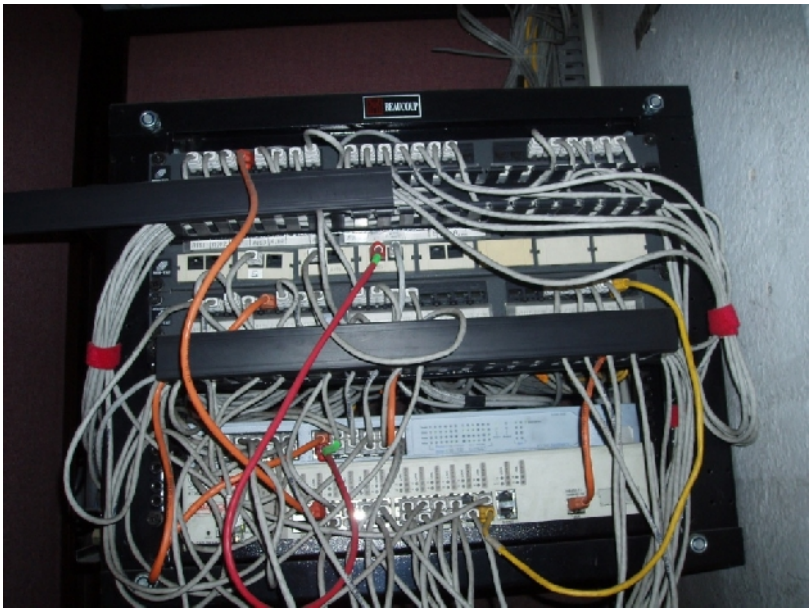


Figura 1.6 Switches Rack”C”

Por razones de seguridad el administrador de la red LAN del edificio Xerox del Ecuador se reservó el derecho de proporcionar el direccionamiento IP que esta implementado en la red LAN actual; por este motivo para el diseño de la red inalámbrica se utilizara un direccionamiento IP asignado por los autores de este proyecto a medida que se presenten necesidades en la red inalámbrica.

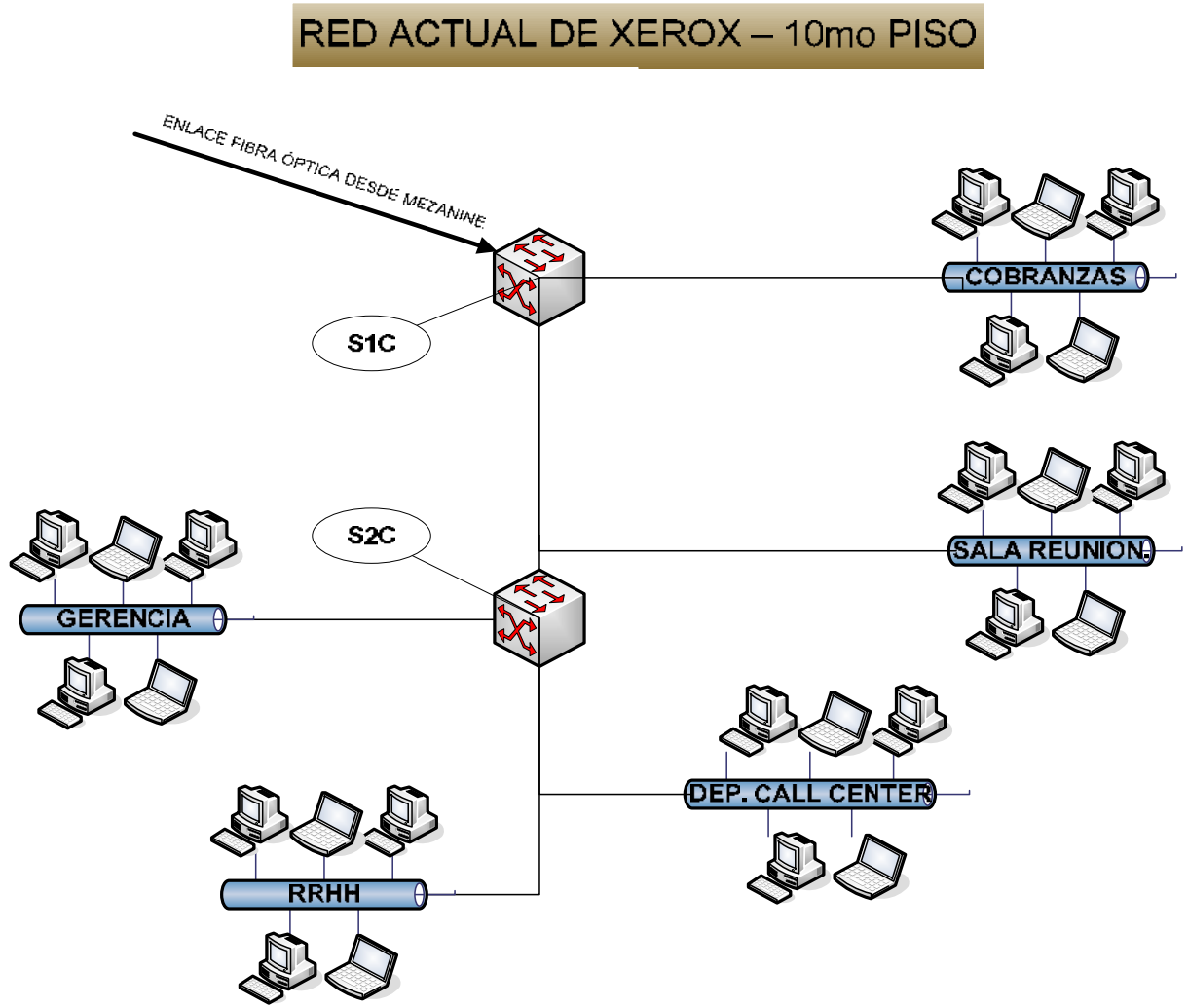


Figura 1.7 Estructura de la red LAN del décimo piso del edificio Xerox

NOMENCLATURA DE SWITCH	
ABREVIATURA	**NOMBRE**
S1A	SWITCH NUM. 1 DEL RACK “A”
S2A	SWITCH NUM. 2 DEL RACK “A”
S3A	SWITCH NUM. 3 DEL RACK “A”
S1B	SWITCH NUM. 1 DEL RACK “B”
S2B	SWITCH NUM. 2 DEL RACK “B”
S3B	SWITCH NUM. 3 DEL RACK “B”
S1E	SWITCH NUM. 1 DEL RACK “E”
R1A	ROUTER NUM. 1 DEL RACK “A”
S1C	SWITCH NUM. 1 DEL RACK “C”
S2C	SWITCH NUM. 1 DEL RACK “C”

Tabla 1.4 Nomenclatura de Switches

1.7 REQUERIMIENTOS DE LA RED INALAMBRÁMBRICA PARA EL EDIFICIO MATRIZ DE XEROX

De acuerdo a las observaciones realizadas se reconoce que las necesidades de los usuarios no son las mismas. Algunos requieren acceso de tiempo real a información de importancia crítica. Otros buscan una herramienta de productividad. Y algunos simplemente se enfrentan a un problema geográfico ya que requieren una "oficina virtual" para compensar la dispersión, es por eso que se pueden establecer los siguientes requerimientos:

- ✓ Poseer una red inalámbrica que le garantice movilidad al usuario de la red; es decir el personal se puede alejar de sus sitios de trabajo y desplazarse fácilmente por las oficinas sin perder la conexión con la red.
- ✓ Privacidad, Integridad y Disponibilidad de la información.
- ✓ Menores complicaciones en la integración de nuevos dispositivos y aplicaciones, en respuesta a los distintos niveles de demanda conforme la compañía requiera o solicite.

1.8 REQUERIMIENTOS DEL SISTEMA DE CONTROL DE ACCESO PARA EL EDIFICIO MATRIZ DE XEROX

- ✓ El ingreso debe ser restringido a las diferentes dependencias que considere Xerox de riesgo para su seguridad.
- ✓ Establecer derechos de acceso a los usuarios.
- ✓ Facilidad en la administración del sistema de control.
- ✓ Debe ser un sistema que permita su integración a la red inalámbrica a ser diseñada.
- ✓ Facilidad en la instalación y configuración.

CAPÍTULO II

REDES INALÁMBRICAS 802.11

2.1 INTRODUCCIÓN

El punto de partida de las redes inalámbricas ó WLAN (Wireless LAN) se da en 1979 en base a los experimentos realizados en Suiza por ingenieros de IBM que trabajaron con enlaces infrarrojos para formar una red local, con el tiempo se realizaron investigaciones tomando como referencia las pruebas realizados con infrarrojos aplicadas esta vez con microondas.

En mayo de 1985 la Comisión Federal de Comunicaciones de Estados Unidos FCC[2] (Federal Comunication Comission) asignó las bandas Industrial, Científica y Médica ISM[3] (Indrustrial, Scientific and Medical). En1989 se forma el comité IEEE 802.11 para normalizar las redes inalámbricas. En 1994 se resume el primer borrador y finalmente en el año 1999 se da por finalizada la norma. En esta última edición se define a la capa física (PHY-Physical Layer) y la capa de control de acceso al medio (MAC-Medium Access Control).

La tecnología inalámbrica ha tenido éxito porque permite a las personas conectarse entre sí independientemente de su ubicación. La tecnología de sistema de redes de datos inalámbricos más exitosa que en estos últimos años se ha normalizado bajo los criterios y políticas del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE[4] Institute of Electrical and Electronics Engineers) es el estándar 802.11, la misma que se le conoce por diversos nombres, algunos la denominan Ethernet inalámbrico para enfatizar su linaje compartido con la tradicional

[2] FCC: Agencia independiente del gobierno estadounidense responsable de la regulación de las comunicaciones interestatales e internacionales por radio televisión y cable
[3] ISM: Son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética.
[4] IEEE: Asociación estadounidense dedicada a la estandarización.

Ethernet. Un segundo nombre que ha crecido en popularidad, es Wi-Fi [5](Wireless Fidelity), gracias al programa de certificación de interoperatividad de Wi-Fi Alliance[6] que anteriormente se la conocía como WECA (Wireless Ethernet Compatibility Alliance).

Las WLAN son sistemas de comunicaciones que utilizan ondas electromagnéticas (radio e infrarrojo) para transmitir y recibir información entre los equipos que forman parte de la red. La comunicación en estas redes se basa generalmente en la propagación de ondas de radio emitidas por una antena omnidireccional (Equipo radio base o punto de acceso) en un área determinada dentro de las cuales se encuentran las estaciones de trabajo.

Las redes inalámbricas ó WLAN (Wireless LAN) comparten diversas ventajas importantes, independientemente de cómo se diseñen los protocolos o el tipo de datos que transporten.

La principal ventaja de un sistema WLAN es su movilidad. Los usuarios pueden conectarse a redes existentes y posteriormente pueden transitar libremente, siempre que sigan estando dentro del rango de la estación base.

La flexibilidad es otra gran ventaja de los sistemas inalámbricos que se traduce en una implantación rápida. Añadir un usuario a una red inalámbrica normalmente puede reducirse a una materia de configuración para que reconozca y ofrezca servicios a los nuevos usuarios. La flexibilidad puede ser particularmente importante en edificios más antiguos porque reduce la necesidad de construcción.

Las redes locales inalámbricas más que una sustitución de las Lan convencionales es una extensión de las mismas, siendo imperceptible al usuario al momento de

[5] Wi-Fi: (Wireless Fidelity) Conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11

[6] Wi-Fi Alliance: Organización creada por líderes proveedores de software y equipos inalámbricos con la misión de certificar los productos basados en el 802.11 para lograr interoperabilidad y promover el término Wi-Fi como una marca global para cualquier producto basado en el 802.11.

intercambiar la información. Al considerar que las redes inalámbricas son un complemento se pueden mezclar las redes cableadas y las inalámbricas generando una “Red Híbrida”; en este sentido el objetivo fundamental de las redes WLAN es el de proporcionar ventajas no disponibles en los sistemas cableados y formar una red en donde estos dos tipos de sistemas se asocien y trabajen conjuntamente en armonía.

Las redes inalámbricas ó WLAN (Wireless LAN) al igual que todas las redes utilizan un medio para transmitir datos, en este caso este medio debe cubrir una amplia área para que los usuarios puedan moverse a través de un área de cobertura. Las primeras redes inalámbricas utilizaban la luz e infrarrojos pero estas tenían sus limitaciones ya que se bloqueaban debido a obstáculos físicos como paredes, divisiones y otros elementos constructivos de una oficina, es por eso que actualmente son usadas las ondas de radio.

2.2 ESTÁNDAR 802.11

802.11 es una serie de especificaciones para tecnologías de red de área local inalámbricas que forma parte de la familia IEEE 802.

A continuación se puede visualizar en la figura 2.1 las relaciones de la familia 802.11 y su correspondiente lugar en el modelo OSI.

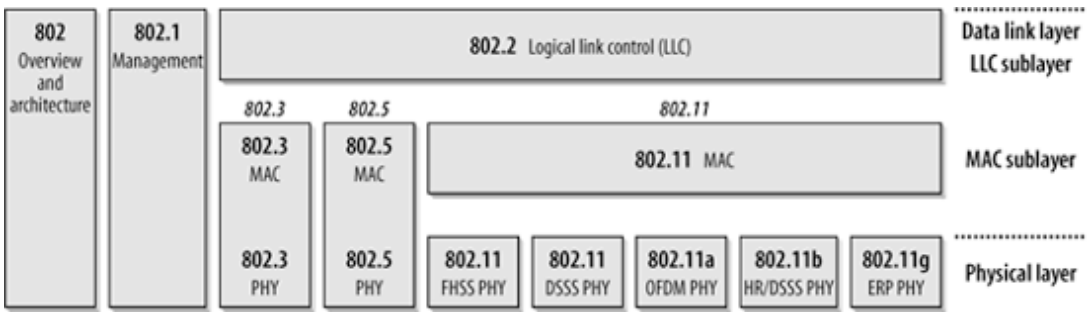


Figura 2.1. Familia IEEE 802 y su relación con el modelo OSI

Las especificaciones IEEE802.11 se enfocan en las dos últimas capas inferiores del modelo OSI, las redes 802.11 están conformadas por un componente MAC y un componente físico (PHY).

2.3 COMPONENTES FÍSICOS DE UNA RED INALÁMBRICA

En la figura 2.2 se puede observar los componentes físicos más importantes en una red inalámbrica.

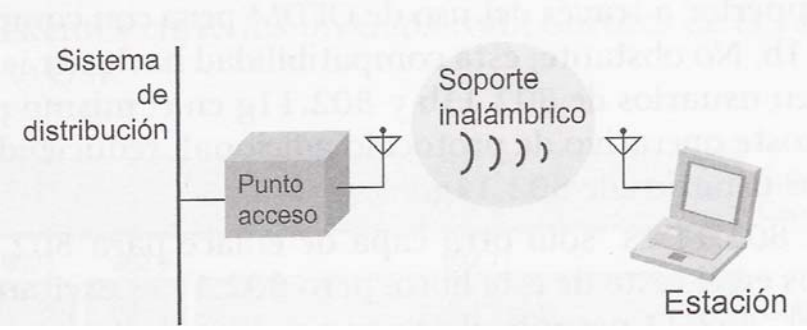


Figura 2.2. Componentes de las LAN 802.11

a) **Las estaciones o terminales** son dispositivos informáticos con interfaces de red inalámbricas que no necesariamente deben ser portables, el sistema de red inalámbrico puede evitar incluir un nuevo cable permitiendo que los computadores personales se conecten a través de la LAN inalámbrica.

b) **Los Puntos de acceso** (AP[7], Access Point) realizan la función de puente inalámbrico a cable.

c) **Medio inalámbrico** para mover las tramas de una estación a otra, el estándar utiliza un medio inalámbrico. En un principio se estandarizaron dos capas físicas una de radio frecuencia (RF, Radio Frequency) y otra de infrarrojo.

[7] AP Dispositivo parecido a un puente que une estaciones 802.11

d) **Sistemas de distribución** se constituyen cuando se conectan diversos puntos de acceso para formar una gran área de cobertura, el sistema de distribución es el componente lógico de 802.11 el cual es utilizado para reenviar las tramas a su destino.

2.4 TOPOLOGÍAS DE RED INALÁMBRICA

Las necesidades de una organización y el nivel de inversión, determinan la topología de una red inalámbrica; es así que estas redes se construyen utilizando dos topologías básicas. Para estas topologías se utilizan distintos términos, como administradas y no administradas, alojadas y par a par, e infraestructura (Wired) e independientes o ad hoc (Stand Alone)". En esta tesis se utilizarán los términos "infraestructura" e "independientes".

La red 802.11 se basa en BSS (Basic Service Set - conjunto de servicios básicos), siendo este un grupo de estaciones que se comunican entre sí.

Las estaciones inalámbricas o BSS se comunican utilizando ondas electromagnéticas (de radio o infrarrojas) para transmitir información de un punto a otro. Las BSS son conectadas a una capa de distribución de red o DS. Cada BSS está conformado por nodos móviles que se encuentran controlados por una función de coordinación distribuida DCF(Distribuited Coordination Funtion) la que designa que nodo tiene derecho a transmitir o recibir información en el medio inalámbrico. Las estaciones móviles de un BSS acceden a la capa de distribución y por consiguiente a otros nodos inalámbricos fuera de la cobertura inalámbrica a través del AP. La DS soporta la movilidad de los nodos mediante direccionamiento e integración de forma transparente al usuario.

Los BSS se los define de dos tipos: Independientes y de infraestructura como se muestra en la figura 2.3

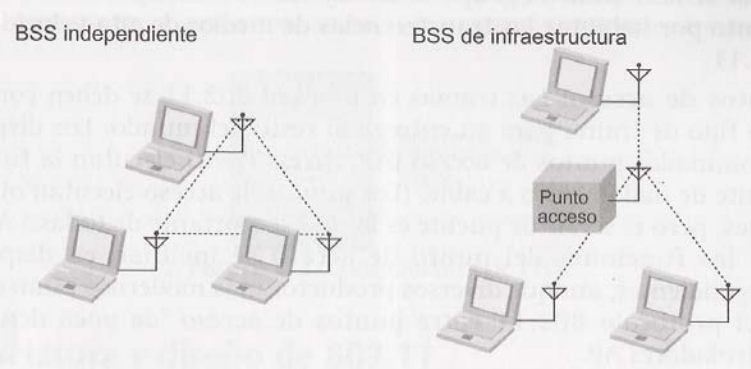


Figura 2.3. BSS independiente y de infraestructura

2.4.1 REDES INDEPENDIENTES O AD-HOC

Las estaciones en un IBSS (Independent Basic Service Set - Conjunto de Servicios Básicos Independientes) se comunican directamente entre si razón por la cual deben estar dentro del alcance directo de la comunicación. Las IBSS son creadas específicamente para eventos de periodo corto, también son conocidas como redes provisionales.

En una red inalámbrica independiente como se visualiza en la figura 2.4 no existe ningún punto de acceso ni controlador central ya que cada dispositivo se puede comunicar con todos los demás; esto es que los propios equipos inalámbricos crean la red LAN, los cuales se comunican directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. En una red inalámbrica independiente, cada nodo forma parte de una red punto a punto, para lo cual se debe disponer de una identidad del conjunto de servicios SSID (Service Set Identity**)** igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento. A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre si

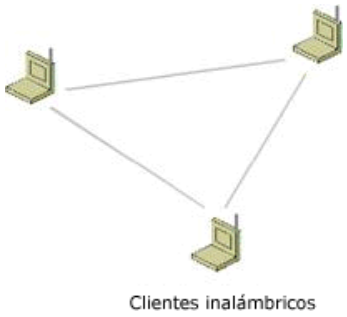


Figura 2.4. Red Independiente

2.4.2 REDES DE INFRAESTRUCTURA

Este tipo de topología es muy usada en casos donde se necesita extender una red LAN con cable existente incorporando dispositivos inalámbricos mediante una estación base, denominada punto de acceso Wi-Fi o nodo central. Las redes de infraestructura se distinguen por un particular y es que emplean puntos de acceso sean estos uno o varios como se muestra en la figura 2.5. El punto de acceso sirve de enlace para la red LAN inalámbrica y la red LAN con cable y además se encarga de controlar y coordinar la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; esto quiere decir que para poder establecer la comunicación, todos los dispositivos inalámbricos deben estar dentro de la zona de cobertura del punto de acceso. En la modalidad de infraestructura, pueden existir varios puntos de acceso para dar cobertura a una zona grande o a un único punto de acceso para una zona pequeña.

Para que una estación móvil pueda comunicarse con una segunda estación móvil dentro de una red BSS de infraestructura debe primero transferir la trama desde la estación origen al punto de acceso para que luego este sea enviado a la estación destino con lo que se puede apreciar que existen dos saltos para que se realice la comunicación.

Un conjunto de servicio básico (BSS) de infraestructura está definido por la distancia a la que se encuentra desde el punto de acceso.

Los puntos de acceso (AP) tienen la capacidad de advertir cuando entra una estación en un modo de ahorro de potencia y copiar en el búfer las tramas.

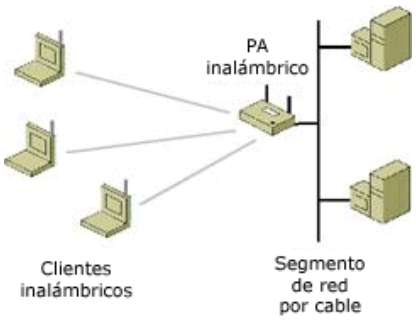


Figura 2.5. BSS de infraestructura

La estación en el ámbito de las redes LAN inalámbricas de infraestructura, primero identifica los puntos de acceso y las redes disponibles, luego la estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación que es el intercambio de información y datos de capacidad. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

El tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino ya sea a la red LAN con cable o a la red inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones. En las redes de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso.

2.4.3 ÁREAS DE SERVICIO EXTENDIDAS.

Un ESS (Conjunto de servicios extendidos, Extended Service Set) se crea encadenando los BSS entre sí con una red troncal, en un ESS todos los puntos de acceso tienen el mismo identificador del conjunto de servicios (SSID, Service Set Identifer), que es utilizado como nombre de red para los usuarios.

En la Figura 2.6 se puede apreciar la unión de cuatro BSS con lo que se forma una ESS, siempre y cuando todos los puntos de acceso estén configurados como parte del mismo ESS

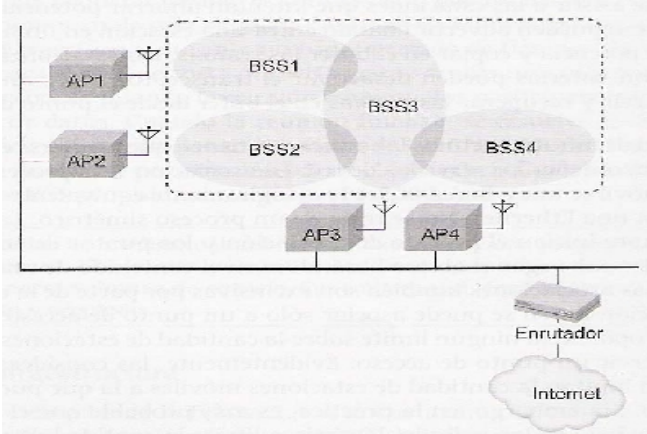


Figura 2.6. Conjunto de servicio extendido

Para que las estaciones en un conjunto de servicios extendidos (ESS) se puedan comunicar entre sí, el medio inalámbrico debe actuar como una sola conexión de capa 2, la comunicación directa entre las estaciones que se encuentran en un ESS requiere que la red troncal también parezca una conexión de capa 2, para eso los productos actuales utilizan una variedad de tecnologías de túnel para emular el entorno de la capa 2.

El enrutador que se observa en la Figura 2.6., toma la dirección MAC de la estación como destino para entregar las tramas a una estación móvil, solo al punto de acceso (AP) al que está asociada esa estación móvil entrega la trama.

2.4.4 ENTORNOS DE MÚLTIPLES BSS: "AP VIRTUALES" Y REDES DE SEGURIDAD ROBUSTAS (RSN)

En una red inalámbrica pueden existir varias redes lógicas con el fin de dividir a nuestros usuarios (internos e invitados) esto se lo puede realizar creando dos conjuntos de ESS en la misma infraestructura física, esto ayuda a dar privilegios a las estaciones para asociarse a la red a esto también se lo denomina puntos de acceso virtuales. Cada BSS actúa como su propio punto de acceso (AP), con su propio **i**dentificador de conjunto de servicios extendidos (ESSID), dirección MAC, configuración de autenticación y configuración de cifrado.

Los puntos de acceso (AP) virtuales se los puede crear gracias a los chips de radio 802.11 actuales que permiten definir 32 o incluso 64 BSS.

802.11i confirmada en junio de 2004, especifica un conjunto de mecanismos de seguridad mejorados que proporcionan Asociaciones de red de seguridad robusta (RSNA, Robust Security Network Asociación). La compatibilidad con 802.11i puede estar compuesta de hardware, software o ambos dependiendo de la arquitectura exacta de un dispositivo en particular.

2.5 CAPA FÍSICA

2.5.1 PROPAGACIÓN DE RADIO FRECUENCIA

La propagación de RF (Radio Frecuencia) es más complicada en comparación con las redes cableadas ya que se limitan al cálculo de la longitud del cable para que no haya algún tipo de interferencia.

Para que exista una comunicación de radio depende de que la señal sea legible sobre el ruido de fondo, su rendimiento se lo expresa principalmente por la tasa de señal a ruido (SNR, Signal-To-Noise Ratio) que se la puede visualizar en la figura 2.7

Una señal fuerte es el primer paso ya que otro factor es el de elevar la potencia para compensar el fondo de ruido alto pero esto tiene un limitante por ser redes sin licencia la potencia no puede sobrepasar las estrictas restricciones normativas por consiguiente se pone énfasis en introducir el menor ruido adicional posible antes de descodificar la señal de radio.

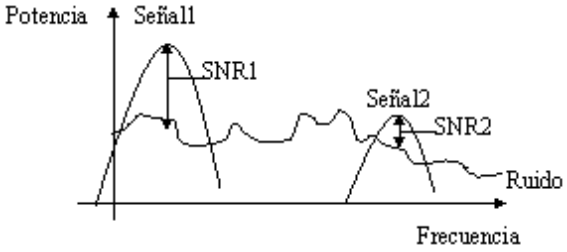


Figura 2.7 Tasa de señal a ruido y el fondo del ruido.

2.5.1.1 EL LÍMITE DE SHANNON

El teorema de Shannon refleja una realidad teórica de una velocidad de bits ilimitada. La capacidad del canal de comunicaciones la proporciona el teorema de Shannon – Hartley el cual expresa los bits de capacidad C por segundo como una función de ancho de banda W en Hertzios y la tasa absoluta de la potencia de la señal al ruido.

$$C <= W \log2 (1 + S / R) \quad (S / N \text{ como tasa de potencia})$$

$$C <= W \log2 (1 + 10 \wedge (0.1 * SNR) \quad (SNR \text{ en decibelios})$$

Realizando los cambios pertinentes se puede utilizar el teorema de Shannon para el cálculo de la tasa señal a ruido teóricamente mínima para conseguir una velocidad de datos determinada.

$$S / N = 2 \wedge (C/W) – 1 \qquad (S / N \text{ como tasa de potencia})$$

$$SNR = 10 * \log 10 (2 \wedge (C/W) – 1) \qquad (SNR \text{ como dB})$$

2.5.1.2 PERDIDA DE RUTA, RANGO Y RENDIMIENTO

En la tecnología 802.11, la velocidad de la red depende del rango. Las modulaciones de velocidad superior empaquetan más bits en un determinado

periodo de tiempo y requiere de una señal más clara para que se pueda decodificar con éxito.

La degradación de la señal con la distancia limitara la tasa de señal a ruido en el receptor, a medida que la estación se desvía de un punto de acceso, el nivel de la señal desciende como se lo puede apreciar en la Fig. 2.8

Para el cálculo de la degradación de la señal cuando no existe obstáculos que obstruyan la onda de radio se utilizara la siguiente ecuación

La perdida de ruta (perdida de espacio libre) depende de la distancia y la frecuencia de onda de radio por lo tanto distancias superiores y frecuencias superiores conducen a una pérdida de ruta superior.

Perdida de ruta (dB) = 32.5 + 20 log F + log d

F: Frecuencia (GHz)
d: Distancia (m)

Para el cálculo de rangos normalmente se incluyen un factor de fallo denominado margen de enlace para tener en cuenta las perdidas imprevistas:

Pérdida total = Potencia TW + ganancia de antena TX – perdida de ruta – perdida de obstáculo – margen de enlace + ganancia de antena RX

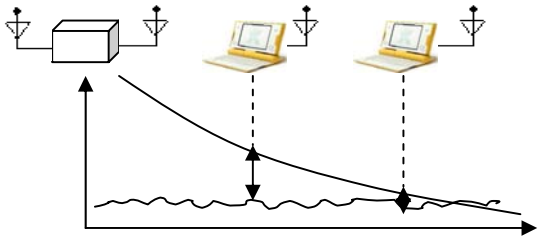


Figura 2.8 Nivel de la señal desciende

Existen varios fenómenos que pueden inhibir la recepción de la señal con 802.11 pero uno de los principales es el desvanecimiento de múltiples rutas. Las ondas se superponen como se muestra en la figura 2.9

Cuando convergen en un punto múltiples ondas, la onda total es simplemente la suma de las ondas. Un resultado muy común de ondas en redes inalámbricas es que dos ondas son casi exactamente opuestas entre si y su resultado neto es casi nulo, en cuyo caso el receptor no entenderá la transmisión ya que no habrá recibido ninguna.

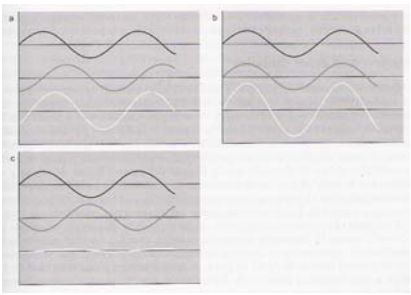


Figura 2.9 Combinación de ondas por superposición.

Este desvanecimiento de múltiples rutas es un caso especial de Interferencia entre símbolos (ISI, Inter-Symbol Interference).

Otro aspecto relevante es la dispersión retardada que no es más que al añadir frentes de onda de múltiples rutas, el resultado del tiempo de llegada del primer frente de onda y el último eco de múltiples ondas es lo que se denomina dispersión retardada.

2.5.1.3 CÁLCULOS DE POTENCIA

En la radiofrecuencia la salida de potencia de transmisión se mide en dos puntos distintos de un sistema inalámbrico, siendo estos en el emisor intencional (IR, intencional radiator) y en la potencia radiada isotrópica equivalente (EIRP, equivalent isotropically radiated power).

El IR incluye al transmisor de radio y todos los cables y conectores, pero sin incluir la antena que se emplee. El EIRP es la potencia realmente radiada desde la antena; tanto las potencias IR como EIRP se encuentran reguladas por la FCC (Federal Communications Commission) en EEUU (en la Parte 47 CFR, Capítulo 1, Sección 15.247) o la ETSI (el Instituto Europeo de Normas de Telecomunicaciones) en la Unión Europea.

Para el cálculo tanto de la potencia de la energía emitida como la sensibilidad de recepción de un dispositivo inalámbrico se utilizan vatios (comúnmente milivatios, mW) o decibelios. Tanto la ganancia de potencia debida a las antenas y amplificadores como las pérdidas debido a las distancias, los obstáculos y la resistencia eléctrica de los cables, conectores, protectores frente a descargas, divisores y atenuaciones se mide en decibelios o, de un modo más preciso, en dBm. La “m” de “dBm” significa que se toma como referencia 1 mW. Esto quiere decir a que 1 mW equivale a 0 dBm.

En cuanto a la ganancia de potencia de las antenas se expresa en dBi (“i” procede de “isotrópica”), siendo utilizado del mismo modo que los dBm en los cálculos de potencia de radiofrecuencia. Por lo que podemos afirmar que, P dBm equivale a 10 log P mW. Lo que queremos decir es que, cada cambio de 3 dB duplica o reduce a la mitad la potencia, y cada diferencia de 10 dB incrementa o reduce la potencia en un orden de magnitud.

Para el cálculo del valor EIRP de un sistema inalámbrico hay que realizar la suma de todos los valores dBm de los dispositivos y conectores involucrados. Para mayor comprensión se va a realizar el cálculo de la potencia de un conjunto de partes (hardware) de un sistema estándar que comprende de lo siguiente: tarjeta PCMCIA cliente de 20 dBm (100 mW), un conector pigtail largo con una pérdida de 2 dBm yb una antena omnidireccional de montaje magnético con una ganancia de 5 dBi. Realizando los cálculos nos quedaría:

$$20 – 2 + 5 = 23 \text{ dBm}$$

Lo que sería una potencia de salida de 200 mW. Claro teniendo en cuenta que cada aumento de 6 dBi en el valor de la EIRP duplica el alcance de transmisión o recepción (regla de los 6 dB).

2.5.2 ESTÁNDARES DE LA CAPA FÍSICA

En principio se estandarizaron tres capas físicas:

- ✓ Capa física de radio de espectro disperso de Salto de frecuencia (FH, Frequency-Hopping).
- ✓ Capa física de radio de espectro disperso de Secuencia directa (DS, Direct-Sequence).
- ✓ Capa física de Luz infrarroja (IR, Infrared Light).
- ✓ Luego se desarrollaron capas físicas basadas en la tecnología de radio:
- ✓ 802.11a: Capa física de Multiplexado de división de frecuencia ortogonal (OFDM, Orthogonal Frequency Division Multiplexing).
- ✓ 802.11b: Capa física de secuencia directa de alto porcentaje (HR/DS o HR/DSSS, High-Rate Direct Sequence).
- ✓ 802.11g: Capa física de Velocidad extendida (ERP, Extended Rate PHY).

El futuro 802.11n: denominada MIMO[8] PHY o PHY de alto rendimiento.

802.11 divide la PHY[9] en dos componentes de medio físico genéricos: PLCP[10] (Physical Layer Convergente Procedure - Procedimiento de Convergencia de. la Capa Física) para asignar las tramas MAC en el medio y un PMD[11] (Physical

[8] MIMO:Multiple-input/Multiple-output.- Múltiples entradas/Múltiples salidas
[9] PHY Abreviatura común de IEEE para la capa física
[10] PLCP Procedimiento de convergencia de capa física
[11] PMD Sistema dependiente del medio físico

Médium Dependent - Física dependiente del medio) para transmitir dichas tramas como se indica en la figura 2.10

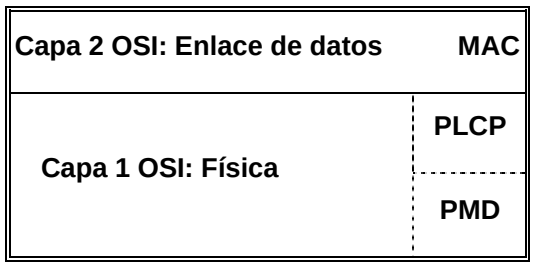


Figura 2.10 Subcapas de la capa física

2.5.3 TECNOLOGÍA DEL ESPECTRO DISPERSO CON SALTO DE FRECUENCIA (FREQUENCY-HOPPING, FH O FHSS)

La tecnología del espectro disperso con salto de frecuencia utiliza diferentes frecuencias para transmitir cada segmento de información en un intervalo de tiempo llamado dwell time el cual no debe ser mayor a 400 ms, pasado este tiempo cambia la frecuencia siguiendo un patrón conocido solamente por el emisor y el receptor. Si el receptor desconoce el patrón la interpretara como ruido. Si los saltos de frecuencia se mantienen sincronizados se conseguirá que la comunicación se mantenga en un solo canal a nivel lógico aunque el tiempo se cambie de canal físico.

La banda de los 2.4 GHz es utilizada por la tecnología FHSS la cual se organiza en 79 canales, cada canal con un ancho de banda de 1 MHz esto dependiendo del área geográfica. La modulación aplicable en este caso es la FSK[12] (Frecuncy Shift Keying – Desplazamiento de Frecuencia) con velocidades de 1 Mbps, 2 Mbps aplicables a 11 Mbps. En la tabla 2.1 se observa las diferentes frecuencias utilizadas en la técnica FHSS:

[12] FSK: Modulación que relacionada dos diferentes frecuencias.

Canal	Valor	Canal	Valor	Canal	Valor
2	2.402	28	2.428	54	2.454
3	2.403	29	2.429	55	2.455
4	2.404	30	2.430	56	2.456
5	2.405	31	2.431	57	2.457
6	2.406	32	2.432	58	2.458
7	2.407	33	2.433	59	2.459
8	2.408	34	2.434	60	2.460
9	2.409	35	2.435	61	2.461
10	2.410	36	2.436	62	2.462
11	2.411	37	2.437	63	2.463
12	2.412	38	2.438	64	2.464
13	2.413	39	2.439	65	2.465
14	2.414	40	2.440	66	2.466
15	2.415	41	2.441	67	2.467
16	2.416	42	2.442	68	2.468
17	2.417	43	2.443	69	2.469
18	2.418	44	2.444	70	2.470
19	2.419	45	2.445	71	2.471
20	2.420	46	2.446	72	2.472
21	2.421	47	2.447	73	2.473
22	2.422	48	2.448	74	2.474
23	2.423	49	2.449	75	2.475
24	2.424	50	2.450	76	2.476
25	2.425	51	2.451	77	2.477
26	2.426	52	2.452	78	2.478
27	2.427	53	2.453	79	2.479
				80	2.480

Tabla2.1. Valores de frecuencias usadas en Norteamérica y Europa.

2.5.4 TECNOLOGÍAS DEL ESPECTRO DISPERSO DE SECUENCIA DIRECTA (DIRECT-SEQUENCE, DS O DSSS) Y DE ALTO PORCENTAJE (HR/DS O HR/DSSS, 802.11B)

La transmisión de secuencia directa es una técnica de espectro disperso, alternativa que se puede utilizar para transmitir una señal sobre una banda de frecuencia mucho más ancha. La función básica de las técnicas de secuencia directa es propagar la energía de radio frecuencia (RF)[13] sobre una banda ancha para que los receptores puedan ejecutar procesos correlativos buscando cambios.

En este tipo de tecnología se utiliza un patrón redundante, para cada bit que se transmita. Mientras más extenso sea el patrón existen más posibilidades que los bits transmitidos sean recuperados en el receptor mediante técnicas estadísticas; aunque esto implique un mayor ancho de banda. En el DSSS existe una relación directa entre la señal que se transmite y las interferencias, es decir a mayor señal mayor resistencia a las interferencias.

En la figura 2.11 se muestra el proceso de propagación de una señal tradicional de banda estrecha , la cual en principio se procesa a través de un “propagador” que aplica una transformación matemática para recoger una entrada de banda estrecha y nivelar la amplitud a través de una banda de frecuencia relativamente ancha. Para un receptor de banda estrecha, la señal transmitida parece un ruido de bajo nivel ya que su energía de radio frecuencia (RF) se propaga a través de una banda muy ancha. La clave de la transmisión de secuencia directa es que cualquier modulación de la portadora de RF también se propaga a través de la banda de frecuencia. Los receptores pueden supervisar una banda de frecuencia ancha y buscar cambios que se producen a lo largo de toda la banda. La señal original se recupera con una función de correlación que invierte el proceso de propagación. La correlación proporciona a las transmisiones de secuencia directa una gran protección frente a las interferencias.

[13] RF: Radio Frecuencia (Radio Frecuency) Utilizado como siglas para señalar que algo pertenece a la interfaz de radio.

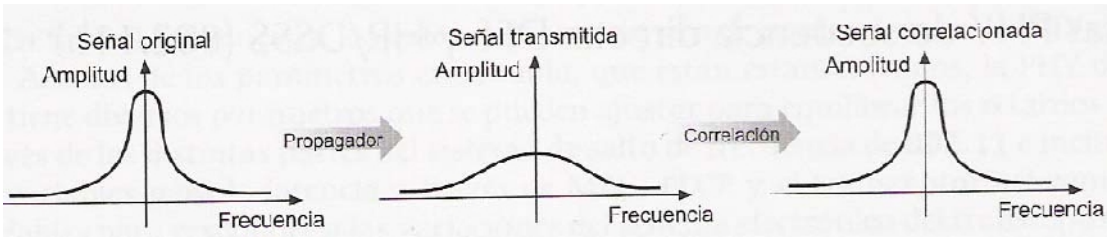


Figura 2.11 Técnica básica de propagación

La modulación de secuencia directa funciona aplicando una secuencia de chips o bits (Patrón de bits redundantes) para el flujo de datos. El estándar IEEE 802.11 recomienda un tamaño de 11 bits para la secuencia de Chip; pero el óptimo es de 100 bits. Esta secuencia de bits se le conoce también como Secuencia de Barker (PseudoNoise), para cada bit del flujo de datos que se modula con un código de Barker de 11bits producen 11 chips que trasportan el único bit de datos

En la figura 2.12 se puede apreciar cómo se utiliza la secuencia de Barker para codificar la señal original a transmitir:

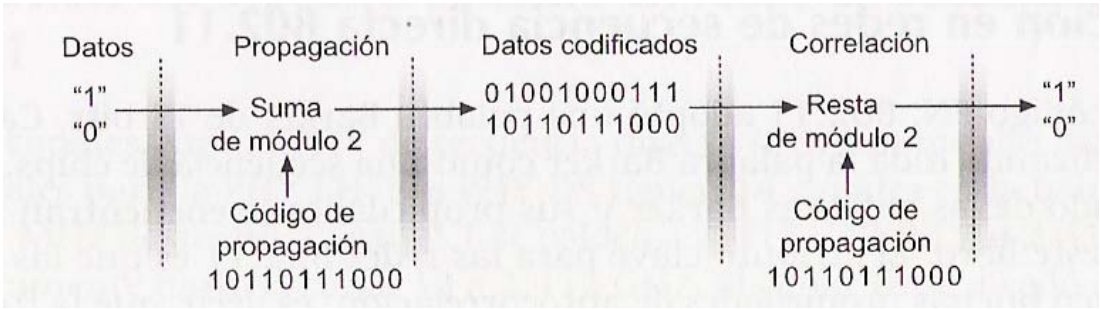


Figura 2.12 Codificación de Barker

Existen dos tipos de modulación para la técnica del espectro disperso por secuencia directa (DSSS):

- ✓ Modulación DBPSK (Differential Binary Phase Shift Keying - manipulación por desplazamiento de fase binaria diferencial) .-Velocidad de transferencia 1Mbps
- ✓ Modulación DQPSK (Differential Quadrature Phase Shift Keying **-** Modulación por desplazamiento de fase en cuadratura diferencial)**).-** Velocidad de transferencia 2Mbps.

Una de las cifras más importantes en un sistema de secuencia de radio es la velocidad de propagación, que es la cantidad de chips utilizada para transmitir un solo bit; es por eso que en un diseño de sistemas de secuencia directa para el mundo real, la velocidad de propagación debe ser lo más baja posible para satisfacer los requerimientos de diseño y evitar la pérdida de ancho de banda

La capa física de secuencia directa tiene 14 canales en la banda de los 2,4 GHz y 5 MHz de ancho. El canal 1 se coloca a 2,412 GHz, el 2 a 2,417 GHz, y así sucesivamente hasta el canal 13 a 2,472 GHz. El canal 14 se diseño exclusivamente para uso del Japón.

La capa física de secuencia directa original está compuesta por dos elementos: El procedimiento de convergencia de capa física (PLCP, Physical Layer Convergente Procedure) el cual ejecuta un entramado adicional dependiente de la capa física antes de la transmisión y la capa dependiente del medio físico (PMD, Physical Médium Dependant) que es la responsable de la transmisión real de las tramas

En 1997 se estandarizo una segunda capa física basada en la tecnología del espectro disperso de secuencia directa (DSSS) denominada HR/DS, con velocidades de datos de 1 y 2 Mbps. Luego en 1999, se mejoro las velocidades para esta capa física con velocidades de datos que van de 5,5 a 11 Mbps en 802.11b

La capa física de secuencia directa de alta velocidad a diferencia de la capa física de secuencia directa original se distingue porque se ejecuta a una velocidad de 11 Mbps y se abrevia como HR/DSSS. Al igual que su predecesora, se divide a través de un procedimiento de convergencia que prepara las tramas para su transmisión por radio y una capa dependiente del medio los bits en ondas de radio en el aire.

2.5.5 TECNOLOGÍA INFRARROJA

Las redes inalámbricas por infrarrojos son aquellas que usan el rango infrarrojo del espectro electromagnético para transmitir información mediante ondas por el espacio libre

La utilidad de esta tecnología es muy limitada ya que generalmente las estaciones deben estar ubicadas en espacios reducidos como por ejemplo en un piso dentro del edificio.

Este sistema de transmisión por infrarrojos utiliza frecuencias altas para transportar los datos.

El inconveniente que presenta esta tecnología es que al igual que la luz, los rayos infrarrojos no traspasan cuerpos opacos ya que el emisor y el receptor deben estar en el mismo ángulo de vista.

El principio en el que se basa esta tecnología es el mismo que utilizan los controles remotos de los aparatos domésticos es decir que un transmisor envía un haz de luz infrarroja hacia un receptor el cual se encarga de codificar y decodificar la señal

Para las redes infrarrojas tenemos las siguientes velocidades de información:

- ✓ 1 y 2 Mbps infrarrojos de modulación directa

- ✓ 4 Mbps infrarrojos portadora modulada
- ✓ 10 Mbps infrarrojos con modulación de múltiples portadoras

2.5.6 MULTIPLEXADO DE DIVISIÓN DE FRECUENCIA ORTOGONAL (OFDM; 802.11A)

En un principio 802.11a se diseño para las bandas de infraestructura de información nacional sin autorización (U – NII, Unlicensed Nacional Information Infraestructure) en los Estados Unidos. OFDM es un método de recortar un canal de frecuencia largo en diversos subcanales. OFDM no es una técnica nueva. Sin embargo, OFDM difiere de las técnicas de codificación emergentes, como el Acceso múltiple de división de código (CDMA, Code Division Multiple Access) en su solución. CDMA utiliza transformaciones matemáticas complejas en una sola portadora; OFDM codifica una sola transmisión en múltiples subportadoras.

OFDM adopta una solución de múltiples enlaces: cuando un enlace no es suficiente, se utilizan varios enlaces en paralelo.

La Multiplexado de división de frecuencia (FDM, Frequency Division Multiplexing) al igual que OFDM divide el ancho de banda disponible en sectores denominados portadoras o subportadoras y hacen que dichas portadoras estén disponibles como canales distintos para la transmisión de datos.

El problema del FDM tradicional es que las bandas de protección desperdician ancho de banda reduciendo la capacidad para evitar este desperdicio OFDM selecciona canales superpuestos pero que no interfieran entre sí. La figura 2.13 ilustra el contraste entre el FDM tradicional y OFDM

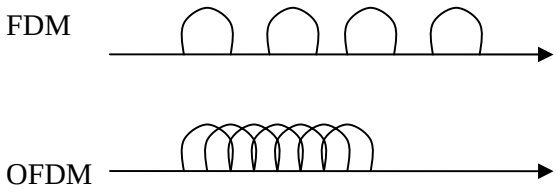


Figura 2.13 FDM frente a OFDM

Se permiten las portadoras superpuestas ya que las subportadoras se definen de forma que se pueden distinguir fácilmente. La capacidad para separa las subportadoras crea una relación matemática compleja denominada ortogonal.

Los sistemas OFDM utilizan múltiples subportadoras de distintas frecuencia. Las subportadoras se empaquetan en un canal operativo y los pequeños desfases en las frecuencias de las portadoras pueden producir interferencias entre portadoras, fenómeno denominado Interferencias entre portadoras (ICI, Inter-Carrier Interference).

2.5.7 VELOCIDAD EXTENDIDA (ERP; 802.11G)

Este estándar utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbps, o cerca de 24.7 Mbps de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias.

802.11g está compuesto por diversas especificaciones de capa física en una sola. Añade una cláusula que comprende la capa física de velocidad extendida (ERP Extended Rate PHY).Sin embargo existen diversos tipos de ERP:

- ✓ ERP-DSSS y ERP-CCK[14]: Estos modos son compatibles con la especificación de secuencia directa original (1Mbps y 2 Mbps) así como con las mejoras de 802,11b (5,5 Mbps y 11 Mbps)
- ✓ ERP-OFDM: Esté es el modo principal de 802.11g. Básicamente ejecuta 802.11a en la banda de frecuencia ISM (Indrustrial, Scientific and Medical - Industrial, Científica y Médica) (2,5 Ghz) con algunos cambios menores para proporcionar compatibilidad hacia atrás. Admite las mismas velocidades que 802.11a: 6, 9, 12,18, 24, 36,48 y 54Mbps.
- ✓ ERP-PBCC: Ésta es una extensión opcional para el estándar PBCC [15] establecido en 802.11b y proporciona velocidades de datos de 22 y 33 Mbps; pero no es muy utilizado.
- ✓ DSSS-OFDM: Éste es un esquema híbrido, que codifica los paquetes utilizando encabezados DSSS y la codificación OFDM de la carga útil.

802.11g adopta la secuencia directa DSSS de 802.11a y la capa física de cifrado de código complementario CCK de alta velocidad de 802.11b salvo que efectúa algunos cambios que ayuda a la coexistencia con implantaciones más antiguas.

2.6 CAPA ENLACE (MAC) 802.11

La clave para la especificación de 802.11 es la MAC que recorre todas las capas físicas y controla la transmisión de datos de usuario en su medio que es el aire. Además proporciona las operaciones principales de las tramas y la interacción con una red troncal con cables.

802.11 utiliza el esquema de Acceso múltiple con escucha de portadora y evitación de la colisión (CSMA/CA, Carrier Sense Multiple Access / Collision

[14] CCK: Cifrado de código complementario (Complementary Code Keying). Un esquema de modulación que transforma los bloques de datos en códigos complejos y puede codificar diversos bits por bloque.
[15] PBCC: Codificación d circunvolución de paquete binario (Packet Binary Convolution Coding). Medoto alternativo para codificar datos en redes 802.11b.

Avoidance). 802.11 al igual que Ethernet utilizan un esquema de acceso distribuido sin un controlador central, las estaciones 802.11 para acceder al medio utilizan el mismo método.

La calidad del enlace de radio frecuencia la afectan varios factores, al utilizar las bandas ISM hay que tener en cuenta que van existir interferencias, ruido, desvanecimiento de la señal, perdidas de las rutas de transmisión de las tramas debido a que el nodo se mueve hacia un punto muerto.

802.11 incorpora acuses de recibo (ACK)[16] positivos, esto lo hace diferente a muchos protocolos de capa enlace, se ilustra de forma grafica en la figura 2.14

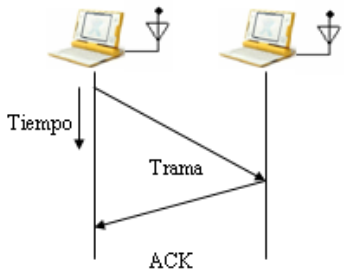


Figura 2.14 Acuse de recibo positivo de las transmisiones de datos

Para que la trama llegue con éxito a su destino se debe completar toda la secuencia caso contrario se considera fallida, por no existir un acuse de recibo, de todas formas la trama de datos tiene que volver a transmitirse.

Un aspecto importante que influye en la calidad del enlace de radio es la velocidad a la que funciona la red, la calidad de la señal se degrada con el rango, esto indica que la velocidad de transmisión de los datos de una estación 802.11 está ligada a la ubicación con relación al punto de acceso.

[16] ACK: Abreviatura de la palabra inglesa Acknowledgment, acuse de recibo

El método que aplica 802.11 para evitar colisiones es que las estaciones utilicen señales de solicitud de emisión (RTS, Request to Send) y de autorización de emisión (CTS, Clear to Send) para despejar un área como se muestra en la siguiente figura 2.15

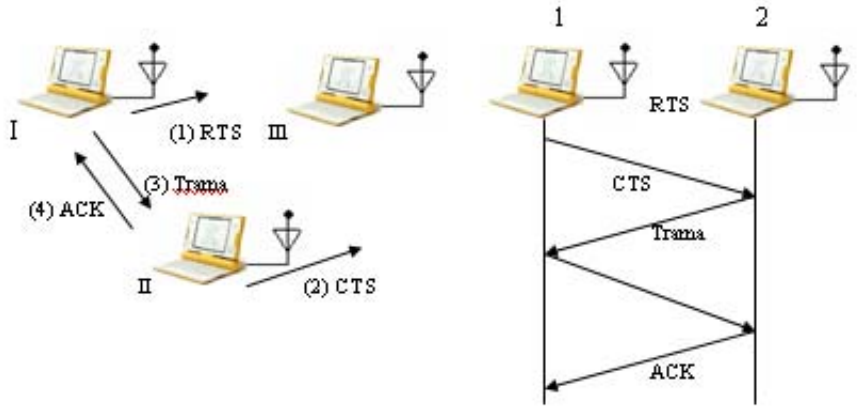


Figura 2.15 Procedimiento RTS / CTS

El proceso de envió de las tramas es el siguiente: cuando el nodo “I” tiene una trama para enviar, el proceso se inicia enviando una trama RTS la misma que sirve para reservar el enlace de radio y además silencia cualquier estación que pueda estar escuchando, la estación destino responde con un CTS, de la misma forma que RTS silencia las estaciones que se encuentren cercanas. Al completar la secuencia RTS/CTS, el nodo “I” puede transmitir sus tramas sin temor de interferencia, con la secuencia RTS/CTS también debe existir acuse de recibo positivo de todas las tramas.

2.6.1 MÉTODO DE ACCESO AL MEDIO CSMA/CA

En 802.11 el acceso al medio se controla mediante las funciones de coordinación de CSMA/CA: Función de coordinación distribuida (DCF, Distributed Coordination Funtion), función de coordinación de punto (PCF, Point Coordination Funtion), función de coordinación híbrida (HCF, Hybrid Coordination Funtion). Las

funciones de coordinación se describen a continuación y se ilustran el la figura 2.16:

a) **DCF:** Esta función primero verifica que el enlace de radio esté libre para luego transmitir, evita colisiones usando un tiempo aleatorio (backoff) tras cada trama. DCF también puede utilizar la técnica de limpieza RTS/CTS.

b) **PCF:** Proporciona servicios sin contención para lo cual se utilizan estaciones especiales llamadas coordinadoras de puntos, las cuales residen en los AP .A diferencia de DCF, PCF permite a las estaciones transmitir tramas tras un intervalo más corto.

c) **HCF:** Permite a las estaciones mantener múltiples colas de servicio equilibrando el acceso al medio en aplicaciones que soliciten mejor calidad de servicio

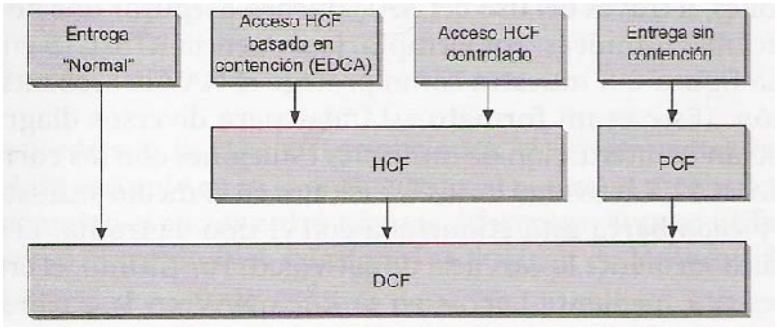


Figura 2.16. Funciones coordinación MAC

2.7 DEFINICIÓN Y ANÁLISIS DE SEGURIDAD EN REDES 802.11

En una red inalámbrica la seguridad es una aliada inseparable ya que su ausencia implicaría que la red deje una puerta abierta a la manipulación libre de la información, que sola dicha red puede acceder y el asegurar este medio es el desafió que se plantea, en esta parte del capítulo se revisara los métodos y

medios que permitan un acceso restringido y por ende protejan los datos que van a estar viajando en el medio físico que en nuestro caso es el aire.

Para poder proporcionar límites en un medio que físicamente casi no se lo puede hacer, se debe necesariamente utilizar criptografía para proteger las firmas del usuario y los datos que fluyen sobre conexiones establecidas. El cifrado es una ayuda para establecer confianza entre los dispositivos conectados. Dentro de la criptografía se puede establecer la identidad del usuario y además asegurar que los AP sean parte de la red a la que dicen pertenecer, una vez realizada la autenticación con la criptografía se codifica el tráfico de la red para que la información no sea interceptada.

En inicios de las redes 802.11 existían ya las primeras inseguridades a partir del momento de integrar redes con cables a extensiones con redes inalámbricas, esto da entre ver que la seguridad de la red esta entrelazada con la arquitectura de red, pero en la actualidad los protocolos de seguridad mejorados han permitido que una red inalámbrica se puede integrar en la redes con cables.

Para tener un panorama más comprensible se tomara como ejemplo el caso de la telefonía móvil con respecto a la telefonía fija, la primera utiliza equipos y sistemas de administración apropiados para su funcionamiento dentro de la red de telefonía fija siendo estas (telefonía móvil) extensiones lógicas de dicha red, situación que para los usuario es transparente ya que a la final hacen la misma labor de comunicación (voz).

A la seguridad de datos se la puede definir en función de tres aspectos, no siendo estas las únicas definiciones a seguir pero las citadas ayudan notablemente a comprender como una red puede ser segura:

- ✓ Integridad: esta queda violada cuando alguien no autorizado ha modificado los datos.

- ✓ Anonimato: la mayoría por no decir todos tiene secretos y es fácil entender el porqué de una filtración de información confidencial.
- ✓ Disponibilidad: los datos solo sirven en el momento que se los requieren, es por esto que los ataques de denegación de servicio son la amenaza más común ante la disponibilidad.

Antes de realizar cualquier diseño sobre seguridad se debe tener en claro cuáles son los problemas más importantes de seguridad en la red, cuanto se puede invertir para cumplir el objetivo de seguridad ya que en el mercado existen varias alternativas que facilitan la solución del problema.

Por diseño las LAN inalámbricas son flexibles pero a su vez la flexibilidad por seguridad es un gran inconveniente. La criptografía servirá de mucha ayuda al proporcionar autenticación y es así que permite identificar a usuarios que pueden acceder a los datos y los que no, una vez identificado el usuario se establecen las claves criptográficas utilizadas para los protocolos de confidencialidad.

La confidencialidad en si es mantener en secreto los datos que viajan a través del enlace inalámbrico para esto aplicamos un control criptográfico en base a un protocolo de cifrado que proporciona las claves para acceder a los datos solo a usuarios autorizados.

En los siguientes párrafos se va a exponer varios aspectos que forman parte de la inseguridad que puede estar asociada a una red LAN inalámbrica.

- ✓ Se debe tomar en cuenta que los AP de la red inalámbrica pueden ser una ruta hacia la red omitiendo las seguridades implantadas a estos dispositivos se los denomina puntos de acceso no autorizados (“simulados”), que pueden estar conectados a la red sin permisos pero pueden ser detectados y limitados en el daño que puedan causar por lo que se considera un problema manejable pero evidentemente sin despreocuparnos de su presencia.

- ✓ Otro aspecto importante que puede ocasionar problemas en una red inalámbrica es la inserción de tramas falsas (spoofing[17]) y falsear la integridad de la información para dar una solución sólida hay que requerir a un conjunto completo de protocolos criptográficos a esto se lo puede reforzar con un protocolo de cifrado (WPA, Acceso Wi-Fi protegido) que nos permita autenticar cada trama para evitar ataques de inserción y falsificación.
- ✓ El ruido en las bandas de frecuencia 802.11 puede interrumpir drásticamente las comunicaciones evitando así que fluya cualquier dato, la mejor solución es encontrar el origen del ruido y anularlo.
- ✓ Clientes falsos, son los usuarios que con sus equipos personales se integran a la red de la oficina, estos equipos generalmente no se encuentran con las respectivas seguridades básicas (antivirus)que si los tienen los equipos de las oficinas, provocando que sean un potencial problema de inseguridad. Para poder manejar a estos clientes falsos ("vectores virales") se están desarrollando dos opciones, la primera es ejecutando un escaneo de los bordes de la red esto con escáneres de virus y además con herramientas similares en los conmutadores de la red, siendo su respuesta a largo plazo; la segunda opción que es nueva por tanto se está desarrollando, es la de Microsoft, la cual requiere que se realice la autenticación tanto del equipo como del usuario con esto se lograría asegurar que el usuario está trabajando con una maquina autorizada y por ende con sus respectivas protecciones de seguridad, encargándose los servidores de autenticación de unir tanto la autenticación del usuario con la maquina, pero esto tiene una contra, criptográficamente no es aconsejable unir ambas autenticaciones debido a que no están fuertemente ligadas.
- ✓ Al servir las redes inalámbricas a varios usuarios hay que clasificarlos por grupos separados sin que puedan compartir información para

[17] Spoofing: uso de técnicas de suplantación de identidad

conservar esta separación en el enlace inalámbrico se necesita de diferentes claves criptográficas para cada grupo a través de VLAN (Virtual Local Area Network, Red de Área Local Virtual), filtros de paquetes y cortafuegos. Esta separación no tiene mucho efecto realizarla si el lugar donde va a ser implementado es relativamente pequeño.

2.7.1 AUTENTICACIÓN Y CONTROL DE ACCESO

La facilidad con la que se pueden conectar las estaciones a las redes inalámbricas es una ventaja que brindan muchas de las nuevas tecnologías inalámbricas y para su protección se debe implementar un control de acceso sólido aplicado de las siguientes cuatro formas:

- ✓ Autenticación de estación: En principio se realiza una autenticación de clave compartida que depende de una clave WEP[18], en varios productos del mercado realizan un filtrado de direcciones MAC (Medium Access Controller, Control de Acceso al Medio) para evitar el acceso de usuarios no autorizados.
- ✓ Asociación: Ya con la aprobación de la autenticación, las estaciones intentan asociarse con el punto de acceso en esta instancia no existe componente de seguridad.
- ✓ Capa de enlace: Una vez que la asociación a establecido el puerto de red virtual en el punto de acceso para una estación inalámbrica, es necesario aplicar protocolos de seguridad de la capa enlace basados en 802.1X para clasificarlos en usuarios autorizados y los que no serán rechazados de la red.
- ✓ Capa de transporte o de red: En este nivel se pueden utilizar los cortafuegos para aislar redes no confiables y autenticar usuarios y a

[18] WEP: Privacidad equivalente al cableado (Wired Equivalente Privacy). Estándar para codificación individual de las tramas de datos.

demás dispositivos de terminación VPN (Virtual Protocol Network, Protocolo Virtual de Red) suministrando cifrado en redes que no son de confiar.

Existe un enlace estructural entre el modelo OSI y los protocolos de autenticación ya que su funcionamiento actúa según sus capas, siendo en la capa enlace donde se ha desarrollado sólidamente mecanismos de seguridad.

En la tabla 2.2 se indican los protocolos a ser utilizados por los administradores de la red, partiendo desde el más débil al más sólido.

PROTOCOLOS	DESCRIPCION
Autenticación de clave WEP compartida	Los sistemas que quieren acceder a la red responden a un desafío desde el AP
Filtrado de direcciones MAC	Cada AP de la red es programado con una lista de direcciones MAC que pueden acceder a la red
Clave WPA compartida previamente (VPA-PSK o WPA Personal)	WPA incorpora el modo de clave compartida previamente esto permite a las estaciones autenticarse a una red mientras esté en posición de una sola contraseña de paso
Protocolos basados en 802.1X	Nos permite identificar y autenticar usuarios antes de que puedan acceder a la red. Se basa en EAP, Extensible Authentication Protocol. (WPA Enterprise)
Autenticación de la capa red	Las redes basadas en IP son muy inseguras pero existen varios sistemas y protocolos aplicables cuando se haya establecido la capa red (IP) y en redes inalámbricas se unirá a la tecnología VPN

Tabla 2.2 Protocolos de seguridad inalámbricas

No es recomendable aplicar la seguridad en la fase de autenticación de la estación o en la fase de asociación ya que no son nada sólidos. Existen dos opciones de “seguridad” en estas fases que son: “red cerrada” (supresión de difusión SSID) y la autenticación de clave WEP compartida. A la red cerrada también se la conoce como red encubierta, en la cual las estaciones se tenían que configurar con el nombre de la red (SSID) utilizada por un punto de acceso (AP). Su funcionamiento es el siguiente: Los AP envían tramas Beacon pero sin el SSID con esto existía una ganancia mínima sobre la privacidad. Por otro lado los clientes para asociarse debían enviar una petición de prueba con el SSID (Clave Oculta) sin embargo las peticiones de prueba no están cifradas, esto conlleva a que cualquier estación puede observar el intercambio de tramas de pruebas y ver el SSID para luego ser utilizadas en posteriores asociaciones.

La segunda opción es la autenticación de clave WEP compartida, en el cual el AP emite un desafío para un dispositivo que está buscando acceso a la red, pero esta autenticación es fácil de romper con lo cual no tiene protección ante usuarios malignos que intentan autenticarse en la red. Se puede escuchar una respuesta legítima a un desafío WEP (Wired Equivalente Privacy, Privacidad equivalente al cableado) sin conocer la clave WEP pero es imposible enviar tráfico sin recuperar en primera instancia la clave WEP.

Otra opción es el filtrado de direcciones MAC (Medium Access Controller, Control de Acceso al Medio) en los cuales los puntos de acceso (AP) registran una lista de direcciones MAC autorizadas y son rechazadas las peticiones de acceso a las estaciones que no se encuentran registrados en dicha lista, pero también es vulnerable a los ataques ya que los paquetes de la red pueden ser supervisados para obtener un listado de direcciones MAC permitida

- ✓ Autenticación de la capa de enlace: El acceso a la red es más restringido por la autenticación y solo puede obtener el acceso completo cuando se haya identificado de forma positiva. La autenticación de la capa enlace

es transparente para los protocolos de red y funcionara perfectamente con el que elijan.

Las redes que se basan en IP e IPX cada vez son más homogéneas. Para asegurar tanto IP como IPX se puede utilizar la autenticación de la capa enlace.

- ✓ WPA[19] Personal (Clave compartida previamente): Su funcionamiento se basa en distribuir una clave compartida previamente (WPA– PSK) a todos los clientes inalámbricos, la clave que se utiliza para el enlace inalámbrico se la calcula en base a números aleatorios intercambiados junto con la clave compartida previamente, WPA PSK en un método abreviado que calcula la clave maestra compartida previamente a partir de la contraseña de paso y del SSID, siendo estas utilizadas por todas las estaciones de la red.

  En cuanto a la seguridad de WPA-PSK está ligada a la calidad de la contraseña de paso, la cual no debe ser muy corta ya que estaría sujeto al ataque, lo ideal sería que utilice la clave de 256 bits compartida que sería una contraseña de paso sólida.

  Generalmente el uso de la clave WPA compartida previamente tiene sentido en redes relativamente pequeñas y cuyo riesgo de seguridad no tiene mucho valor.

- ✓ Autenticación EAP basada en 802.1X: Más que un protocolo EAP (Extensible Authentication Protocol, Protocolo de autenticación extensible) basado en 802.1X es una estructura extensible de la cual se puede seleccionar desde un menú de protocolos dependiendo de sus fortalezas y debilidades, considerando los requerimientos prácticos impuestos por las redes inalámbricas como son: un cifrado fuerte de

[19] WPA (Wi-Fi Protected Access, Acceso Protegido Wi-Fi)

credenciales, autenticación mutua, criptografía, claves WEP aleatorias. A estos requerimientos satisfacen los siguientes protocolos:

Lightweight LEAP (Tecnología de Extensiones de Clientes de Cisco) el primer protocolo en calcular claves dinámicamente para cada usuario, transmite credenciales cifradas, no proporciona protección criptográfica significativa y la autenticación solo mediante la ejecución de dos intercambios MS-CHAP (Microsoft Challenge Handshake Authentication Protocol, Protocolo de autenticación por desafió mutuo de Microsoft).

Los siguientes tres protocolos están basados en estándares de protocolo de seguridad de la capa transporte EAP (EAP-TLS, EAP-Transport Layes Security), el protocolo EAP protegido (PEAP, Protected EAP) y el protocolo de seguridad de capa transporte con túnel (TTLS, Tunneled Transport Layer Security). Como se puede apreciar los tres utilizan TLS, el cual proporciona protección criptográfica sólida a las credenciales del usuario y utilizan el intercambio de claves TLS para proporcionar una semilla para las claves de la capa enlace.

EAP-TLS utiliza certificados en ambas direcciones para la autenticación la cual requiere la existencia de un PK (Public Key Infrastructure, Infraestructura de clave compartida) para generar firmas digitales y distribuir certificados si no lo dispone probablemente EAP-TLS no sea un protocolo a ser elegido.

PEAP y TTLS utilizan el certificado del servidor en el túnel TLS para proporcionar la primera fase de la autenticación de la red al usuario, además el túnel TLS sirve para cifrar las credenciales del usuario utilizadas para la autenticación a la red en la segunda fase. TTLS es más flexible al pasar los datos de autenticación del usuario a la red a través del túnel y se puede utilizar con casi cualquier forma de autenticación de segunda fase. PEAP es más limitado debido a que la segunda fase se

ejecuta utilizando un método EAP. En la práctica el solicitante PEAP utilizado más comúnmente es el integrado en Windows XP/2000, el cual solo admite un protocolo de segunda fase que no requiere certificados: MS-CHAP, versión 2(Actualización MS-CHAP V1, es un proceso unidireccional con contraseña cifrada y autenticación mutua).

- ✓ Autenticación de capa red: Los cortafuegos en las primeras redes proporcionaban alguna funcionalidad de control de acceso además de mecanismos de autenticación sólidos, con la capacidad demostrada de integrarse con sistemas de contraseñas de una sola vez, como los token SecurID de RSA. Varios dispositivos Ipsec VPN (Virtual Protocol Network, Protocolo Virtual de Red) también tienen esa capacidad pero necesitan de extensiones de protocolo como eXtended Authentication (XAUTH), Hybrid Mode IKE o Challenge/Reponse for Authenticated Control Keys (CRACK). En lugar de terminación de Ipsec, el dispositivo VPN puede ser un dispositivo SSL VPN, el cual en vez de utilizar un software de cliente los dispositivos VPN basados en SSL pueden ser mucho más fáciles de utilizar ya que solo requieren un explorador Web.

  En la actualidad en lugar de implementar un cortafuegos se está empezando a utilizar sistemas de autenticación basados en la Web. La primera petición para un sitio Web queda atrapada por un Proxy, se redirecciona a una página de inicio de sesión segura, el sistema Web recoge cualquier paquete del cliente antes de finalizar la autenticación cuando esta tiene éxito se permite la transmisión de los paquetes del sistema del cliente, hay que tener en cuenta que varios de los sistemas de autenticación Web cifran al inicio de la sesión y no lo hacen en la capa de enlace sólido.

- ✓ Integración de la autenticación del usuario a través de RADIUS: Este combina el filtrado, la autenticación, la autorización del paquete y

servicios de cuentas (AAA)[20] que normalmente está configurado para un acceso remoto; que se lo utiliza como el fondo de la autenticación, independientemente de donde se ejecute la autenticación en la pila del protocolo. En muchas organizaciones se han colocado un servidor RADIUS para proteger las cuentas de usuarios que se encuentran centralizadas, proporcionando el acceso a muchos dispositivos de red.

Los servidores RADIUS se despliegan de forma que hagan referencia otros orígenes de datos para las cuentas de usuario para lo cual el servidor RADIUS actúa como traductor del protocolo. Varias de las formas más comunes de bases de datos de usuarios externos son:

- Dominios Windows: Integrar el Servidor RADIUS como contraseña Windows (Dominio Windows o Active Directory) es fácil para los usuarios ya que dichas contraseñas casi siempre son las credenciales del usuario principal. En el dominio de Windows los usuarios pueden utilizar la misma credencial para varios propósitos, esto es una ayuda para los usuarios que no les gusta recordar varias contraseñas.

- Token Card (como RSA SecurID): Muchos servidores RADIUS también pueden pasar credenciales directamente a un servidor de Token Card para su aprobación su integración permite a los administradores requerir una autenticación token larga con redes inalámbricas.

- Directorios LDAP(Lightweight Directory Access Protocol, Protocolo ligero para acceder al servicio de directorio): En un directorio se pueden guardar todas las contraseñas, los derechos de acceso, las directivas y la información de contacto y cuando se quiere acceder a los directorios LDAP, los servidores RADIUS pueden dar la autorización basándose en la información aprendida de LDAP.

[20] AAA: (Autenticación, Autorización y Administración de uso). Puede interpretarse como una estructura para el control de acceso de recursos informáticos.

- Áreas Kerberos: Los servidores RADIUS aceptan credenciales del usuario final y las utilizan para obtener una etiqueta Kerberos, su integración es imprecisa ya que dichas etiquetas de usuarios están vacías y no se utilizan en la autorización

- Sistemas de contraseña Unix: Incluyen Módulos de autenticación de conexión (PAM, Pluggable Authentication Modules) y el Sistema de información de red (NIS, Network Information System). Los servidores RADIUS que utilizan estos esquemas de autenticación se instalan en el sistema Unix e intentan validar las credenciales de usuario con una llamada al sistema.

- Proxy RADIUS: Los servidores RADIUS pueden pasar peticiones de autenticación a otros servidores RADIUS, en un entorno de cuentas y de usuarios distribuidos es muy posible la creación de una base de datos centralizada. La mejor solución es asegurarse de que los servidores RADIUS puedan hacer referencia a peticiones de autenticación a otros servidores RADIUS para el procesamiento.

- TACACS: Siendo un servicio de control de acceso alternativo se utiliza para guardar cuentas para cualquier persona que no pertenezca al personal de administración de la red.

✓ Autenticación RADIUS y bases de datos de Microsoft Windows: En Windows las llamadas de la API (Application Programming Interface, Interfaz de Programación de Aplicaciones) del sistema operativo pueden buscar cuentas de usuarios en los controladores de dominio otra opción es utilizar protocolos de red entre servidores para buscan cuentas de usuario. Los servidores RADIUS externos pueden ejecutar un software diseñado para un controlador de dominio y por consiguiente buscar cuentas de Windows en la red. RADIUS debe estar instalado sobre un controlador de dominio para buscar cuentas de usuario en Windows.

El servidor de autenticación de Internet (IAS, Internet Authentication Server), el servidor RADIUS de Microsoft, pueden utilizar comunicaciones Active Directory[21] para buscar cuentas de usuario guardadas en otros servidor miembro Active Directory. Cuando la petición de credenciales de usuario se despacha a controlador del dominio a través de su API, el controlador del dominio puede proceder a utilizar protocolos de Active Directory para buscar cuenta del usuario remotamente.

En la mayoría de instalaciones actuales de Active Directory ahora se basan en un modo nativo sin opción de compatibilidad. Si se requiere efectuar una autenticación de las cuentas de usuario con Active Directory una opción es utilizar IAS de Microsoft o buscar un controlador de dominio para servidor RADIUS de terceros (Teniendo en cuenta que la mayoría de servidores RADIUS de terceros no pueden ser instalados en el entorno Windows).

2.7.2 SEGURIDAD A TRAVÉS DEL CIFRADO

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior. Es por eso que una red tiene que proteger las transmisiones del usuario ante las posibles escuchas clandestinas. En las LAN inalámbricas se utilizan diversos protocolos de cifrado:

[21] Active Directory: es un servicio de directorio de Microsof que almacena información acerca de los objetos de una red y la pone a disposición de los usuarios y administradores de la red

- ✓ WEP estático: (Wired Equivalent Privacy, Privacidad Equivalente al Cableado) es un protocolo de cifrado de último recurso, con este protocolo se utiliza una sola clave para asegurar las transmisiones entre el cliente y el punto de acceso.

  Este sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes inalámbricas está basado en el algoritmo de cifrado RC4 y utiliza claves de 64 bits (40 bits más 24 bits del vector de inicialización IV), de 128 bits (104 bits más 24 bits del IV).

  El protocolo WEP se basa en dos componentes para cifrar las tramas que circulan por la red: el algoritmo de cifrado RC4 y el algoritmo de chequeo de integridad CRC. (Mecanismo de detección de errores en sistemas digitales).

  RC4 es un algoritmo de cifrado de flujo. Es decir, funciona expandiendo una semilla o "seed" para generar una secuencia de números pseudoaleatorios de mayor tamaño. Esta secuencia de números pseudoaleatorios se unifica con el mensaje mediante una operación XOR para obtener un mensaje cifrado. Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar el mismo seed para cifrar dos mensajes diferentes, ya que obtener la clave sería trivial a partir de los dos textos cifrados resultantes. Para evitar esto, WEP especifica un vector de inicialización IV) de 24 bits que se modifica regularmente y se concatena a la contraseña (a través de esta concatenación se genera el seed que sirve de entrada al algoritmo RC4) para evitar secuencias iguales; de esta manera se crean seeds nuevos cada vez que varía.

  El principal problema con la implementación del algoritmo anteriormente descrito es el tamaño de los vectores de inicialización. A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que

rápidamente se encuentren dos mensajes con el mismo vector de inicialización, y por lo tanto sea fácil identificar la clave. Por lo tanto es inseguro debido a su implementación. Aumentar los tamaños de las claves de cifrado sólo aumenta el tiempo necesario para romperlo.

- ✓ WEP dinámico basado en 802.1x: En el cifrado dinámico las claves aparecen en forma aleatoria, que pueden provenir de un método de autenticación que las genere en cortos intervalos de tiempo o se puede introducir como secreto compartido previamente.

  WEP dinámico es un paso intermedio hacia mejores protocolos de seguridad y solo se debe utilizar cuando el equipamiento no admite TKIP. Cuando se utilice WEP dinámico hay que asegurarse de establecer una duración de clave relativamente corta.

- ✓ Protocolo de Integridad de clave temporal (TKIP Temporal Key Integrity Protocol): Es un protocolo de gestión de claves dinámicas admitido por cualquier adaptador que permite utilizar una clave distinta para cada paquete transmitido. La clave se construye a partir de la clave base, la dirección MAC de la estación emisora y del número de serie del paquete como vector de inicialización. Este protocolo forma parte de 802.11i e incluye dos nuevos mecanismos de seguridad de capa enlace y está diseñado para ofrecer una seguridad incrementada sobre interfaces inalámbricas con asistencia de hardware para funcionar con el procesamiento de tramas WEP primitivas es por eso que mantiene el cifrado basado en el algoritmo RC4,al igual que el protocolo WEP dinámico TKIP depende de una fuente de datos aleatorios para servir como base de sus claves, más allá de las similitudes básicas, añade un cifrado por trama para interrumpir los ataques contra el IV y reproducir la protección para evitar que las tramas se retransmitan posteriormente TKIP también mejora la comprobación de integridad al asegurar que el

remitente de una trama tiene la clave criptográfica apropiada para detectar cualquier sabotaje de la trama durante su transmisión.

- ✓ Protocolo CB-MAC en modo contador: (CCMP[22], Counter Mode CBC-MAC Protocol): Es un protocolo importante de 802.11i, utiliza nuevas operaciones criptográficas y que tiene las siguientes características:

  - ➢ Algoritmo criptográfico que proporciona integridad y confidencialidad.

  - ➢ Permite utilizar una sola clave para cifrado e integridad reduciendo así la sobrecarga de cálculo y mejorando la eficiencia.

  - ➢ Se basa en el modo CCM del algoritmo de cifrado AES23 y utiliza claves de 128 bits con vectores de inicialización de 48 bits.

  - ➢ Consta del algoritmo de privacidad que es el "Counter Mode" (CM) y del algoritmo de integridad y autenticidad que es el "Cipher Block Chaining Message Authentication Code" (CBC-MAC).

  - ➢ El inconveniente principal de CCMP es una deficiencia de implantación común en el software cliente.

- ✓ Protocolos de seguridad de capa superior (Ipsec, SSL[24] y SSH[25]): En lugar de proteger la red inalámbrica en la capa de enlace, es posible aplicar protocolos de cifrado de larga duración en la capa de red, como IPsec, SSL o SSH; pero el inconveniente de utilizar una seguridad en niveles superiores de la pila es que los protocolos de seguridad solo pueden proteger su contenido.

---

[22] CCMP: (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) modo contrario con protocolo del código de la autentificación del mensaje de encadenamiento del bloque de la cifra.

[23] AES: (Advanced Encryption Standard) Estándar de cifrado avanzado de datos

[24] SSL: (Secure Socket Layer) capa de zócalo segura, es un protocolo comúnmente usado para manejar la seguridad de la transmisión de mensajes en el Internet

[25] SSH (Secure SHell) Estructura Segura, es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red

Ipsec: Es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y cifrado y, de esta manera, asegurar las comunicaciones a través de dicho protocolo. IPsec actúa a nivel de capa de red, protegiendo y autenticando los paquetes IP entre los equipos que forman parte de la red, no está ligado a ningún algoritmo de encriptación o autenticación, tecnología de claves o algoritmos de seguridad específico. Es más, IPsec es un marco de estándares que permite que cualquier nuevo algoritmo sea introducido sin necesidad de cambiar los estándares.

Este protocolo proporciona una forma de identificar usuarios, cifrar tráfico y asegurarse de que los paquetes no han sido saboteados durante su trayecto.

La protección en la capa de red proporciona servicios de seguridad a la capa de red y a cualquier elemento superior en la pila, pero no a las capas que están por debajo de está.

IPsec es independiente de la aplicación con la que se utiliza. Siempre que las aplicaciones puedan tratar la demora incrementada del encapsulado y descifrado de IPsec.

Una alternativa a IPsec es admitir solo aplicaciones con fuertes sistemas criptográficos integrados. Los sistemas basados en Web se pueden asegurar con una capa de zócalo segura (SSL, Secure Socket Layer). También se puede utilizar SSH (Secure Shell, utiliza un canal de comunicación encriptada y mecanismos de validación de usuarios) para asegurar varios tipos de tráfico de red basados en TCP.

2.7.3 PUNTOS DE ACCESO FALSOS

Los denominados puntos de acceso (AP)"falsos" pueden suponer amenazas importantes. La principal es que un dispositivo instalado por usuarios no tendrá toda la configuración de seguridad de una implantación autorizada. Los dispositivos no autorizados pueden interferir en el funcionamiento de la red existente.

Los AP no autorizados que instalan los empleados para su uso propio o para el departamento son una gran preocupación para los administradores de redes. Estos empleados suelen instalarlos porque están en puntos "muertos" de cobertura o porque no están satisfechos con la capacidad que ofrecen sus redes de área local (LAN) tradicionales. Los puntos de acceso no autorizados que instalan los empleados crean una infraestructura paralela de LAN inalámbrica que permite que cualquier usuario con un adaptador de cliente se conecte a la red. Estos puntos de acceso falsos forman una conexión de LAN inalámbrica no protegida que pone en peligro a toda la red.

- ✓ Detección de los puntos de acceso falsos: El primer paso para tratar los dispositivos falsos es descubrir que existen. Algunos dispositivos de radio, en alguna parte tienen que advertir la existencia de un dispositivo no autorizado, es por eso que por razones de administración y coste, ahora la detección está integrada en los sistemas LAN inalámbricos principales. Dependiendo de la implantación del suministrador, el componente de detección se puede implantar a través del uso de una opción de escaneado para explorar periódicamente el sistema en busca de dispositivos no autorizados. Los escaneados en busca de dispositivos no autorizados pueden ser escaneados pasivos, que escuchan tráfico, tramas Beacon o respuestas de prueba o pueden ser escaneados activos, que utilizan las tramas de petición de prueba 802.11 para hacer que se muestren las redes no autorizadas.

Para ser efectiva la detección tiene que cubrir todos los canales 802.11 disponibles.

Las opciones de detección pueden estar integradas dentro de la infraestructura de LAN inalámbrica o pueden requerir dispositivos independientes tales como sensores dedicados que proporcionan la mejor detección pero son costosos. Otra opción sería utilizar radios que proporcionan servicio a los usuarios para detectar dispositivos no autorizados, es mucho más barato pero puede interrumpir o disminuir el servicio proporcionado a los usuarios.

Algunos sistemas 802.11 completos también pueden observar el trafico del cliente y comparar la lista de clientes vista en el dominio de radio con los clientes asociados a la infraestructura. Cualquier cliente presente en esta última lista que no se encuentre en la primera lista, está asociado a implantaciones no autorizadas.

- ✓ Ubicación física de los puntos de acceso falso: Una vez detectado un punto de acceso falso, es necesario localizarlo para lo cual existen diversos tipos de tecnologías de localización tales como:

  - Cálculos de radio del punto de acceso (AP) más cercano: El método más fácil para localizar un punto de acceso falso es utilizar el radio al AP más cercano como se muestra en la figura 2.16 Tras buscar por la red una dirección MAC, el sistema puede localizar un punto de acceso falso basándose en la ubicación del AP que ha detectado el dispositivo. Tomando en cuenta la fuerza de la señal recibida en el AP que detecta, se puede calcular el radio máximo localizando la distancia a la que está operando un dispositivo a una potencia de transmisión máxima para que la fuerza de la señal recibida calculada coincida con el valor medido.

Los cálculos de radio de punto de acceso (AP) sufren de distintos fallos. En primer lugar, el radio del espacio libre de una señal trasmitida a la potencia máxima es muy probable que sea mucho mayor que el radio real. Mientras que un modelo de propagación de espacio libre puede permitir un radio de cobertura de unos 30 metros y medio, el espacio de aproximadamente 2800 kilómetros cuadrados resultante es demasiado largo para ser útil. Para detectar mejor el dispositivo falso, algunas herramientas de localización crearán un modelo matemático para el entorno de radio y tendrán en cuenta cualquier característica del edificio a lo largo de una ruta determinada.

Una pared como se indica en la figura 2.17 tiene el efecto de reducir el radio de cobertura ya que las señales de radio tienen que penetrar la pared. Cuando la señal de radio se encuentra frente a la pared, la fuerza de la señal cae, lo que tiene el efecto de reducir el área de cobertura. La corrección del radio de cobertura para las características del edificio funciona mejor cuando existe un gran número de ellos; no es mucho más que una mejora en las oficinas llenas de cubículos típicos donde la distancia de propagación es mucho más larga.

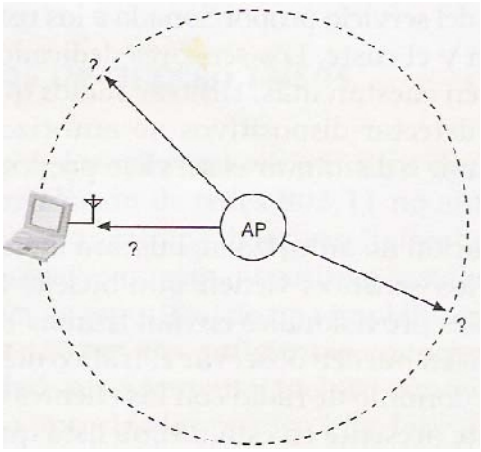


Figura 2.17 Método de Cálculo de radio de punto de acceso (AP) más cercano

- Triangulación: Este método mide la distancia desde tres puntos conocidos para determinar una ubicación. Muchas de las técnicas de "triangulación" utilizadas en los sistemas LAN inalámbricos pueden funcionar con más de tres puntos de medida.

  La superposición de áreas de cobertura, la superposición de radios y, en algunos casos, las simulaciones probabilísticas se utilizan para calcular las ubicaciones probables de los dispositivos. En la figura 2.18, las áreas de cobertura superpuestas de los tres AP se utilizan para calcular una probabilidad de la ubicación. Igual que en la solución del radio AP, se pueden utilizar algunos algoritmos de triangulación junto con los conocimientos de construcción del edificio para definir aún más la ubicación.

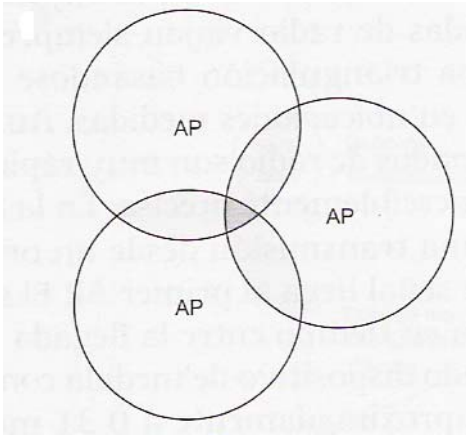


Figura 2.18 Método de Triangulación

- Huella de radio frecuencia (RF): La ubicación se puede detallar aún más tomando medidas de la huella RF Tras generar un común de presiones sobre cómo interactúan las bandas de radio, el modelo matemático se define con más detalle sobre cómo se comportan realmente las ondas. Para crear una base de datos de huellas los

dispositivos símbolo se colocan en ubicaciones conocidas y posteriormente se miden. Los datos sobre la fuerza de la señal recibida y otras características se guardan entonces como una "huella" de dicha ubicación. Las huellas incluyen todas las características de propagación de la señal que son difíciles de calcular, como la reflexión de las paredes y la interferencia de múltiples rutas. Cuando se han colocado dispositivos desconocidos, sus características de señal se pueden comparar con la base de datos de huellas para definir con más detalle la predicción de la ubicación. Mejorar la calidad de las predicciones de la ubicación depende de la: cantidad de ubicaciones de huellas recopiladas como parte de la investigación extendida del sitio. Aunque la huella puede mejorar la información de la ubicación, pueden que requieran la recopilación de una gran cantidad de datos adicionales para crear una base de datos de huellas bastante grande para obtener la precisión deseada.

- Cronometraje diferencial: Un método final de ubicación se basa en el tiempo relativo de las señales recibidas. La fuerza de la señal depende de una variedad de factores, incluyendo la construcción del edificio. Sin embargo, las ondas de radio viajan siempre a la velocidad de la luz. Se puede llevar a cabo una triangulación basándose en el tiempo de llegada relativo de las transmisiones en ubicaciones medidas. Aunque esta técnica es potencialmente más precisa, las ondas de radio son muy rápidas y se requiere una sincronización de los tiempos increíblemente precisa. Como se indica en la figura 2.19, dos puntos de acceso (AP) están midiendo la llegada de una transmisión desde un origen. Pasada una determinada cantidad de tiempo, la señal llega al primer AP. El sistema de localización tiene que medir la diferencia en tiempo entre la llegada de la señal al primer dispositivo de medida y el segundo dispositivo de medida con una extrema precisión. Las ondas de radio viajan aproximadamente a 0,31 metros por nanosegundo, lo

que requiere que los dispositivos de localización puedan distinguir diferencias de tiempo muy pequeñas entre los dispositivos distribuidos. La solución de llegada de tiempo diferencial normalmente requiere el uso de dispositivos muy especializados con equipamiento de cronometraje si es mucho más preciso de que existe realmente en los puntos de acceso típicos.

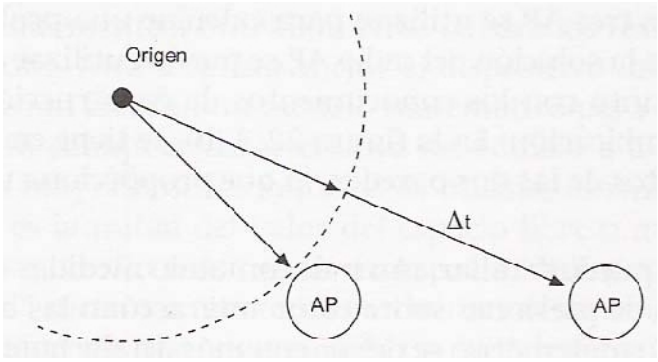


Figura 2.19 Cronometraje diferencial

CAPÍTULO III

HARDWARE DE LA RED INALÁMBRICA

3.1 TARJETAS INALÁMBRICAS

Una tarjeta inalámbrica viene definida por la compañía, el modelo y el bus.En cuanto a las compañías algunas de las más conocidas son: Conceptronic, Linksys, ICOM, D-Link, Cisco/Aironet. y son las empresas encargadas de la manufactura y venta de la tarjeta. Estas empresas se encargan de montar la tarjeta, no de desarrollar el chipset ni sus drivers, de ahí que diferentes modelos de una misma compañía puedan tener distintos chipsets

El modelo constituye una serie de números y letras y el tipo de bus o interfaz entra dentro de los fundamentos físicos de los computadores y es la ranura de entrada o el puerto de conexión de la tarjeta a continuación se nombra brevemente los puertos de conexión más comunes y en qué situaciones se utilizan:

- ✓ PCI (Peripheral Component Interconnect): Es un bus de computadora estándar para conectar dispositivos periféricos directamente a la tarjeta madre de la computadora (bus local).
- ✓ MINIPCI: es una ranura de menor tamaño que la PCI para portátiles
- ✓ PCMCIA: (Personal Computer Memory Card International Association), Asociación de la industria de fabricantes de hardware para ordenadores portátiles encargada de la elaboración de estándares. Ranura normalmente utilizado en computadoras portátiles

3.1.1 TIPOS DE TARJETAS INALÁMBRICAS PCMCIA, MINI PCI, PCI Y USB

a) Las tarjetas PCMCIA, se usan en ordenadores portátiles, que normalmente son los que vienen equipados con este tipo de conector como se muestra en la figura 3.1

Figura 3.1 Tarjeta inalámbrica PCMCIA

b) Las MiniPCI, vienen incorporadas habitualmente en los portátiles y los routers inalámbricos, es un pequeño circuito similar a la memoria de los ordenadores portátiles, como se puede apreciar en la figura 3.2 Incluye la antena, aunque en la mayor parte de los dispositivos se puede incorporar una antena externa adicional

Figura 3.2 Tarjeta inalámbrica MiniPCI

c) Las tarjetas inalámbricas PCI son similares a las tarjetas de red, llevan una pequeña antena para recepción-emisión de la señal. Su uso está indicado en ordenadores de sobremesa. En la figura 3.3 se puede apreciar su similitud con las tarjetas Ethernet que normalmente encontramos en un equipo.

Figura 3.3 Tarjeta inalámbrica PCI

d) Las tarjetas USB son fáciles de instalar ya que pueden ser usadas en cualquier ordenador que disponga de puertos USB, sea sobremesa o portátil, incluso es posible adaptarlos a cualquier aparato electrónico que disponga de ese tipo de conector tal y como se muestra en la figura 3.4

Figura 3.4 Tarjeta inalámbrica USB

3.1.2 TARJETAS EXISTENTES EN EL MERCADO NACIONAL

a) TARJETA DE RED PCMCIA CNET WIRELESS

Figura 3.5 Tarjeta PCMCIA CNET Wireless

Características:

- ✓ Esta nueva tecnología proporciona casi 5 veces la velocidad del Standard existente.
- ✓ Los productos Wireless de CNet son completamente compatibles con todos los productos existentes.
- ✓ Una excelente ventaja de estos productos CNet Wireless, es que son muy fáciles de instalar y de operar.

En la tabla 3.1 se detalla las características técnicas de la tarjeta PCMCIA CNET Wireless.

CARACTERÍSTICAS TÉCNICAS DE LA TARJETA INALÁMBRICA PCMCIA CNET	
Modelo	CWC-854
Estándar	802.11g, 802.11b
Canales	1-11 (U.S.) 1-13 (Elsewhere Worldwide) 1-13,14 (Japan)
Modulación	802.11b: CCK, DQPSK, DBPSK 802.11 g: OFDM
Protocolo de red	TCP/IP, IPX, NetBEUI
Software que soporta	Windows XP/ME/2000/98SE
Interface	Cardbus
Antena	Built-in Antenna with diversity support.
Potencia de transmisión	15 dBm Typical
LED	Active/RX
Bits de clave WEP	64-Bit and 128-Bit
Dimensiones	117mm x 53mm x 3mm
Peso	0.13 kg
Voltaje	3.3V
Temp. Operación	-4° F to 158° F (-20° C to 70° C)
Temp.Almacenamiento	-40° F to 176° F (-40° C to 80° C)
Operation Humidity	10% to 90%, Non-Condensing
Storage Humidity	10% to 90%, Non-Condensing

Tabla 3.1 Características técnicas de la tarjeta PCMCIA CNET Wireless

b) TARJETA DE RED PCMCIA 3COM 54MB 802.11G

Figura 3.6 Tarjeta PCMCIA 3COM 802.11 g

Características:

- ✓ La tarjeta 3Com OfficeConnect Wireless 802.11g PC trabaja a velocidades de hasta 54 Mbps, a una distancia de hasta 100 metros (3,28 pies),por lo que este producto resulta ideal para pequeñas oficinas que trabajan con aplicaciones de audio, vídeo y multimedia exigentes.
- ✓ Esta tarjeta funciona con el punto de acceso 3Com Wireless 802.11g y es compatible con los productos 802.11b.
- ✓ La tarjeta 802.11g PC Card de OfficeConnect ofrece funciones de resistencia a fallos, tales como Dynamic Rate Shifting (cambio dinámico de velocidad), que adapta automáticamente la mejor velocidad de conexión a las condiciones ambientales, por lo que las conexiones permanecen claras y abiertas.
- ✓ Utiliza encriptación avanzada WAP de 256 bits, así como encriptación WEP por clave compartida de 40/64 y 128 bits para ayudar a proteger los datos en la LAN inalámbrica.

En la tabla 3.2 se detalla las características técnicas de la tarjeta PCMCIA 3COM 802.11g

CARACTERÍSTICAS TÉCNICAS DE LA TARJETA PCMCIA 3COM 54MB 802.11g	
Tipo de Ranura :	Type II o Type III PC Card de 32 bits (3,3 V)
Drivers Soportados:	NDIS 5: Me, 2000, 98 SE NDIS 5.1: Windows XP
Compatibilidad con normas:	Certificación Wi-Fi 802.11b y WPA, IEEE 802.11b, versión provisional del estándar IEEE 802.11g
Velocidades de Datos:	54, 48, 36, 24, 18, 12, 9, 6 Mbps (802.11g) 11, 5,5, 2, 1 Mbps (802.11b)
Banda de Frecuencias:	2,4 - 2,4835 GHz
Alcance Operativo:	Máxima de interiores: 100 metros (328 pies); Máxima en exteriores: 457 metros (1.499 pies)
Canales Operativos:	5-7 (Israel); 10-13 (Francia, Jordania); 1-11 (EE.UU., Argentina, Brasil, Canadá, Colombia, Méjico, Taiwán); 1-13 (en cualquier otro país)
Medio Inalámbrico:	DSSS (Espectro Ensanchado de Secuencia Directa)
Protocolo de Acceso a Medios:	CSMA/CA
Funciones de Resistencia a Fallos:	Dynamic rate shifting (cambio dinámico de velocidad)
Prestaciones:	Compresión, concatenación, expansión de paquetes, PRISM Nitro Directlink
Seguridad :	Encriptación WPA de 256 bits Encriptación por clave compartida WEP de 40/64 y 128 bits
Administración:	Wireless Card Manager, ajustes por defecto
Indicadores LED:	Enlace; Actividad

Tabla 3.2 Características técnicas de la tarjeta PCMCIA 3COM 802.11g

c) TARJETA INALÁMBRICA INTEL PRO/WIRELESS 2200BG MINI PCI 802.11b/g

Figura 3.7 Tarjeta Intel pro/wireless mini pci 802.11 b/g

Características:

- ✓ Esta tarjeta Mini PCI proporciona flexibilidad, velocidad y productividad en las conexiones inalámbricas y está diseñado para los portátiles.
- ✓ ThinkPad inalámbricos y ampliables con la antena UltraConnect integrada.
- ✓ El funcionamiento en doble modalidad servirá a los usuarios de ayuda para conectarse y conmutar entre las LAN inalámbricas b/g en el lugar de trabajo o, si se abonan y conectan a las LAN inalámbricas, en los lugares a donde viajan.
- ✓ La tarjeta Intel PRO/Inalámbrico 2200BG Mini PCI busca automáticamente la mejor conexión disponible.

En la tabla 3.3 se detalla las características técnicas de la tarjeta Intel pro/wireless mini pci 802.11 b/g

CARACTERÍSTICAS TÉCNICAS DE LA TARJETA INALÁMBRICA INTEL PRO/WIRELESS 2200b/g MINI-PCI	
Tipo de dispositivo	Adaptador de red
Factor de forma	Módulo de inserción
Tipo de interfaz(bus)	Mini PCI
Dimensiones(ancho x profundidad x altura)	6cm x 4,5 cm x 0,5 cm
Peso	12g.
Protocolo de interconexión de datos	IEEE 802.11b, IEEE 802.11g
Velocidad de transferencia de datos	54 Mbps
Banda de frecuencia	2.4 GHz

Tabla 3.3 Características técnicas de la tarjeta Intel pro/wireless mini pci 802.11 b/g

d) TARJETA INALÁMBRICA CNET PCI 54 MBPS WIRELESS-G

Figura 3.8 Tarjeta inalámbrica CNET PCI 54 Mbps g

Características:

- ✓ Cinco veces más rápido y compatible con equipos inalámbricos existentes.
- ✓ Seguridad inalámbrica: Hasta 128 bit WEP
- ✓ Rango de operación: Hasta 350 metros

- ✓ Sistema operativo: MS Windows 98 SE/ME/2000/XP

En la tabla 3.4 se detalla las características técnicas de la tarjeta inalámbrica CNET PCI 54 Mbps g

CARACTERÍSTICAS TÉCNICAS DE LA TARJETA INALÁMBRICA CNET PCI	
Estándar	802.11g, 802.11b
Canales	1-11 (U.S.) 1-13 (Elsewhere Worldwide) 1-13,14 (Japan)
Modulación	802.11b: CCK, DQPSK, DBPSK 802.11 g: OFDM
Protocolos de red	TCP/IP, IPX, NetBEUI
Software que soporta	Windows XP, Windows ME, Windows 2000, Windows 98SE
Interface	PCI
Antena	External Antenna with diversity support
Potencia de transmisión	IEEE 802.11b: 17dBm +/- 2dBm IEEE 802.11g: 14dBm +/- 2dBm
Indicador led	Ready, ACT
WEP Key Bits	64-Bit and 128-Bit
Dimensiones	120mm x 52mm x 1.6mm
Voltaje	5V
Temperatura Operación	-32° F to 104° F (0° C to 40° C)
Temperatura Almacenam.	-4° F to 158° F (-20° C to 70° C)
Operating Humidity	0% to 95%, Non-Condensing
Storage Humidity	0% to 95%, Non-Condensing

Tabla 3.4 Características técnicas de la tarjeta inalámbrica CNET PCI 54 Mbps g

e) TARJETA INALÁMBRICA DLINK PCI DWL-G510

Figura 3.9 Tarjeta inalámbrica DLINK PCI DWLG510

Características:

- ✓ La DWL-G510 es una tarjeta PCI de 32 bits con una velocidad de hasta 54Mbps que se instala rápida y fácilmente en los ordenadores de escritorio y cuando se usa con otros productos D-Link AirPlus G, se conecta de forma automática a la red. Al igual que los otros adaptadores inalámbricos de D-Link, el DWL-G510 puede usarse en modo Ad-Hoc para conectarse directamente a otros ordenadores inalámbricos a 2,4 GHz a fin de compartir datos en modo punto a punto, o en modo infraestructura para conectarse al punto de acceso inalámbrico o al router inalámbrico a fin de acceder a Internet desde una pequeña oficina o desde casa.
- ✓ La tarjeta inalámbrica DWL-G510 es compatible con dispositivos inalámbricos 802.11b/g.
- ✓ La DWL-G510 utiliza encriptación WEP 64/128/152-bit, WPA y 802.1x para la autentificación de los usuarios inalámbricos

- ✓ Esta tarjeta incluye, además, una utilidad de configuración que permite buscar las redes inalámbricas disponibles y crear perfiles de conexión detallados para las redes que se visitan con más frecuencia, así como su memorización.
- ✓ Configuración basada en web.
- ✓ WPA y 802.1x requieren que se use la aplicación «Zero Configuration» de Windows XP.

f) TARJETA INALÁMBRICA 3COM OFFICECONNECT WIRELESS USB 108MBPS 11g

Figura 3.10 Tarjeta inalámbrica 3COM OfficeConnect USB 108 Mbps 11g

Características:

- ✓ Práctica conectividad de alta velocidad y segura.
- ✓ Conexiones inalámbricas sencillas, fiables, de muy alta velocidad y seguras para usuarios de equipos de escritorio y portátiles.
- ✓ Los usuarios pueden acceder a los recursos de la red y al correo electrónico a velocidades de hasta 108 Mbps.

- ✓ Para mantener la privacidad de las conexiones inalámbricas, el adaptador USB soporta la encriptación avanzada WPA, así como la encriptación WEP básica. También soporta la última autenticación 802.1X para ayudar a protegerse contra usuarios no autorizados.
- ✓ Las conexiones inalámbricas de alta velocidad de 108 Mbps y el soporte de USB 2.0 ayudan a garantizar la capacidad de tráfico para aplicaciones que requieren un gran ancho de banda
- ✓ La antena plegable y el conector USB giratorio permiten múltiples orientaciones para un uso flexible
- ✓ La base de conexión USB con cable de extensión funciona con una variedad de diseños de equipos de desktop y portátiles
- ✓ El estándar 11g de alta velocidad también soporta redes 802.11b, preservando así las inversiones en equipos existentes
- ✓ La certificación Wi-Fi ayuda a garantizar la interoperabilidad con productos de otros fabricantes.

En la tabla 3.5 se detalla las características técnicas de la tarjeta inalámbrica 3COM officeconnect usb 108 Mbps 11g

CARACTERÍSTICAS TÉCNICAS DE LA TARJETA INALAMBRICA 3COM OFFICECONNECT USB 108MBPS 11g	
Tipo de bus	USB 2.0
Chipset	Atheros AR5523/AR2112
Interfaces	Cumple normas Wi-Fi 802.11 g/b
Drivers/Sistema operativo soportado:	NDIS 5: Windows 2000; NDIS 5.1: Windows XP
Velocidades inalámbricas de datos:	802.11g: 108, 54, 48, 36, 24, 18, 12, 9 y 6 Mbps 802.11b: 11, 5.5, 2 y 1 Mbps
Banda de frecuencias	2,4-2,4835 GHz

802.11b:	DSSS/CCK (Espectro Ensanchado en Secuencia Directa/Modulación por Código Complementario)
Protocolo de acceso a medios:	CSMA/CA
Canales operativos:	1-11 América del Norte, 1-14 Japón, 1-13 Europa (ETSI)
Alcance operative	En interiores: 100 metros; en exteriores: 400 metros
Tipo de antenna	Antena PCB
Potencia de transmisión inalámbrica:	802.11g: 18,3 dBm máx., 802.11b: 19,4 dBm máx.
Seguridad:	Encriptación AES, WPA, TKIP, y WEP; 802.1X con autenticación EAP-TLS y PEAP
Compatibilidad con normas:	802.11g, 802.11b, 802.3, Wi-Fi, WPA, AES, WEP, 802.1X
Condiciones ambientales operativas	Temperatura de funcionamiento: de 0° a 45° C (de 32° a 113° F) Humedad en funcionamiento: de 5 a 90% sin condensación Temperatura de almacenaje: de -20° a 70° C (de -4° a 158° F) Humedad de almacenaje: de 5 a 95% sin condensación
Requisitos del sistema	El CD de instalación requiere Windows XP o 2000

Tabla 3.5 Características técnicas de la tarjeta inalámbrica 3COM office connect usb 108 Mbps 11g

g) TARJETA INALÁMBRICA 3COM OFFICECONNECT WIRELESS USB 54MBPS 11G

Figura 3.11 Tarjeta inalámbrica 3COM officeconnect usb 54 Mbps 11g

Características:

- ✓ Para conexiones inalámbricas 802.11g sencillas y fiables a velocidades de hasta 54 Mbps ideal para aplicaciones multimedia o que necesiten un gran ancho de banda a distancias de hasta 100 metros (328 pies).
- ✓ El adaptador USB funciona con el punto de acceso 3Com OfficeConnect Wireless 11g para establecer una red de alta velocidad inalámbrica.
- ✓ Este adaptador es compatible hacia atrás con productos 802.11b. El adaptador USB ofrece la flexibilidad y comodidad de las conexiones USB sin sacrificar el rendimiento.
- ✓ Para proteger las conexiones inalámbricas, el adaptador USB soporta la encriptación WPA de 256 bits y la encriptación WEP por clave compartida de 40/64 y 128 bits.
- ✓ La certificación Wi-Fi ayuda a garantizar la interoperabilidad con los productos de otros fabricantes con certificación Wi-Fi

En la tabla 3.6 se detalla las características técnicas de la tarjeta inalámbrica 3COM officeconnect usb 54 Mbps 11g

CARACTERÍSTICAS TÉCNICAS DE LA TARJETA INALAMBRICA 3COM OFFICECONNECT WIRELESS USB 54MBPS 11g	
Tipo de Bus:	USB
Drivers/Sistema Operativo Soportado:	NDIS 5: Windows ME, 2000, 98SE NDIS 5.1: Windows XP
Velocidades de Datos:	54, 48, 36, 24, 18, 12, 9, y 6 Mbps
Banda de Frecuencias :	2,4-2,4835 GHz
Medio Inalámbrico :	DSSS y OFDM
Protocolo de Acceso a Medios :	CSMA/CA
Canales Operativos:	5-7 (Israel) 10-13 (Jordania) 1-11 (EE.UU., Canadá, Colombia, Méjico, Taiwán) 1-13 (Francia, Argentina, Brasil)
Alcance Operativo:	100 metros (3,28 pies)
Sensibilidad en Recepción :	802.11g 54 Mbps: -68 dBm 48 Mbps: -68 dBm 36 Mbps: -75 dBm 24 Mbps: -79 dBm 18 Mbps: -82 dBm 12 Mbps: -84 dBm 9 Mbps: -87 dBm 6 Mbps: -88 dBm 802.11b 11 Mbps: -82 dBm 5,5 Mbps: -84 dBm 2 Mbps: -86 dBm 1 Mbps: -88 dBm
Funciones de rendimiento:	Dynamic rate shifting (cambio dinámico de velocidad), compresión, concatenación, expansión de paquetes aviso de piggyback, PRISM Nitro Directlink
Seguridad :	Encriptación WPA de 256 bits Encriptación por clave compartida WEP de 40/64 y 128 bits
Compatibilidad con Normas :	Certificación WPA, IEEE 802.11g
Tensión de Funcionamiento:	3,0V - 3,6V
Salida máxima de transmisión de alimentación:	17Dbm
Condiciones Ambientales:	Temperatura de funcionamiento: de 0 a 50C (de 32 a 122F) Humedad en funcionamiento: de 0 a 90% sin condensación
Instalación, Configuración, y Administración:	Wireless Card Manager Ajustes por defecto
Dimensiones:	Altura 10,7cm (4,2") Anchura: 2,8 cm (1,1") Fondo: 1,1 cm (0,4")

Requisitos del sistema	PC portátil o de escritorio con puerto USB PC portátil o de escritorio con sistema operativo Windows 98SE/ME/XP/ 2000

Tabla 3.6 Características técnicas de la tarjeta inalámbrica 3COM officeconnect usb 54 Mbps 11g

3.2 ANTENAS

Las antenas siendo uno de los elementos más importantes dentro de un sistema RF (Radio Frecuencia) su utilidad es la de convertir las señales eléctricas de los cables en ondas de radio y viceversa.

En los diagramas de bloque, las antenas normalmente se representan con una forma triangular, tal como se ilustra en la figura 3.12

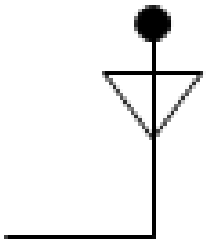


Figura 3.12 Representación de la antena en los diagramas

Es importante ubicar correctamente las antenas para delimitar el perímetro de la red consiguiendo así una forma de proteger la red.

3.2.1 FUNCIONAMIENTO Y TIPOS DE ANTENAS

Su proceso de funcionamiento es el siguiente: siendo la antena de material conductor, las ondas de radio golpean las antenas provocando que los electrones

fluyan en el conductor y se crea una corriente. De las misma forma al aplicar corriente a una antena se crea un campo eléctrico alrededor de la misma con esto a medida que la corriente a la antena cambia, también cambia el campo eléctrico. Un campo eléctrico que cambia produce un campo magnético y la onda se anula.

Una interfaz de red 802.11b que opera en la banda de los 2,4 GHz tiene una longitud de onda de 12,5 centímetros con una antena del tamaño correspondiente, esto se debe a la frecuencia: a mayor frecuencia, menor antena.

Colocar correctamente las antenas delimitara el perímetro de la red y disminuirá el riesgo de detectar la red, al mismo tiempo que reduce el espacio que les queda a los atacantes para maniobrar.

Dentro de las antenas existen dos características que hay que resaltar estas son: la ganancia (o ampliación de potencia) que ofrece la antena y el ancho del haz (que determina la zona de cobertura). La zona de cobertura debe tomarse en cuenta como una tercera variable, ya que los haces laterales y anteriores de algunas antenas son difíciles de describir en forma de anchos de haz.

La ganancia de una antena se expresa en forma de dBi ya que se establece como referencia un dispositivo radiador isotrópico abstracto, un dispositivo imaginario que radia potencia en todas las direcciones (un ejemplo seria una estrella). Se define como pasiva porque la antena no añade potencia. En lugar de este sistema, la ganancia se consigue enfocando las ondas radiadas para conseguir un haz más estrecho. El ancho de haz puede ser tanto vertical como horizontal.

Existen tres tipos generales de antenas que se diferencian en base a su potencia radiada y en el ancho de haz como se muestra en las figuras 3.13

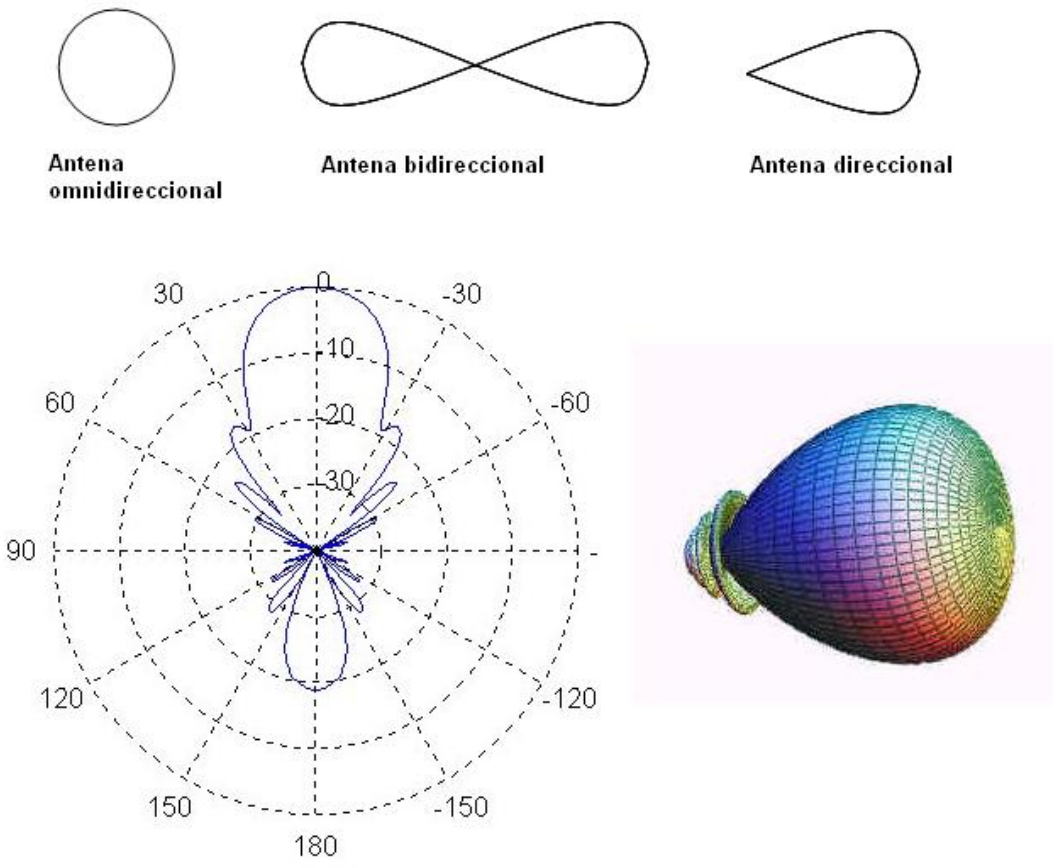


Figura 3.13 Tipos de antenas

1. Antenas omnidireccionales

- ✓ Antena para montaje en mástil
- ✓ Antena para montaje en pilar
- ✓ Antena de plano de tierra
- ✓ Antena para montaje en techo

2. Antenas parcialmente direccionales

   - ✓ Antena de tipo parche
   - ✓ Antena de panel
   - ✓ Antena sectorial
   - ✓ Antena Yagi

3. Antenas de alta direccionalidad

   - ✓ Antena parabólica
   - ✓ Antena de rejilla

A continuación se describen las características de los tres tipos generales de antenas que luego serán seleccionadas de acuerdo a las necesidades del diseño de la red inalámbrica.

a) Las antenas omnidireccionales tienen una zona de cobertura horizontal de 360 grados y consiguen su ganancia limitando el ancho del rayo vertical y son usadas generalmente para proporcionar enlaces punto a multipunto (topología estrella) para varios clientes e incluso redes.

b) Las antenas parcialmente direccionales sectoriales, de tipo parche y de panel crean un patrón de radiación en forma de “burbuja” que se extiende de 60 a 120 grados con respecto a una dirección. Este tipo de antenas se utilizan para cubrir un área a lo largo de una calle o de un pasillo largo. Se pueden colocar varias antenas parcialmente direccionales en círculo, pueden funcionar como en sustitución de una antena omnidireccional, claro con la ventaja de una ganancia y ancho de banda vertical mucho mayor pero a un precio bastante más alto. Las antenas Yagi son antenas parcialmente direccionales sectoriales utilizadas para establecer enlaces de interconexión de rango medio entre edificios corporativos, representa

una alternativa realmente económica con respecto al empleo de fibra óptica esto en situaciones en que el cableado de categoría 5 con su límite de 100 metros para una red Ethernet 100BaseT no valdría.

c) Las antenas de alta direccionalidad emiten un haz cónico muy estrecho capaz de alcanzar el horizonte visible y utilizarse para enlaces punto a punto de largo alcance, o en situaciones en que es preciso disponer de un enlace punto a punto de gran calidad. Debido a su ganancia generalmente elevada, las antenas direccionales son utilizadas para atravesar obstáculos como pueden ser paredes u objetos sólidos o cuando no se disponga de ninguna otra alternativa.

3.2.2 ANTENAS EXISTENTES EN EL MERCADO NACIONAL

a) ANTENA INTERIOR OMNIDIRECCIONAL DLINK ANT24-0501 5dBi

Figura 3.14 Antena interior omnidireccional DLINK ANT24-0501 5dBi

La ANT24-0501 de D-link es una antena omnidireccional de alta ganancia y diseñada para uso en interiores. Esta antena ofrece altas tasas de transmisión y recepción de datos para dispositivos inalámbricos de red LAN en la frecuencia ISM (Indrustrial, Scientific and Medical - Industrial, Científica y Médica). Es compatible

con el estándar 802.11g/b lo cual posibilita su compatibilidad con infinidad de dispositivos wireless como puntos de acceso y routers remotos. Esta antena puede sustituir la antena wireless de serie de su dispositivo aumentando de esta manera su radio de acción. La conexión a su dispositivo puede hacerse a través de un cable de extensión que se incluye con la antena o directamente.

Características:

- ✓ Antena omnidireccional de interiores
- ✓ Ganancia: 5dbi
- ✓ 2.4GHz IEEE 802.11b/g
- ✓ Ángulo de Cobertura H 360º- V 36º
- ✓ Opciones de instalación (escritorio, pared, soporte magnético o directamente a dispositivo) Compatible con antenas dotadas de conectores SMA.
- ✓ Cable de extensión incluido.

b) ANTENA INTERIOR DIRECCIONAL D-LINK ANT24-0600 6dBi

Figura 3.15 Antena interior direccional D-LINK ANT24-600 6dBi

La ANT24-0600 de D-link es una antena direccional amplificadora para uso en interiores y que le brindará mayor rango de cobertura inalámbrica para sus dispositivos wireless. Es compatible con el estándar 802.11g/b lo cual posibilita su compatibilidad con infinidad de dispositivos wireless como puntos de acceso y routers remotos. Esta antena puede sustituir la antena wireless de serie de su dispositivo aumentando de esta manera su radio de acción. La conexión a su dispositivo puede hacerse a través de un cable de extensión que se incluye con la antena o directamente. La ganancia de la antena es de 6dBi y ayuda a suministrar una mejor recepción de transmisión a una mayor distancia de cobertura de los dispositivos inalámbricos D-Link.

Características:

- ✓ Amplia el alcance de la señal inalámbrica
- ✓ Rango de Frecuencia: 2,4GHz - 2,5GHz
- ✓ Ganancia: 6dBi (sin pérdida por cable)
- ✓ Polarización. lineal, vertical
- ✓ Tipo de cable: Filotex 1,5M
- ✓ Mejora la cobertura direccional
- ✓ Funciona con dispositivos inalámbricos a 2,4 GHz con conectores RP-SMA o RP-TNC

c) ANTENA SECTORIAL PANEL 2.4 GHZ DE 14 dBi 90 GRADOS HORIZONTALMENTE POLARIZADO WIRELESS LAN MODELO : HG2414HSP-090

Figura 3.16 Antena sectorial panel 2.4 ghz 14dBi

Aplicaciones:

- ✓ Retransmite Internet sin línea telefónica (opera en todo tipo de clima).
- ✓ Comparta su señal de Internet , para reducir costos (empresas, cabinas, oficinas)
- ✓ Interconecte sucursales y oficinas de empresas públicas y privadas (Wireless LAN).
- ✓ Hot spot públicos inalámbricos
- ✓ Vigilancia y monitoreo (Wireless Video Systems)
- ✓ Proveer servicios de Internet inalámbrico (varios usuarios con una sola antena multipunto). Sistemas WiFi.
- ✓ Bluetooth

La antena sectorial de panel HyperGain HG2414HSP-090 WiFi horizontalmente polarizado combina una alta ganancia con una onda ancha de 90°. Su calidad profesional "cell site" está diseñada principalmente para proveedores de servicio en la banda ISM de 2.4 GHz. También se incluyen las aplicaciones para redes inalámbricas IEEE 802.11b y 802.11g, compatible con todas las marcas de AccessPoint (AP).

Debido a que esta antena está horizontalmente polarizada, es ideal para uso en áreas susceptibles a interferencia donde operan equipos Inalámbricos verticalmente polarizados. Con la reducción de esta interferencia se puede lograr una mejor recepción de la señal inalámbrica.

Durable a prueba de mal tiempo.- Esta antena WiFi ofrece una cobertura de plástico durable y fuerte para operar en todo tipo de clima.

El sistema de montaje permite instalaciones ajustables de 0 a 20 grados de inclinación. Ideal para proveedores de servicio inalámbrico. La cobertura Horizontal es total a 90 grados

3.3 PUNTOS DE ACCESO (ACCESS POINT AP)

El punto de acceso es un elemento que proporciona una "conexión" transparente a dispositivos inalámbricos que amplían su cobertura y su operabilidad dentro de una cobertura determinada. Actúa como un hub en comparación con las redes Ethernet.

Los AP tienen al menos dos interfaces de red: una para red inalámbrica y la otra interfaz para conectarse a las redes con cable, muchos de los puntos de acceso ofrecen la capacidad de utilizar antenas externas para ajustar el rango y el área de cobertura.

Cuando los AP admiten la itinerancia (roaming), puede que sea necesario promover sesiones y datos de usuario entre los puntos de acceso. En los dispositivos comerciales la opción más común es un método propietario de suministrador para mover datos de asociación de un AP a otro sin interrumpir la conectividad de la capa enlace. En un principio la administración a través de una interfaz de red TCP/IP era una característica estándar, en la actualidad una innovación que ha revolucionado es el desarrollo de soluciones de puntos de acceso que desplazan las funciones de administración desde los AP a los dispositivos de concentración central.

Los AP pueden ofrecer varios servicios para los clientes inalámbricos, uno de los más populares es DHCP, el cual asigna direcciones automáticas con la asociación asegurando así la consistencia entre los AP. Varios de los AP también pueden ejecutar una traducción de direcciones de red (NAT, Network Ardes Translation), especialmente los productos tipo “pasarela doméstica” que pueden conectarse a un módem y marcar un ISP (Internet Service Provider, Proveedor de Servicio de Internet).

En las redes inalámbricas la seguridad es un punto sensible para la administración y es así que se han implementado directivas de seguridad en los AP y no podía haber mejor posición ya que los AP son pasarelas para la red con cable. Adicionalmente la mayoría de productos implantan ahora una autenticación más sólida basada en el usuario. El acceso Wi-Fi protegido (WPA, Wi-Fi Protected) se puede ejecutar con una clave compartida previamente en la mayoría de los dispositivos domésticos y con un servidor de autenticación externo en redes más grandes.

3.3.1 PUNTOS DE ACCESO EXISTENTES EN EL MERCADO NACIONAL

Existen varias marcas y modelos de puntos de acceso en el mercado, que ofrecen diversas características y prestaciones cuyos precios varias de acuerdo a sus características y fabricantes.

A continuación se describen algunos puntos de acceso de las marcas más recocidas y sus características principales:

a) ACCESS POINT 3CRWE725075A

Figura 3.17 Punto de Acceso 3Com 3CRWE725075A

El punto de acceso 3Com 3CRWE725075A soluciona problemas de conexión inalámbrica bajo la certificación Wi-Fi 802.11a o 802.11 b/g con velocidades de hasta 108 Mbps

Soporta los siguientes modos de operación:

- ✓ Punto de acceso
- ✓ Puente punto a punto
- ✓ Puente punto a multipunto
- ✓ Cliente
- ✓ Repetidor

La ayuda de la técnica potencia sobre ethernet PoE por sus siglas en ingles (Power over Ethernet) supera problemas de instalación, eliminando la necesidad de un enchufe de corriente alterna en cada AP, suministrando energía sobre los cables UTP de categoría 5 o 6.

Soporta calidad de servicio QoS, que permite dar prioridad al tráfico sensible al retardo (Multimedia).

La interfaz del browser permite configurar y manejar APs de otros fabricantes con tecnologías 802.11/b/g.

b) DLINK ACCESS POINT WIRELESS 108MPBS 802.11g

Figura 3.18 Punto de Acceso Dlink 108Mpbs 802.11 g

Características:

- ✓ Hasta 108Mbps
- ✓ Autentificación WPA y 802.1x
- ✓ Software de administración del SNMP
- ✓ También trabaja como puente punto a punto, puente Punto a múltiples puntos, repetidor y cliente inalámbrico

En la tabla 3.7 se detalla las características técnicas de la antena sectorial panel 2.4 Ghz 14dBi

CARACTERÍSTICAS TECNICAS DLINK ACESS POINT WIRELESS 108MPBS 802.11g	
Estándares	IEEE 802.11g IEEE 802.11b IEEE 802.11 IEEE 802.3 IEEE 802.3u
Seguridad	• 64, 128, 152 WEP • 802.1X (EAP-MD5, EAP-TLS, EAP-TTLS y EAP-PEAP) • WPA - Acceso protegido Wi-Fi • Control de acceso de direcciones MAC (WPA-TKIP y WPA-AES)
Control de acceso al medio	• CSMA/CA con el ACK
Bandas de frecuencia	• 2.4GHz a 2.4835GHz
Rango de la señal	• Dentro: Hasta 328 pies (100 metros) • Al aire libre: Hasta 1312 pies (400 metros)
Modulación	• Multiplexación de división de frecuencia Ortogonal (OFDM) • Complementario del código (CCK) • DQPSK • DBPSK
Sensibilidad de Recepción	• 54Mbps OFDM, el 10% POR, - 66dBm) • 48Mbps OFDM, el 10% POR, - 71dBm • 36Mbps OFDM, el 10% POR, - 76dBm • 24Mbps OFDM, el 10% POR, - 80dBm • 18Mbps OFDM, el 10% POR, - 83dBm • 12Mbps OFDM, el 10% POR, - 85dBm • 11Mbps CCK, el 8% POR, - 83dBm • 2Mbps QPSK, el 8% POR, - 89dBm
Tipo de la antena externa	• dipolo 1.0dB con el conector SMA
Temperatura	• En funcionamiento: 32°F a 140°F (0°C a 40°C) • Almacenado: 4°F a 149°F (- 20°C a 65°C)
Humedad	• máximo del 95%
Entrada de energía	• Exteriores C.C. 5V, 2.0A de la fuente de alimentación
Dimensiones	• L = 5.6 pulgadas (142m m) • W = 4.3 pulgadas (109m m) • H = 1.2 pulgadas (31m m)
Peso	• 0.44 libras (200g)

Tabla 3.7 Características técnicas del punto de acceso DLINK 108Mbps 802.11g

c) LINKSYS WRT54G

Figura 3.19 Punto de Acceso Linksys WRT54G

Este equipo en realidad funciona como tres dispositivos en uno:

- ✓ Punto de acceso inalámbrico.
- ✓ Conmutador 10/100 de 4 puertos duplex
- ✓ Ruteador con conexión a Internet DSL

Este dispositivo funciona correctamente con otros dispositivos y tecnologías inlámbricas, gracias uso de un solo canal de 2,4 Ghz como especifica el estandar inalambrico oficial.

Posee dos antenas desmontables q pueden operar en conjunto o individualmente.

Para proteger datos y privacidad este equipo implementa una encriptacion de 128 bits, dispone de un firewall que le permite proteger los PC’s de ataques desde internet

También puede funcionar como servidor DHCP

3.4 AMPLIFICADORES DE RADIO FRECUENCIA, CABLES Y CONECTORES.

Entre tanto que las antenas consiguen ganancia pasiva enfocando la energía, los amplificadores consiguen ganancia activa inyectando potencia continua (DC) externa en el cable de radiofrecuencia. A esta potencia se la denomina “tensión fantasma” y la lleva el cable RF desde un inyector de corriente a un amplificador. Existen dos tipos de amplificadores siendo los siguientes:

- ✓ Unidireccionales (solo aumentan la potencia de transmisión)
- ✓ Bidireccionales (además incrementan la sensibilidad en la recepción).

Lo que tienen en común los dos tipos de amplificadores es que se pueden encontrar como dispositivos de ganancia fija o variable. Los amplificadores de ganancia fija de potencia son los más apropiados para el diseño de una red, esto debido a su estabilidad global. Los amplificadores son utilizados regularmente para compensar las pérdidas debidas a una excedente longitud del cable ubicado entre la antena y el dispositivo inalámbrico.

Una de las principales fuentes de pérdidas en las redes inalámbricas se ven centradas en los cables de radiofrecuencia. Para evitar estos inconvenientes hay que implementar cables con el menor nivel de atenuación posible (especificando con dB de pérdidas por cada 100 metros a una frecuencia determinada), en lo posible hay que conseguir cables con conectores integrados, existe la posibilidad de instalar los conectores por sí mismo, pero el resultado final no va a ser el esperado ni confiable por los estándares industriales.

Se debe tener en cuenta que el cable debería tener la misma impedancia (50 ohmios) que el resto de sus componentes inalámbricos y escoger los conectores de cable que se correspondan con los dispositivos y antenas que ya tengamos. Es posible conectar cualquier cosa con los conectores de pinza o rosca apropiados,

pero un conector de este tipo podría añadir una pérdida de 2 a 3 dB, con lo que reduciríamos a la mitad su potencia de transmisión y su sensibilidad de recepción.

Se debe recordar que aunque el cableado y los conectores no son directamente importantes para la seguridad inalámbrica, resulta esencial una señal fuerte, clara y una buena sensibilidad de recepción.

CAPÍTULO IV

SISTEMAS DE CONTROL DE ACCESO

4.1 INTRODUCCIÓN

Las empresas requieren buscar constantemente métodos más seguros y eficientes para controlar el acceso de su personal a diferentes sectores de su empresa; por esto, se considera extremadamente útil que una organización opere con un sistema que se encargue del control automático de acceso.

Un sistema de control de accesos debe permitir el ingreso de un determinado grupo de personas a un determinado lugar dentro de un horario preestablecido.

Anteriormente el control de acceso se realizaba con medios mecánicos como llaves, cerrojos, etc., pero en la actualidad estos sistemas vienen siendo sustituidos por sistemas más modernos basados en dispositivos electrónicos.

4.2 TECNOLOGÍAS DE AUTOIDENTIFICACIÓN APLICADAS AL CONTROL DE ACCESO

Dentro del ámbito de la tecnología de identificación aplicada al control de acceso se pueden encontrar diversas tecnologías como: sistemas biométricos, tarjetas magnéticas, códigos de barra y RFID[26]. A continuación se explica las tecnologías más utilizadas.

4.2.1 CÓDIGOS DE BARRAS

Prácticamente obsoletos (se utilizan marginalmente para controlar accesos masivos a estadios y pabellones deportivos). Tiene la ventaja de que las

[26] RFID: (Radio Frecurncy Identication) tecnología de auto identificación que usa frecuencias de radio

acreditaciones son fáciles de generar pero es un sistema muy vulnerable a falsificaciones.

Figura 4.1 Credencial con código de barras

4.2.2 BANDA MAGNÉTICA

El más extendido e instalado hasta hace un par de años. Las credenciales son muy económicas, pero son más complejas de emitir (se requiere impresora y/o codificadora de carnets). Tiene un nivel de seguridad medio aunque son vulnerables a la desmagnetización y el desgaste de uso. Los lectores requieren un mantenimiento continuo (limpieza de cabezales y rodillos de tracción).

Figura 4.2 Credencial con barra magnética

4.2.3 PROXIMIDAD, RADIO FRECUENCIA O RFID

Esta tecnología RFID es la más utilizada actualmente para el intercambio de información en forma inalámbrica, dicha información está escrita en un chip de radio frecuencia (Tag o Transponder) que posee una antena que permite identificar la tarjeta en el momento que se aproxima al lector o encoder. Al igual que las tarjetas de banda magnética, las tarjetas de proximidad requieren una impresora para su personalización y un lector para codificarlas. El nivel de seguridad es alto (las tarjetas normales solo son de lectura por lo que no se puede alterar la información que contienen) y son muy resistentes a la erosión física y química. No requieren mantenimiento ya que es un sistema completamente electrónico sin piezas mecánicas que sufran desgaste. Una de las ventajas que ofrece es que el usuario no tiene porqué sacar la tarjeta de cartera/bolso/mochila para pasar por el control de acceso, con lo que el tiempo medio por acceso es de poco más de 1 segundo.

Figura 4.3 Tarjetas y lectores de proximidad

4.2.4 BIOMÉTRICOS

En el sistema biométrico de mano el usuario tiene que digitar su código en el teclado del lector (identificación) y seguidamente posicionar su mano dentro del lector (autentificación). El nivel de seguridad es alto, aunque el lector requiere un cierto mantenimiento y reparaciones (pese a ser un sistema completamente

electrónico, no es tan robusto como los lectores de proximidad). La principal ventaja que ofrece es la ‘autentificación’, que nos asegura que no se produzcan accesos fraudulentos, pero el inconveniente es que el tiempo medio por acceso es de unos seis segundos y que requiere de capacitación al usuario.

El sistema biométrico de huella tiene características similares al sistema biométrico de mano con la diferencia en su tiempo de acceso que es de 2 segundos y no requiere previamente identificarse con un código o ping.

Figura 4.4 Lectores biométricos de huella

4.3 COMPONENTES Y FUNCIONAMIENTO DE UN SISTEMA DE CONTROL DE ACCESO

Todo sistema de control de acceso requiere de los siguientes componentes:

a) Sistema de autoidentificación (Código de barras, bandas magnéticas, RFID y biométricas). Son sistemas electrónicos de autenticación, que permiten la comprobación de identidad de una persona como mecanismo de seguridad de acceso.

b) Actuadores (Cerradura de puertas). Son contactos magnéticos antisabotaje y se conectan al panel de control, estos dispositivos se encargan de mantener cerrada o abierta las puertas que se requieren controlar

Figura 4.5 Cerraduras magnéticas para puertas

c) Panel de control (controlador). Es el punto central de comunicaciones para el sistema de control de acceso. El panel de control típicamente suple energía y establece interfaces con múltiples lectores en diferentes sitios de acceso. El panel o controlador está conectado con la cerradura electromagnética de la puerta de acceso necesario para físicamente abrir la puerta. El panel puede estar conectado a diferentes alarmas (por ejemplo, sirenas, digitalizadores automáticos, luces). Y finalmente, el panel de control generalmente está conectado a un servidor de control de acceso.

   El controlador o panel de control almacena información sobre los formatos de datos. Esa información identifica que porción del flujo de datos recibidos de una tarjeta es usada para tomar decisiones de control de acceso.

d) Servidor de control de acceso, Software y Base de Datos. Manejo de la información sobre los derechos de acceso de los usuarios.

   En un sistema centralizado, el servidor de control de acceso recibe los datos de la tarjeta del panel de control. El Software correlaciona los datos de la tarjeta con los datos en la base de datos, determina los privilegios de acceso de la persona, e indica si la persona puede o no ser admitida.

   En un sistema descentralizado, el servidor de control de acceso periódicamente envía información de control de acceso actualizada a los paneles de control y les permite operar independientemente, tomando la

decisión de autorización para las credenciales presentadas basadas en los datos almacenados en el panel.

La figura 4.6 ilustra cómo estos componentes básicos están interconectados

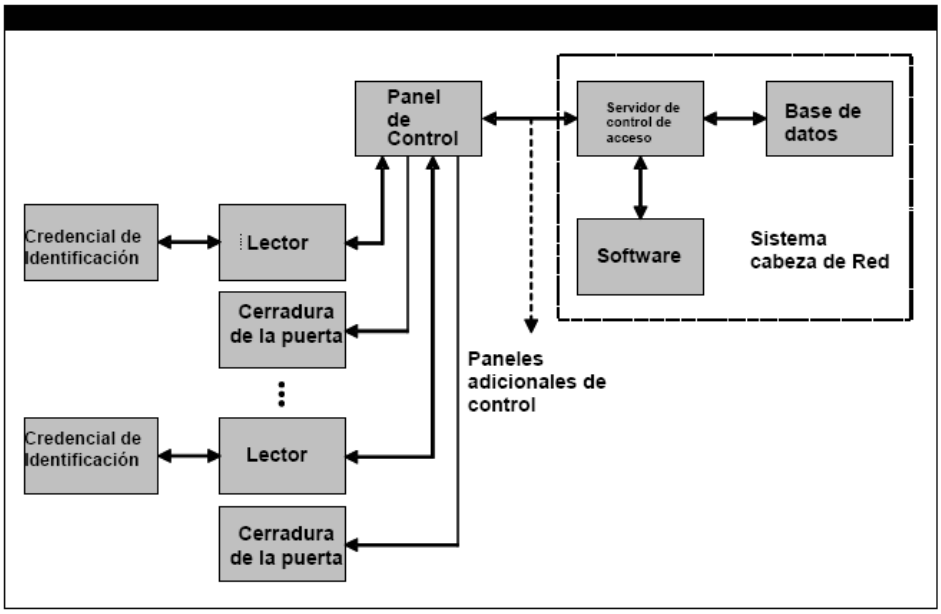


Figura. 4.6 Esquema de un Sistema de Control de Acceso

Los procesos de control de acceso empiezan cuando un usuario activa el sistema de auto identificación; este proceso se valida en el panel de control el cual acepta o no los datos transmitidos por el sistema de auto identificación. Lo que ocurre luego depende si el sistema es centralizado o distribuido.

En un sistema centralizado, el panel de control transmite los datos al servidor de control de acceso. El servidor de control de acceso compara los datos recibidos de la tarjeta con la información sobre el usuario que está almacenado en la base de datos. El programa de control de acceso determina los privilegios de acceso del usuario y su autorización, la hora, la fecha y la puerta a la que se va a ingresar y cualquier otra información que la compañía pueda requerir para mejorar su seguridad. Cuando se autoriza el acceso, el servidor de control de acceso envía una señal al panel de control para abrir una puerta

En un sistema distribuido, el panel de control permite o niega la entrada. El servidor de control de acceso periódicamente provee datos al panel de control, que habilita al software del panel de control a determinar si el usuario está autorizado o no para tener acceso.

4.4 DISEÑO DEL SISTEMA DE CONTROL DE ACCESO

Dentro del diseño del sistema de control de acceso se realizarán dos selecciones:

- ✓ Selección de la tecnología para el sistema de auto identificación.
- ✓ Selección de la tarjeta controladora.

4.4.1 SELECCIÓN DE LA TECNOLOGÍA PARA EL SISTEMA DE AUTOIDENTIFICACIÓN (LECTOR-TARJETA)

Para la selección del tipo de tecnología a utilizar en lo que respecta a la autoidentificación se tomará en cuenta las características de cada una de las siguientes tecnologías expuestas anteriormente, como se detalla en la tabla 4.1

CARÁCTERÍSTICAS	COD. BARRAS	BANDA MAGNETICA	RFID	BIOMETRICA
Tecnología fiable y versátil de Identificación Automática que permite identificar, seguir y gestionar diversos tipos de objetos.	NO	NO	SI	SI
Requiere contacto para operar	SI	SI	NO	SI
Línea de visión directa con el objeto para operar	SI	SI	SI	SI
Mejora la eficiencia de los procesos y la productividad	NO	NO	SI	SI
Incrementa la rentabilidad	NO	NO	SI	NO
Nivel de seguridad alto	NO	NO	SI	SI
Bajos costos de implementación	SI	SI	SI	NO
Mejora la información a la gestión y a los clientes	NO	NO	SI	SI
Ciclo de vida	Corto	Mediano	Indefinido	Indefinido

Tabla 4.1 Características de las tecnologías del sistema de control de acceso

Tomando en cuenta las características descritas anteriormente que ofrecen las diferentes tecnologías para la auto identificación se ha decido utilizar la tecnología RFID, porque a diferencia de las otras tecnologías cumple con la mayor cantidad de especificaciones técnicas que se requieren para mejorar el control de acceso a las instalaciones de Xerox, ofreciendo múltiples posibilidades para mejorar la gestión de sus recursos y automatizar procesos, así como un importante ahorro de costos.

4.4.1.1 SELECCIÓN DE EQUIPOS PARA EL SISTEMA DE AUTOIDENTIFICACIÓN (LECTOR-TARJETA).

En la tabla 4.2 se realiza una comparación de las características técnicas de algunos lectores RFID existentes en el mercado

CARÁCTERÍSTICAS	ZEBRA ZL50	HID MAXIPRO	KIMALDI RD125K
Rango de lectura	8 a 10 cm	6 a 9 cm	5 a 7 cm
Interface configurable	Serial RS-232 Wiegand	Serial RS-232 Wiegand	Serial RS-232 y serial TTL
Dimensiones	5.1x9.3x1.9 cm	12.7x12.7x2.54cm	4.9x4.9x2.0cm
Frecuencia de portadora	125 Khz	125 Khz	125 Khz
Antena incorporada	Si	Si	Si
Consumo de voltaje	12VDC	12-24 VDC	5VDC
Lectura de formato EM	Si	Si	Si
Material	Policarbonato	Policarbonato	Policarbonato
Distancia de cable	100	100	100
Consumo de Energía	150mA	200mA	130mA
Dificultad de instalación y operación	Fácil	Media	Media
Transponder	Solo lectura	Solo lectura	Solo lectura
Precio	Medio	Alto	Medio
Cumple requerimientos del sistema	Si	No	Si

Tabla 4.2 Características técnicas de los lectores RFID existentes en el mercado

4.4.1.2 JUSTIFICACIÓN DE LA SELECCIÓN DEL SISTEMA DE AUTOIDENTIFICACIÓN RFID.

En base a las características técnicas expuestas en la tabla 4.2 se observan que el lector Zebra ZL50 tiene mejores características que los otros dos lectores (HID MAXIPRO, Kimaldi RD125K), necesarias para el diseño del sistema de control de accesos, tales como el rango de lectura permitiendo mayor distancia entre la tarjeta y el lector en el momento en que interactúan (8 a 10 cm), fácil instalación, operación y precios medios en comparación a los otros dos equipos, por todas estas razones se escogió el lector Zebra ZL50 para el sistema de autoidentificación RFID dentro del sistema de control.

Una vez escogido el lector de proximidad se procede a la elección de la tarjeta de proximidad que como único requisito técnico es que trabaje en la frecuencia de 125 KHz, en el mercado existe una variedad de tarjetas que cumplen con este requisito, tal es el caso de la tarjeta de proximidad Kimaldi EMH4120, la cual fue seleccionada.

4.4.2 SELECCIÓN DE LA TARJETA CONTROLADORA

La tabla 4.3 describe las características técnicas de dos tarjetas controladoras existente en el mercado: la tarjeta controladora Zebra ZC500 y tarjeta controladora Kimaldi NdcanMax.

CARÁCTERÍSTICAS	ZEBRA ZC500	KIMALDI NDCANMAX
Puerto de comunicaciones	RS-232 para conexión directa RS-485 para conexión de red	RS-232 RS-485
Salida para puertas	2	2
Entrada para lectores de proximidad	2	2
Entradas para sensores de puerta abierta	2	0
Entradas de pulsador	2	0
Entradas de señal de pánico	1	1
Salida de señal de alarma	1	1
Salida para display	1	1
Dimensiones (cm)	13,7 x 14.3	11.8 X 10.5
Consumo	500 Ma	200 Ma
Alimentación	12 VDC – 15 VDC	5 VDC
Compatibilidad con el lector Zebra ZL50	Certificada por Zebra	No

Tabla 4.3 Características técnicas de las tarjetas controladoras existente en el mercado

4.4.2.1 JUSTIFICACIÓN DE LA SELECCIÓN DE LA TARJETA CONTROLADORA.

De acuerdo a la tabla 4.3 se observa que tanto las características técnicas de la tarjeta controladora Zebra ZC500 Y KIMALDI NDCANMAX son bastante similares; pero lo que les hace diferentes es la compatibilidad que existe entre la tarjeta Zebra ZC500 y el lector RFID Zebra ZL50 seleccionado en el ítem 4.4.1.2 lo que evitaría posibles problemas con la transmisión de la información dentro del sistema de control por este motivo se escogió la tarjeta controladora Zebra ZC500.

4.4.3 DISPOSITIVO PARA EL ACOPLAMIENTO DEL SISTEMA DE CONTROL DE ACCESO A LA RED INALÁMBRICA.

Para que el sistema de control de acceso se acople a la red inalámbrica se utilizará el dispositivo conversor EZL-300W Lite.

Figura 4.7 Conversor serie a Wireless EZL-300W Lite

El EZL-300W Lite permite conectar cualquier dispositivo serie a una red de área local inalámbricamente, siendo solamente necesario la configuración de parámetros básicos. Una vez conectados, la conversión serie a Wireless (estándar IEEE 802.11b) se realiza transparentemente, es decir, el dispositivo serie actúa exactamente igual que un cable serie estándar conectado directamente.

El conversor EZL-300W Lite hace posible conectar un dispositivo serie a la red inalámbrica y comunicarse con cualquier punto de la red.

4.4.4 DISEÑOS PROPUESTOS PARA EL SISTEMA DE CONTROL DE ACCESO.

Para el control de accesos en el Edificio Xerox se propone los siguientes dos diseños:

PRIMER DISEÑO

Para el primer diseño del sistema de control de acceso se utilizarán los siguientes equipos:

- ✓ Panel de control Zebra ZC500 (3 unidades)
- ✓ Lector de proximidad Zebra ZL50 (5 unidades)
- ✓ Conversor serie a wireless EZL-300W Lite (5 unidades)
- ✓ Cerraduras magnéticas para puertas (5 unidades)
- ✓ Cable UTP 5a (70m Aprox)
- ✓ Conversor RS232 a RS485 (1unidad)

Lo particular del primer diseño es que por cada lector de proximidad se utilizara un conversor serie a wireless (EZL-300W Lite), además de que los paneles de control se encuentran comunicados entre sí con cable (UTP 5a) utilizando al interfaz RS-485 lo que implica el uso de un conversor RS-232 a RS-485 para la conexión a la red de Xerox. En la figura 4.8 se visualiza a detalle este diseño.

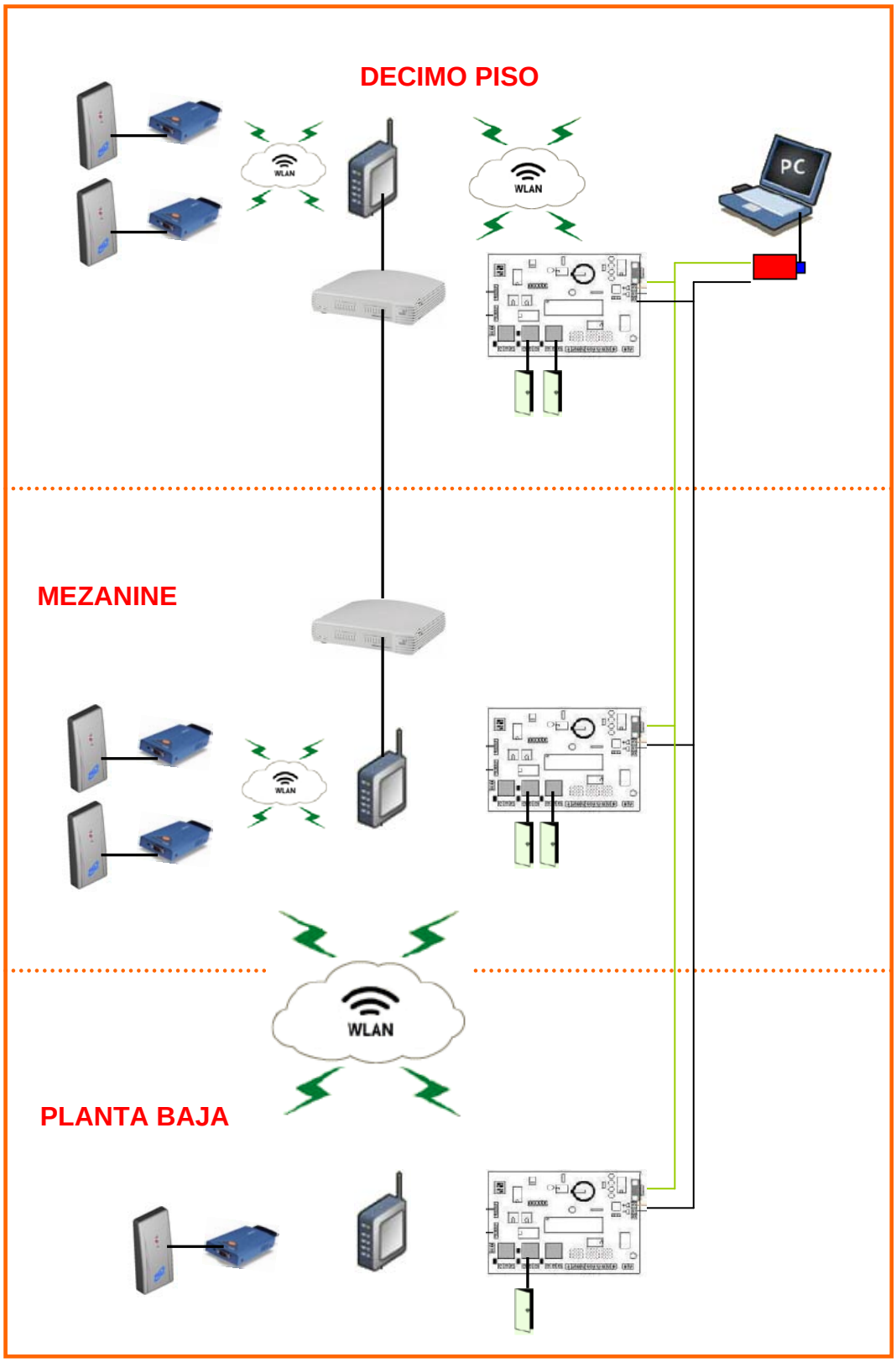


Figura. 4.8 Primer Diseño Propuesto

SEGUNDO DISEÑO

Para el segundo diseño del sistema de control de acceso se utilizarán los siguientes equipos:

- ✓ Panel de control Zebra ZC500 (3 unidades)
- ✓ Lector de proximidad Zebra ZL50 (5 unidades)
- ✓ Conversor serie a wireless EZL-300W Lite (3 unidades)
- ✓ Cerraduras magnéticas para puertas (5 unidades)
- ✓ Cable UTP 5a (30 m Aprox)

Con respecto al segundo diseño propuesto se destaca que solo se utilizará un conversor serie a wireless (EZL-300W Lite) por cada panel de control, la distribución por pisos de los equipos para el segundo diseño propuesto se lo puede observar en la figura 4.9

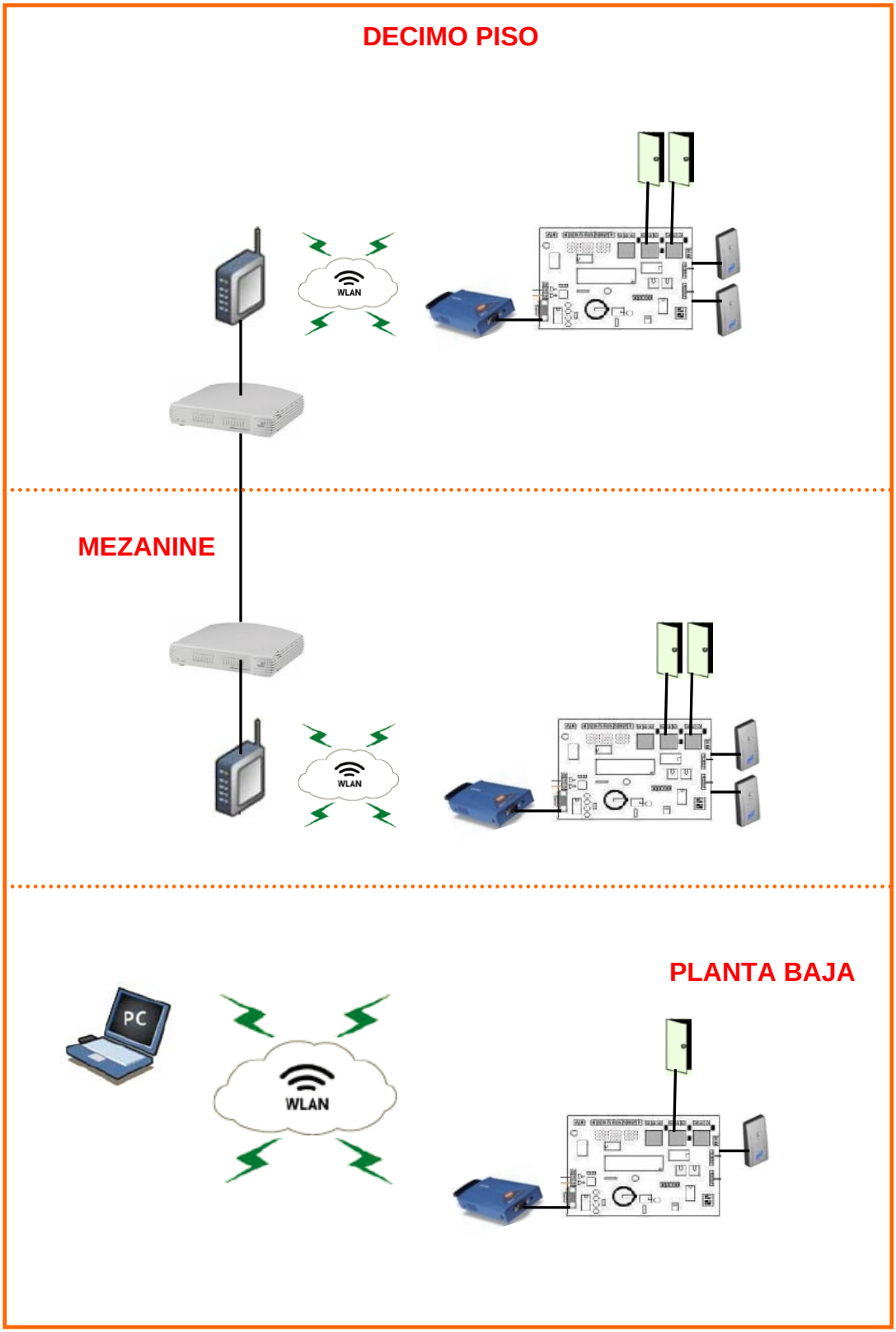


Figura. 4.9 Segundo Diseño Propuesto

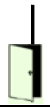
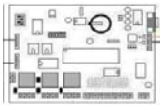
 LECTOR DE PROXIMIDAD	 PUNTO DE ACCESO
 CERRADURAS PUERTAS	 CONVERSOR SERIE A WIRELESS
 PANEL DE CONTROL	 SERVIDOR CONTROL ACCESO
 RED LAN INALAMBRICA	 SWITCH
 CONVERSOR RS232 a RS485	

Figura. 4.10 Cuadro de equipos para diseños propuestos

4.4.4.1 JUSTIFICACIÓN DE LA SELECCIÓN DEL DISEÑO PROPUESTO

Los dos diseños de sistemas de control de acceso propuestos satisfacen la necesidad de Xerox en cuanto al control del ingreso de personas a sus instalaciones y además brindan la posibilidad de acoplamiento a la red inalámbrica, que es parte del objetivo de este proyecto; pero con la diferencia de que el segundo diseño propuesto es distribuido lo que agilita el proceso de manejo de la información dentro del sistema de control de acceso, debido a que las tarjetas controladoras se encargan de ejecutar directamente la petición realizada por el lector, lo que no ocurre con el primer diseño que al ser centralizado la información primero es validada en la base de datos del servidor para luego ser ejecutada teniendo un tiempo de respuesta mayor en comparación al del segundo diseño.

Por otro lado el segundo diseño al utilizar menor cantidad de conversores (EZL-300W Lite) en su estructura y menor cantidad de cableado reduce los costos de implementación.

Por todas las razones anteriormente expuestas se determino que el segundo diseño es el apropiado para el sistema de control de acceso.

4.4.5 CONFIGURACIÓN DEL PANEL DE CONTROL DE ACCESO ZEBRA ZC500

Para configurar el panel de control de acceso Zebra ZC500 se siguen los siguientes pasos:

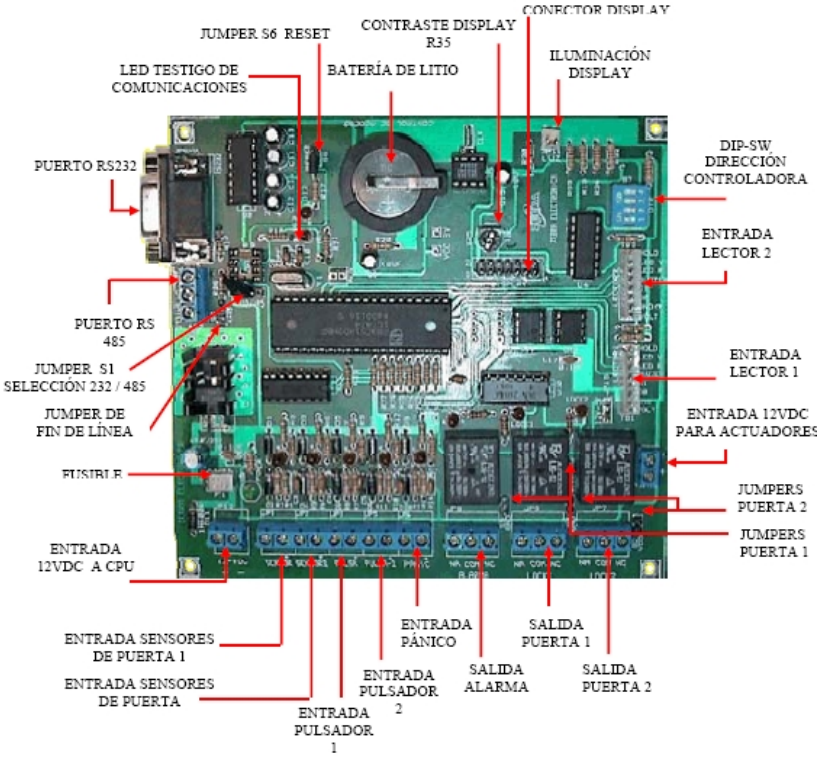


Figura 4.11 Panel de control Zebra ZC500

a) Proceso de Reset

El primer paso antes de iniciar el sistema es realizar el proceso de reset; este proceso se realiza de la siguiente manera:

- ✓ Quitar el voltaje de alimentación de la controladora. Debe tener conectada al menos una lectora.

- ✓ Colocar el jumper S6 de RESET.

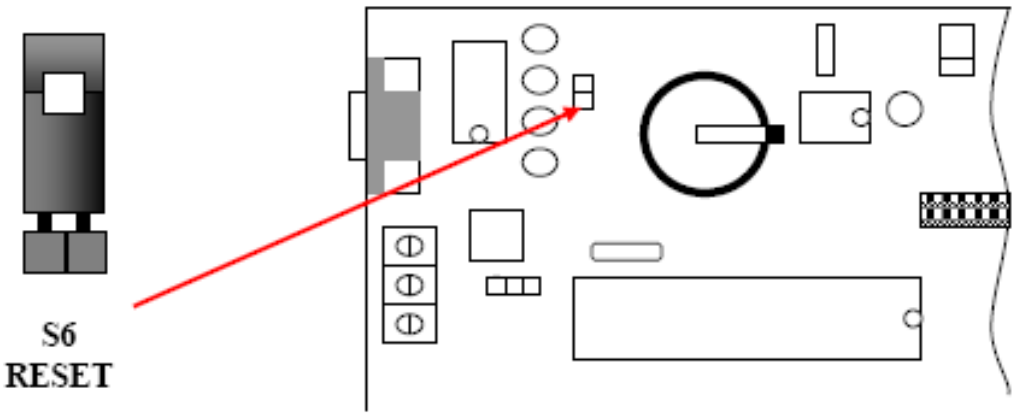


Figura 4.12 Jumper S6 de Reset

- ✓ Alimentar la controladora con los 12VDC y esperar mínimo 2 segundos.
- ✓ Quitar el jumper S6 de RESET y esperar 40 segundos. Si posee display aparece el mensaje BORRANDO EVENTOS. Al finalizar la lectora emitirá un pito confirmando la finalización del proceso.
- ✓ Después de terminado el proceso de reset, la controladora queda lista para configurarla, este proceso elimina los usuarios, grupos, horarios, eventos y configuración. La controladora quedará en operación normal.
- ✓ Retire el jumper S6 Reset después de usarlo.

b) Asignación de Dirección

Cada controladora posee un Dip-Sw S7 de dirección; en la red no pueden existir 2 o más controladoras con igual dirección.

La figura 4.13 muestra la asignación de direcciones para cada controladora que se requiere en el diseño seleccionado:

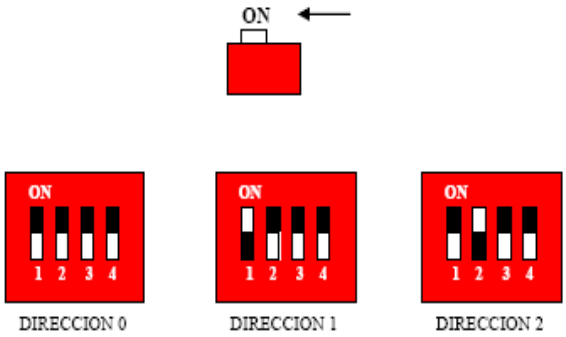


Figura 4.13 Direcciones asignadas a las controladoras

c) Selección del tipo de comunicación

Como se muestra en la figura 4.14 en este diseño se usa el puerto de comunicación RS232 de la tarjeta controladora ZC500 conectado al puerto serie (RS232) del conversor RS232 a WI-FI, el cual se encarga de mantener la comunicación entre el sistema de control y la red inalámbrica

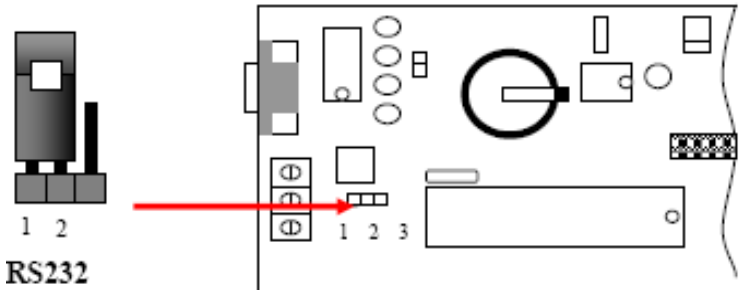


Figura 4.14 Selección de tipo de comunicación

Para más detalles sobre la configuración de la tarjeta controladora Zebra ZC500, revisar el anexo 1.

4.4.6 SOFTWARE DE CONTROL DE ACCESO ZEBRA ZC500 V1.0

El software permite llevar el registro de entrada y salida de personas a las instalaciones de un lugar (empresa, conjunto residencial, etc.). Este software puede operar en conjunto con el sistema de control de acceso ZC500, tal que no solo se lleve el registro de ingreso de los visitantes, sino que también se puede restringir el acceso de los mismos a ciertas áreas del lugar.

- ✓ Administración integrada de empleados y visitantes.
- ✓ Operación en red empleando un esquema cliente-servidor.
- ✓ Reportes de eventos.
- ✓ Perfiles configurables de operador.
- ✓ Autorización en tiempo real.
- ✓ Asignación de tarjeta de proximidad.
- ✓ Requiere PC dedicado.

4.4.6.1 CONFIGURACIÓN DEL SOFTWARE.

- ✓ Instalar el motor de la base de datos INTERBASE software.
- ✓ Instalar el control de acceso Zebra ZC500 ejecutando SETUP.EXE que está ubicado en la carpeta ZC500.
- ✓ Ejecutar ZebraCA.exe.

Cuando se ejecuta por primera vez el software de Control de Acceso aparece una pantalla de identificación donde se debe ingresar nombre de usuario y contraseña, el nombre inicial es “ZEBRA” y la contraseña es “zebra”; estos parámetros pueden ser cambiados por el usuario, como se muestra en la figura 4.15.

Figura 4.15 Pantalla de inicio del software ZC500

Cuando se ingresa al sistema aparece una pantalla donde se despliegan las utilidades y configuración del mismo, tal como se muestra en la figura 4.16

Figura 4.16 Pantalla de inicio del software ZC500

Dentro de los que es la configuración los parámetros a establecerse son:

- ✓ Puerto serial de comunicación con la controladora (COM1).
- ✓ Perfil del administrador del sistema.
- ✓ Usuarios del sistema.
    - o Registro de tarjetas de usuarios
    - o Registro de grupo de usuarios
    - o Reporte de usuarios
- ✓ Horarios.
- ✓ Días festivos.
- ✓ Grupos de acceso.

- ✓ Controladores (detección de hardware instalado).
- ✓ Operar controladores y puertas.
- ✓ Visor de eventos.

Para más detalles sobre el software Zebra ZC500, referente a su instalación, configuración y operación revisar el anexo 2.

4.4.7 CONFIGURACIÓN DEL CONVERSOR SERIE A WIRELESS EZL-300W LITE

Los parámetros de configuración del conversor EZL-300 Lite son los siguientes:

a) Modo de funcionamiento

El dispositivo EZL-300W Lite soporta distintos modos de funcionamiento siendo el modo T2S (TCP to Serial) el que se empleara para el acoplamiento del sistema de control a la red inalámbrica.

El conversor EZL-300W Lite cuando trabaja en el modo T2S, es decir cuando recibe una conexión TCP desde un host remoto, la acepta, y se establece una conexión; una vez establecida, los datos entrantes por el puerto serie son transmitidos al host remoto, y los provenientes del host remoto son transferidos al puerto serie.

La comunicación entre el conversor y el host remoto se lleva a cabo a través de sockets, que consiste en la combinación de una dirección IP y puerto TCP/UDP, con otra dirección IP y puerto. Por lo tanto, para el establecimiento de una conexión, se debe especificar un puerto de enlace en el conversor.

b) Características del puerto serie

Para una adecuada comunicación serie, entre la tarjeta controladora ZC500 y el conversor EZL-300W Lite, se debe configurar el mismo sistema de comunicación serie en los dos dispositivos, especificando los siguientes parámetros:

- ✓ Velocidad en baudios (Baudrate).
- ✓ Paridad (Parity).
- ✓ Número de bits de datos (Data Bits).
- ✓ Bits de parada (Stop Bit).
- ✓ Control de flujo (Flow Control).

Por defecto, la tarjeta controladora ZC500 está preparada para comunicar a 19200, N,8,1; es decir, a 19200 baudios, ningún bit de paridad, ocho bits de datos , y un bit de parada. Por consiguiente, las características del puerto serie del conversor han de coincidir.

c) Configuración WLAN

El conversor EZL-300W Lite puede trabajar en modo ad-hoc y modo infraestructura pero para el diseño seleccionado del sistema de control se maneja en el modo infraestructura.

En el modo infraestructura los conversores se comunican con un AP (Access Point - Punto de acceso). Este punto de acceso actúa como un puente y reenvía las comunicaciones a la red inalámbrica, como se ilustra en la figura 4.17

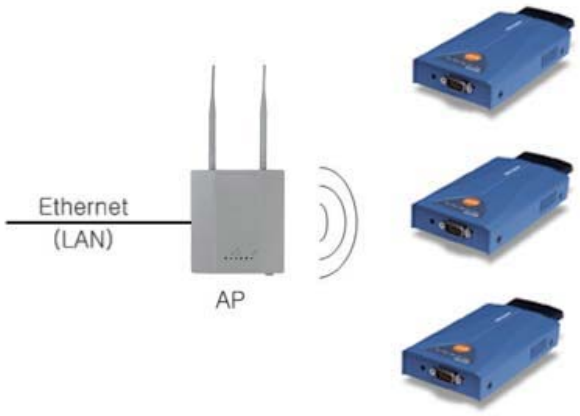


Figura 4.17 Modo infraestructura del conversor EZL-300W Lite

Una vez montada y configurada la red inalámbrica, se especifican en los conversores los siguientes parámetros:

- ✓ Nombre de la red (SSID).
- ✓ Canal de radio (Channel).
- ✓ Sistema de cifrado (los equipos EZL-300W Lite sólo soportan el sistema de cifrado WEP – Wired Equivalent Privacy).
- ✓ Finalmente, se asigna una dirección de red (dirección IP y máscara de subred), y una puerta de enlace o gateway.

La figura 4.18 muestra la configuración de un conversor, tomando en cuenta los parámetros establecidos por defecto en la tarjeta controladora (19200, N,8,1), con respecto al direccionamiento IP será asignado en el capítulo siguiente.

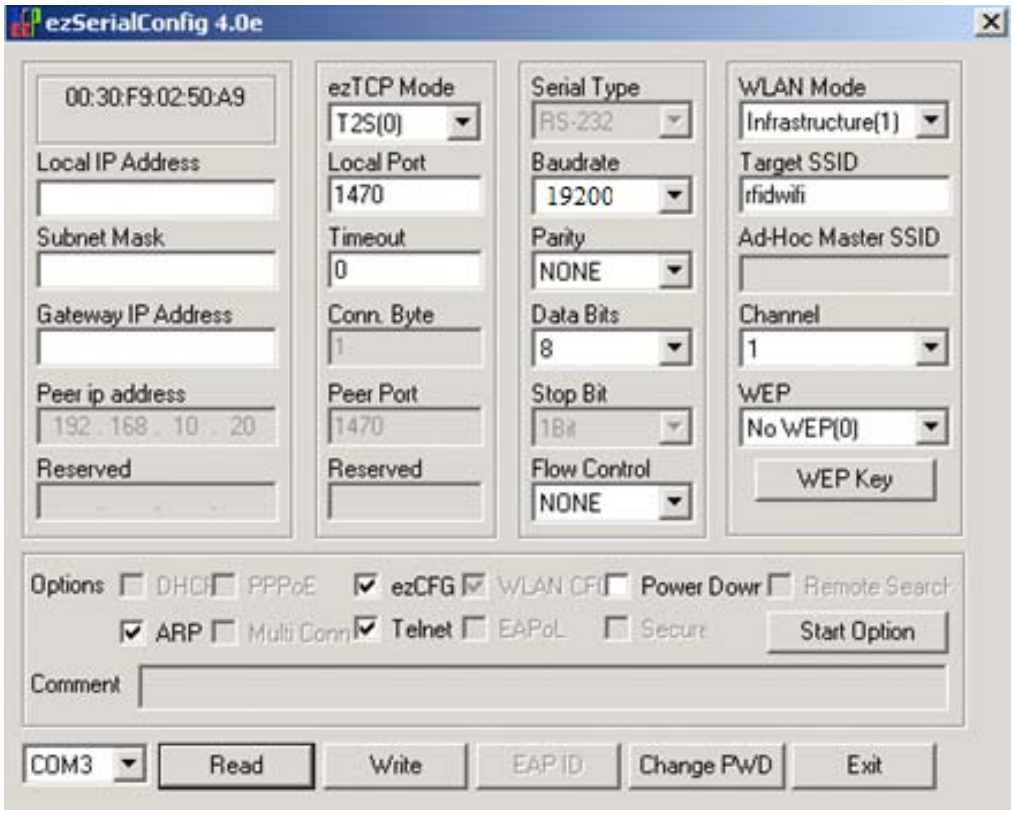


Figura 4.18 Configuración del conversor EZL-300W Lite

En el anexo 3, se detalla con mayor profundidad los pasos a seguir en la configuración del dispositivo EZL-300W Lite.

4.4.8 UBICACIÓN DE LOS EQUIPOS DEL SISTEMA DE CONTROL DE ACCESO EN EL EDIFICIO XEROX

En los siguientes gráficos se muestran las ubicaciones físicas de los diferentes equipos necesarios para el funcionamiento del sistema de control de acceso, en los diferentes pisos del edificio matriz Xerox:

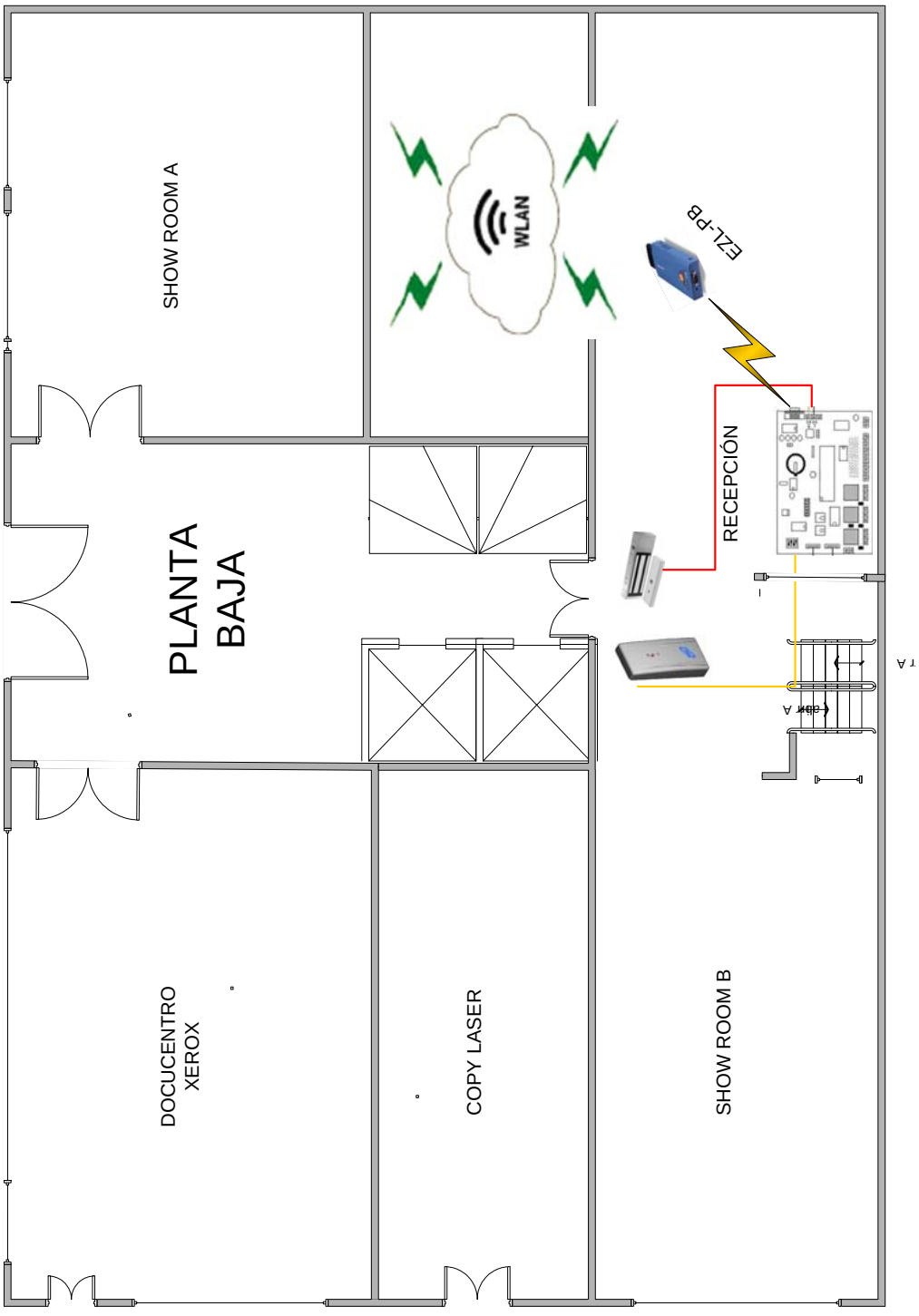


Figura 4.19 Ubicación de los equipos del sistema de control de acceso en la planta baja.

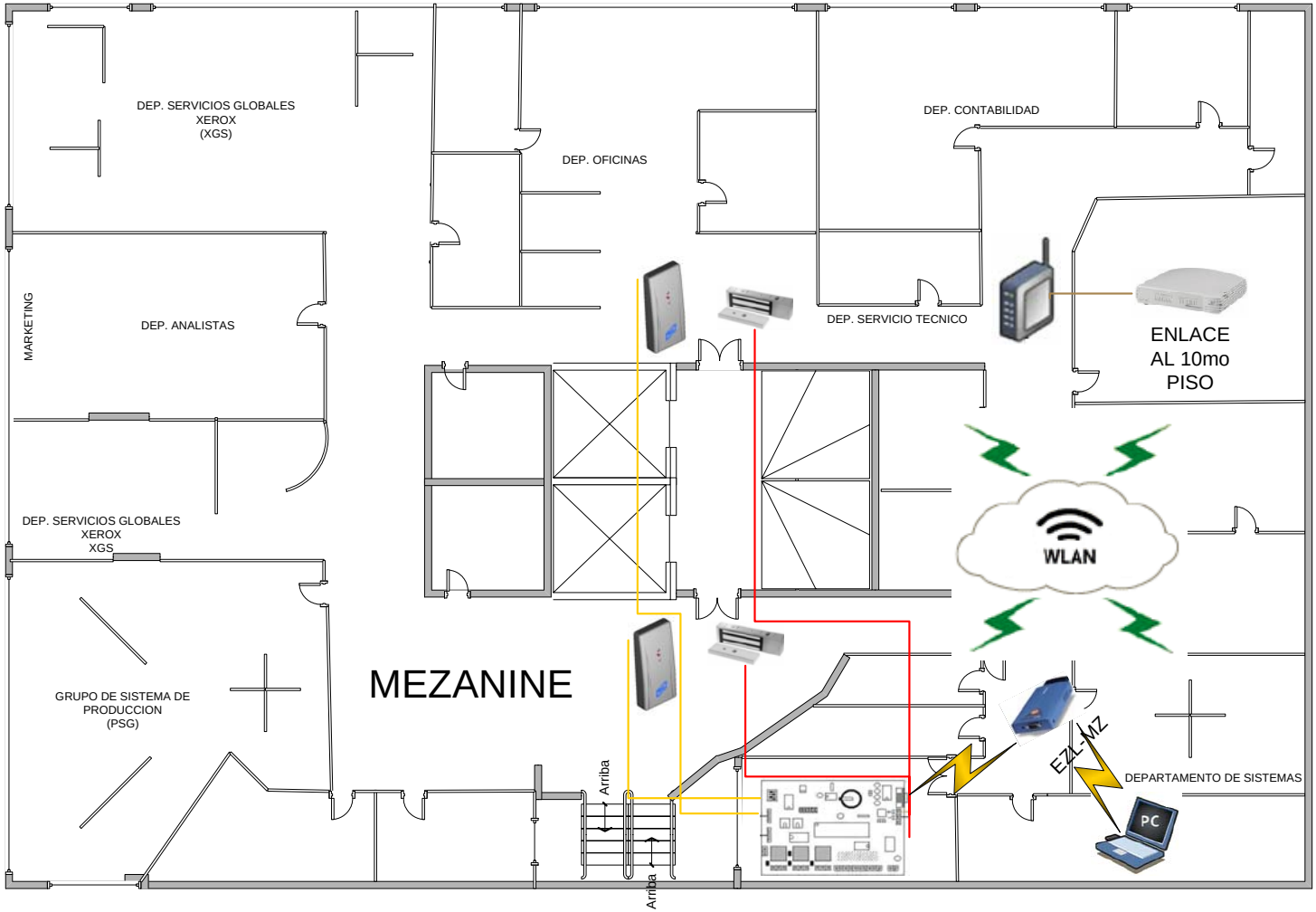


Figura 4.20 Ubicación de los equipos del sistema de control de acceso en el mezanine.

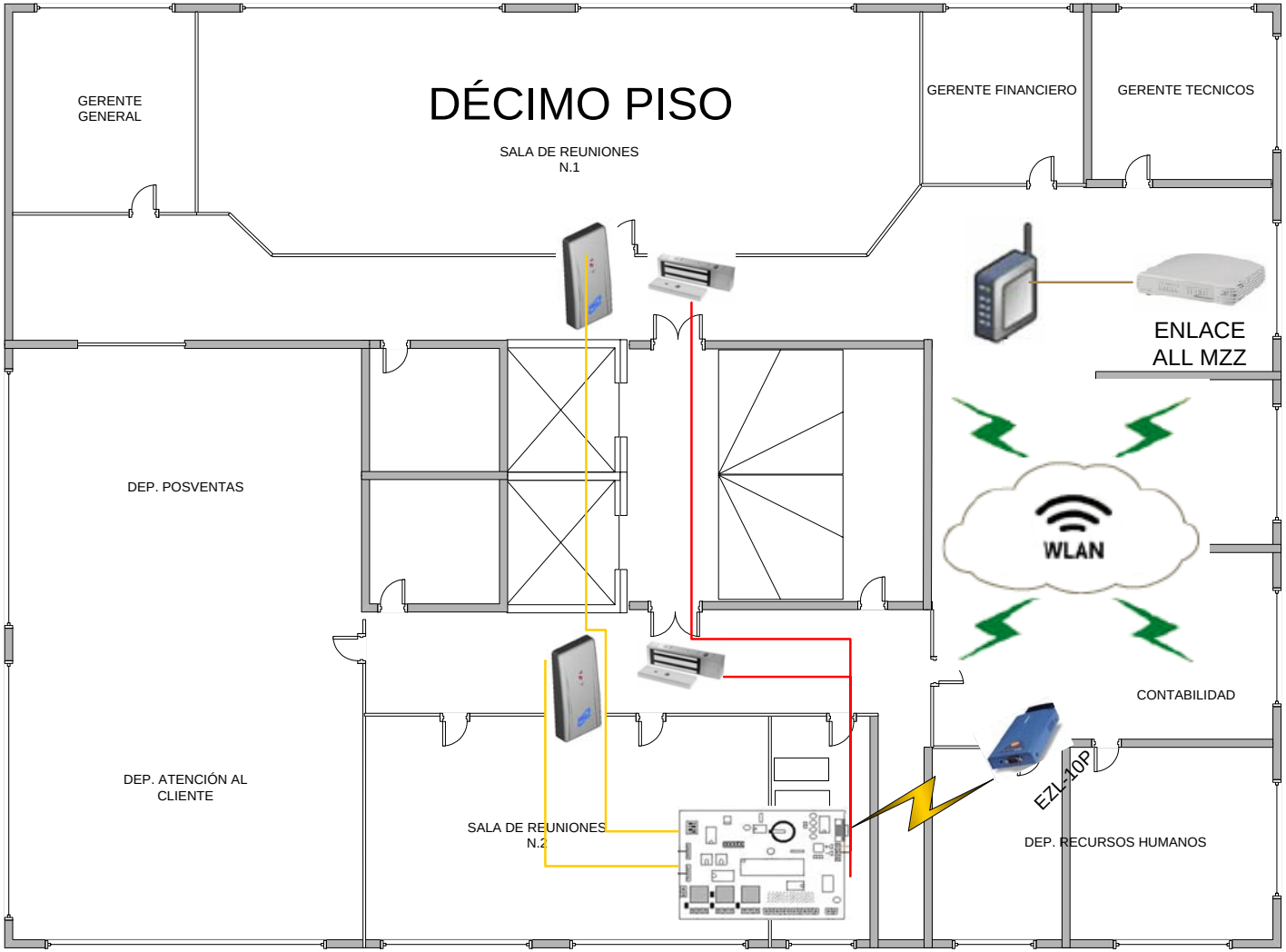


Figura 4.21 Ubicación de los equipos del sistema de control de acceso en el décimo piso.

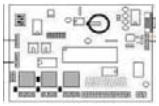
LECTOR DE PROXIMIDAD	**PUNTO DE ACCESO**
CERRADURAS MAGNETICAS	 **CONVERSOR SERIE A WIRELESS**
 **PANEL DE CONTROL**	 **SERVIDOR CONTROL ACCESO**
 **RED LAN INALAMBRICA**	 **SWITCH**

Figura 4.22 Cuadro de simbología de equipos del sistema de control de acceso

NOMENCLATURA DE CONVERSORES EZL-300W Lite	
ABREVIATURA	**NOMBRE**
EZL-PB	CONVERSOR EZL-300W Lite PLANTA BAJA
EZL-MZ	CONVERSOR EZL-300W Lite MEZANINE
EZL-10P	CONVERSOR EZL-300W Lite DECIMO PISO

Tabla 4.4 Nomenclatura de conversores EZL-300W Lite

CAPÍTULO V

DISEÑO DE LA RED INALÁMBRICA LOCAL 802.11

5.1 INTRODUCCIÓN

En el presente capítulo se realizarán todos los cálculos para obtener los requerimientos técnicos de la zona Wi-Fi óptima que cumplan con los objetivos definidos al inicio del proyecto.

Luego de revisar los requerimientos de la Red de Xerox se ha considerado la utilización del modo de configuración ESS[27] (Ver Capitulo II) ya que se utilizará más de un punto de acceso en la estructura de la red Wi-Fi

Otro aspecto importante a tomarse en cuenta en el diseño de una WLAN es determinar el área de cobertura, que para este caso de estudio se distribuyen en tres pisos del Edificio Xerox: planta baja (1054,22 m^2), mezanine (1054,22 m^2) y décimo piso (576,25 m^2) del Edificio Xerox.

5.2 SELECCIÓN DE LA TECNOLOGÍA

Al tratarse de redes inalámbricas que hacen uso del espectro radioeléctrico se ha considerado la banda de los 2,4 GHz ya que es una banda de uso libre según las normas establecidas por el organismo de regulación del espectro radioeléctrico en el Ecuador denominado CONATEL (Consejo Nacional de Telecomunicaciones).

La banda de los 2,4Ghz es implementada en el estándar 802.11b (Wi-Fi) que ha tenido gran acogida entre los fabricantes de dispositivos inalámbricos razón por la cual se han reducido costos, factores que han sido vitales para la selección de la tecnología en este proyecto.

[27] ESS Conjunto de servicios extendidos, Extended Service Set

En toda red inalámbrica el dispositivo fundamental es el punto de acceso, el mismo que determina el área de cobertura y el número de usuarios que pueden acceder a la red

5.3 SELECCIÓN DE EQUIPOS

En la tabla 5.1 se realiza una comparación de las características técnicas de algunos puntos de acceso existentes en el mercado y que se expusieron anteriormente en el capítulo III

CARACTERÍSTICAS	3com 7250	Dlink DWL-2100AP	Linksys Wrt54g
Potencia de Transmisión	17 dBm		18 dBm(31 mW)
Sensibilidad	1 Mbps: -91 dBm 2 Mbps: -89 dBm 5,5 Mbps: -87 dBm 11 Mbps: -83 dBm 12 Mbps: -81 dBm 24 Mbps: -80 dBm 36 Mbps: -75 dBm 54 Mbps: -68 dBm.	54 Mbps:-66 dBm 48 Mbps: - 71 dBm 36 Mbps : - 76 dBm 24 Mbps:- 80 dBm 18 Mbps: - 83 dBm 12 Mbps: - 85 dBm 11 Mbps: - 83 dBm 2 Mbps: - 89 dBm	54 Mbps:-65dBm 11 Mbps:-80dBm
Velocidad en Mbps	1,2,5.5,9,11,18,24,36,48,54	1,2,5.5 y 11	54 Mbps (802.11g) 11 Mbps (802.11b)
Numero de puertos Ethernet	4	4	4
Rango de frecuencia	2.400 – 2.4825 GHz	2.400 – 2.4825 GHz	2.400–2.4825GHz
Antenas integradas	2	1	2
Ganancia de antenas integradas	2 dBi	2 dBi	4 dBi
Soporte para antenas externas	Si	Si	Si
Modo de funcionamiento repetidor	Si	Si	3 funciones en 1

Servidor DHCP	Si	Si	Si
QoS	Si	Si	Si
Soporte de VLANs	Si	Si	Si
Nivel de máxima encriptación wep	128 bits	128 bits	128 bits
Soporte de WPA	Si	Si	Si
Soporta 802.1X	Si	Si	Si
Precio	Alto	Bajo	Medio

Tabla 5.1 Comparación de puntos de acceso

Al igual que en la tabla anterior, en la tabla 5.2 se describen las características técnicas de las tarjetas inalámbricas clientes existentes en el mercado mencionadas en capítulos anteriores.

CARACTERÍSTICAS	DLINK PCI DWL-G510	3COM officeconnect USB 54 Mbps 11g
Bus de datos	PCI	USB 2.0
Potencia de Transmisión	15 dBm ± 2 dBm	19 dBm
Sensibilidad	-69 dBm 54 Mbps -70 dBm 48 Mbps -74 dBm 36 Mbps -77 dBm 24 Mbps -83 dBm 12 Mbps -84 dBm 11 Mbps -85 dBm 6 Mbps -86 dBm 5,5 Mbps -88 dBm 2 Mbps -89 dBm 1 Mbps	11 Mbps: -74 dBm 5.5 Mbps: -87 dBm 2 Mbps: -87 dBm 1 Mbps: -91 dBm
Velocidad en Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	54, 48, 36, 24, 18, 12, 9, y 6 Mbps
Antenas integradas	1	1
Ganancia de antenas integradas	2dBi	1dBi
Soporte para antenas externas	No	No

Rango de frecuencias	2.400 – 2.4825 GHz	2.400 – 2.4825 GHz
Soporte de VLANs	Si	No
Nivel de máxima encriptación Wep	152 bits	256 bits
Soporte de WPA	Si	Si
Soporta 802.1X	Si	Si
Precio	Medio	Bajo

Tabla 5.2 Comparación de tarjetas de red inalámbricas cliente

Para establecer el enlace entre el mezanine y el décimo piso se utilizará la intranet existente en el edificio Xerox

5.3.1 JUSTIFICACIÓN DE LA SELECCIÓN DE EQUIPOS.

De acuerdo a la tabla 5.1 que detalla las características técnicas de los puntos de acceso que se encuentran en el mercado ecuatoriano; estos productos han sido tomados en cuenta primero porque los equipos mencionados ofrecen características importantes que satisfacen las necesidades de este proyecto, especialmente en lo que tiene que ver con características de rangos de frecuencia, seguridad, sensibilidad, soporte de antenas externas y facilidad de instalación, configuración y administración.

Los tres equipos comparados en la tabla muestran similares especificaciones técnicas; sin embargo la diferencia que se puede observar en estos dispositivos es que el equipo de Linksys Wrt54g en realidad supone tres dispositivos en uno, ya que trabaja como punto de acceso para conectar dispositivos inalámbricos, como conmutador 10/100 para conectar dispositivos Ethernet con cables y como tercera opción como ruteador que permite compartir una conexión a Internet DSL o por cable de alta velocidad por toda la red, además este punto de acceso tres en uno tiene un costo promedio en comparación a los otros dos citados, se concluye que el equipo Linksys Wrt54g es el adecuado para el diseño de la red inalámbrica.

Para la conexión a los equipos cliente de escritorio se ha analizado las especificaciones técnicas de las tarjetas descritas en la tabla 5.2 donde se toma en cuenta:

- ✓ El bus de datos.
- ✓ Sensibilidad.
- ✓ Ganancia de la antena.
- ✓ Compatibilidad con el punto de acceso (rango de frecuencia)

Por tanto, se estima conveniente el uso de la tarjeta DLINK PCI DWL-G510.

5.4 CONFIGURACIÓN DE EQUIPOS SELECCIONADOS PARA LA RED INALÁMBRICA.

5.4.1 CONFIGURACIÓN DEL PUNTO DE ACCESO LINKSYS WRT54G

Existen dos formas de instalación inicial del punto de acceso, una por medio del CD-ROM de configuración y el otro empleando la utilidad basada en Web.

Para facilitar el manejo de las utilidades de configuración del punto de acceso Linksys Wrt54g se utilizará la opción de configuración por Web (Explorador), con un ordenador conectado al punto de acceso, ver anexo 4, con el siguiente procedimiento:

1. Se inicia una sesión en el explorador Web con la dirección IP 192.168.1.1, que es una dirección predeterminada para el punto de acceso.

2. Aparece una pantalla en la cual solicita el usuario y contraseña, en el campo de usuario se lo deja en blanco y en el campo de contraseña se digita **admin**, y se acepta, como se muestra en el figura 5.1

Figura 5.1. Pantalla de inicio de instalación del equipo Linksys Wrt54g

3. Seguidamente como indica la fig. 5.2 aparece la pantalla de configuración o setup basada en Web solicitando datos del proveedor de servicios de Internet siendo estos campos opcionales dependiendo del proveedor de servicio de Internet (ISP)

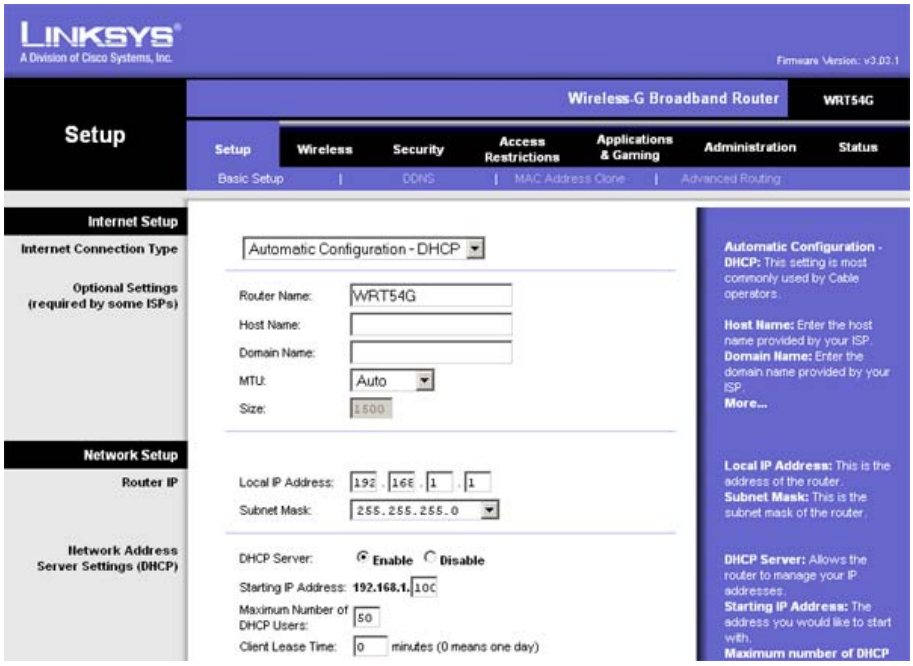


Figura 5.2 Primera pantalla de configuración (Internet)

4. Seleccionamos la pestaña wireless para configurar parámetros de la red inalámbrica, en cuyo menú desplegable se puede seleccionar:

   a. En el primer campo los estándares inalámbricos (802.11g o 802.11b o ambos) que se pueden ejecutar en la red.

   b. En el segundo campo el SSID que es el nombre de la red inalámbrica.

   c. En el tercer campo se selecciona el canal común de la red inalámbrica

   d. Y por último el campo SSID Broadcast con opciones de habilitado y deshabilitado, que permite difundir el SSID del punto de acceso a todo cliente inalámbrico que requiera acoplarse a la red inalámbrica, tal y como se muestra en la figura 5.3

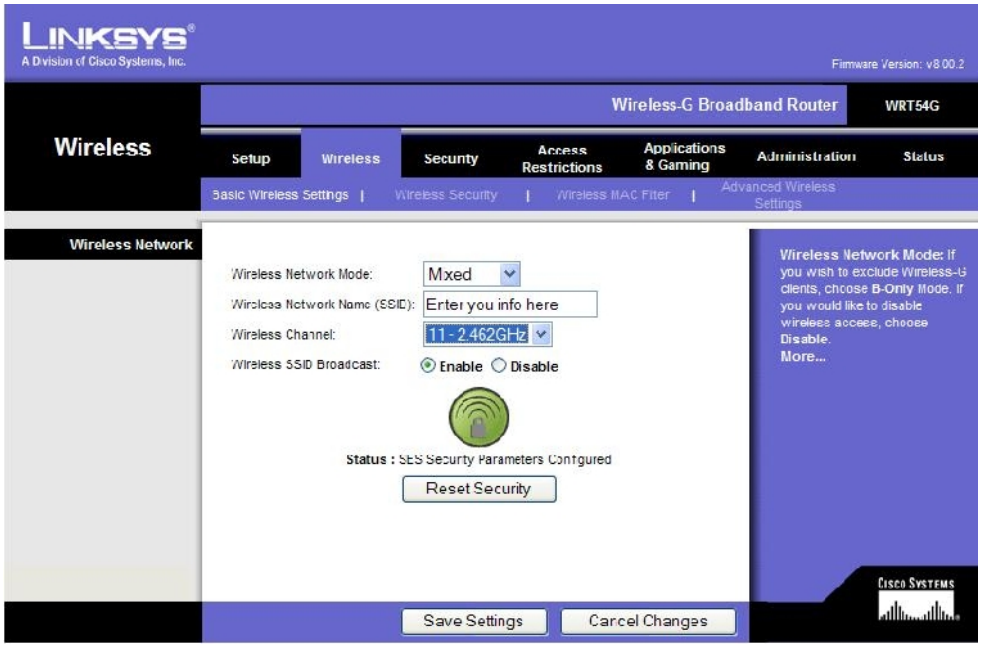


Figura 5.3. Pantalla de configuración de la red inalámbrica

5. Una vez configurado el punto de acceso se debe configurar la seguridad inalámbrica ya sea por uno de los tres métodos de seguridad WEP, WPA2 PERSONAL y WPA ENTERPRISE o RADIUS que soporta este punto de acceso. Como ya se ha visto en capítulos anteriores la seguridad WEP es vulnerable y no es una buena opción para la red inalámbrica, con respecto al método WPA ENTERPRISE no es factible ya que por el momento no se cuenta con un servidor Radius disponible en las instalaciones del Edificio

Xerox, pero en el futuro se lo puede adquirir, la opción más factible que puede ser implementada es el método WPA2 PERSONAL que a su vez ofrece dos métodos de encriptación TKIP (Temporal Key Integrity Protocol) y AES (Advanced Encryption Standard, Estándar de cifrado avanzado de datos), con claves de encriptación dinámica. Al elegir el método WPA282 PERSONAL como se muestra en la figura 5.4, se debe configurar los siguientes parámetros:

a. WPA ALGORITHM (Algoritmo WPA) se selecciona el método que se desea utilizar TKIP o AES

b. WPA SHARED KEY (Clave compartida WPA) se introduce una clave compartida de 8-63 caracteres.

c. GROUP KEY RENEWAL (Renovación de clave de grupo): se introduce un periodo de renovación de clave de grupo, que indica al punto de acceso la frecuencia con que debe cambiar las claves de encriptación

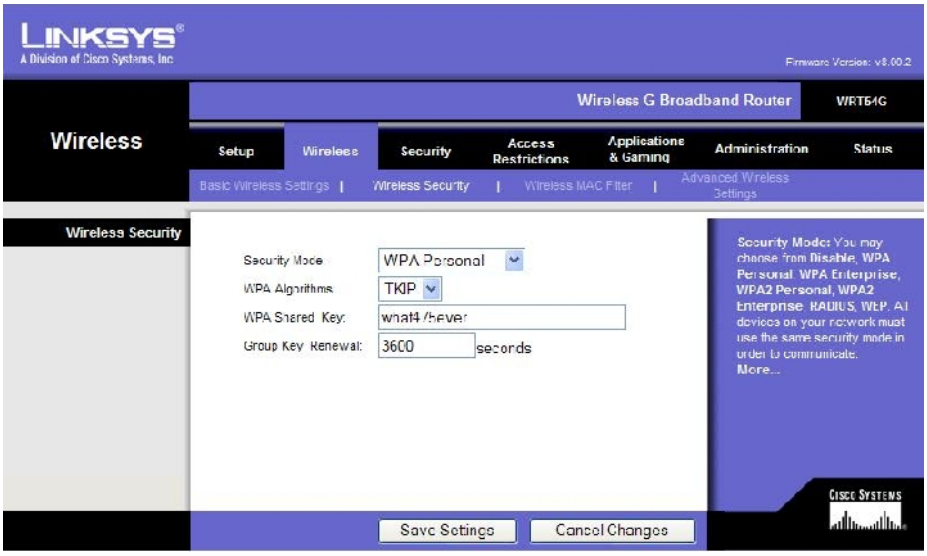


Figura 5.4. Pantalla de configuración de seguridad WPA2 PERSONAL

Para mayor seguridad de la red inalámbrica es posible configurar la opción de filtrado de direcciones MAC que controla el acceso inalámbrico mediante el uso

[28] WPA (Wi-Fi Protected Access, Acceso Protegido Wi-Fi)

de direcciones físicas de los dispositivos inalámbricos, en la figura 5.5 se muestra la pantalla, que presenta los siguientes puntos a activar:

a. Wireless MAC[29] Filter. Para filtrar los usuarios por dirección MAC, ya sea para permitir o para bloquear el acceso, se habilita Enable. Y lo contrario si no se desea filtrar los usuarios por direcciones MAC se selecciona Disable.

b. Prevent (Evitar) se bloqueara el acceso inalámbrico por dirección MAC.

c. Permit Only (Permitir solo) se permitirá el acceso inalámbrico por dirección MAC.

d. Edit MAC Address Filter List (Lista de filtros de direcciones MAC). Al hacer clic en este botón se abrirá la lista de filtros de direcciones MAC (MAC Address Filter List) como se muestra en la figura 5.6. En esta pantalla se pueden enumerar por dirección MAC los usuarios a los que desea proporcionar o bloquear el acceso. Para facilitar la referencia, haga clic en el botón

e. Wireless Client MAC List (Lista de MAC de clientes inalámbricos) para mostrar una lista de usuarios de la redpor dirección MAC

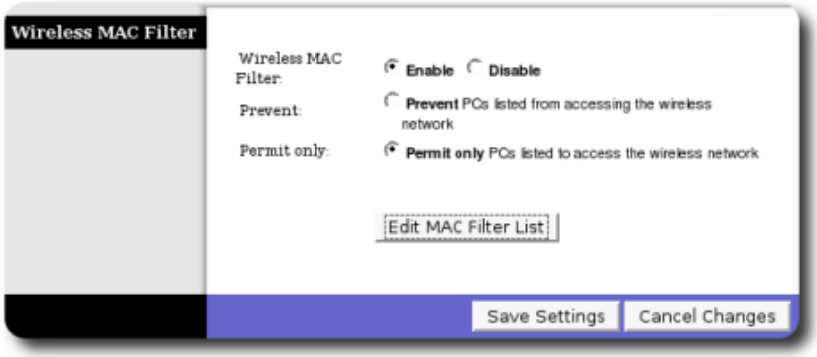


Figura 5.5 Pantalla de configuración de direcciones MAC

[29] MAC (Medium Access Control address o dirección de control de acceso al medio)

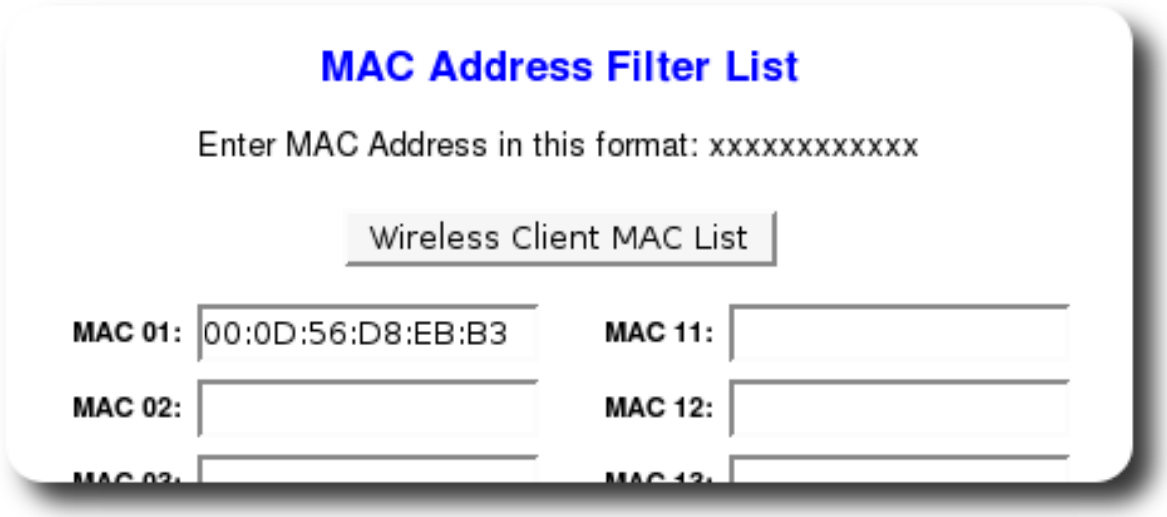


Figura 5.6 Pantalla de lista de filtros de direcciones MAC

5.5 DETERMINACIÓN DEL ÁREA DE COBERTURA, ALCANCE Y CANALES DE COMUNICACIÓN

El área de cobertura es el espacio hasta donde tiene alcance la señal que se transmite a través de la red inalámbrica, que en el caso de este proyecto el área de cobertura se limitara a tres plantas (Planta baja, Mezanine y Décimo) de los diez pisos del edificio Xerox.

PLANTA BAJA

En esta planta se encuentra ubicada la recepción de ingreso a las instalaciones del Edificio y una sala de exhibición de equipos donde no existe mayor concentración de usuarios ni obstáculos que interfieran en la calidad de señal, como se muestra en la figura 5.7

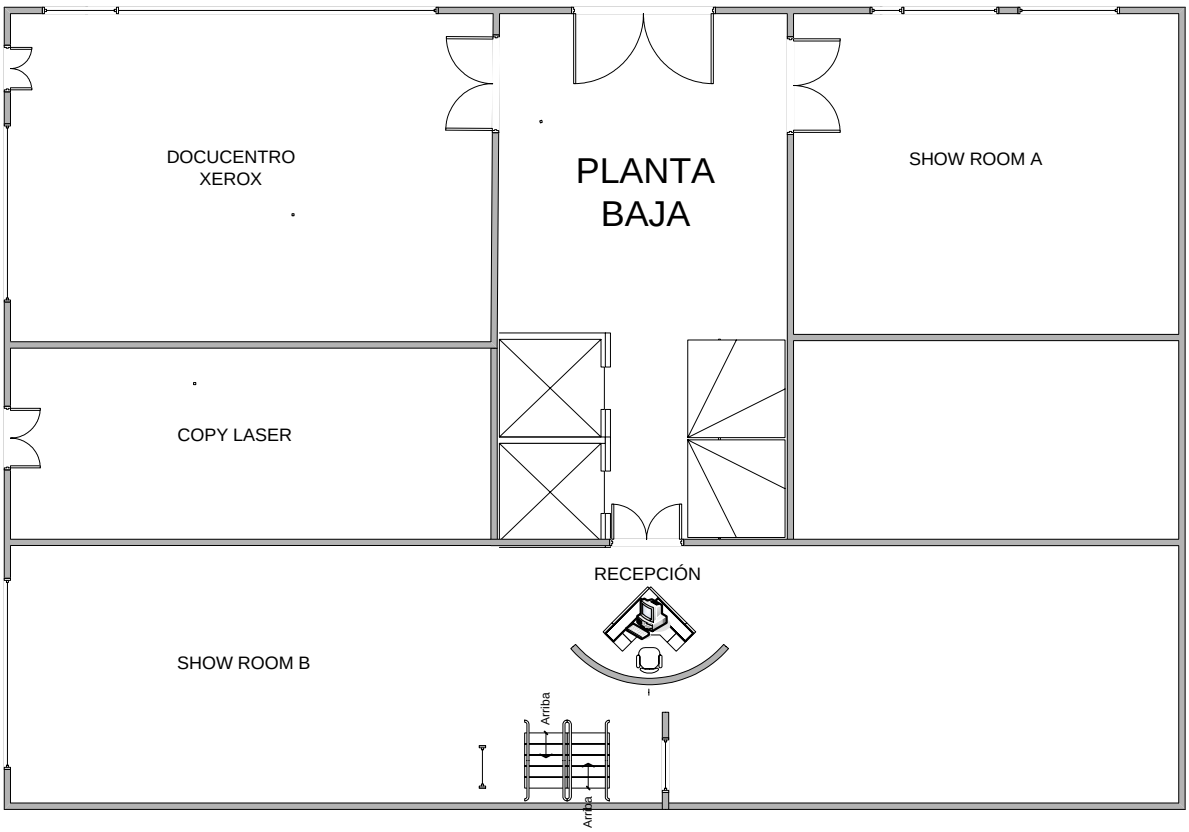


Figura 5.7 Plano Planta Baja

MEZANINE

Dentro de este piso se encuentran la mayor cantidad de usuarios potenciales donde se debe poner mayor atención al servicio que presta la red inalámbrica, tomando en cuenta que al existir paneles divisorios y el ascensor que son agentes que interfieren en la calidad de la señal, siendo el ascensor el mayor obstáculo a tomarse en cuenta, como se muestra en la figura 5.8.

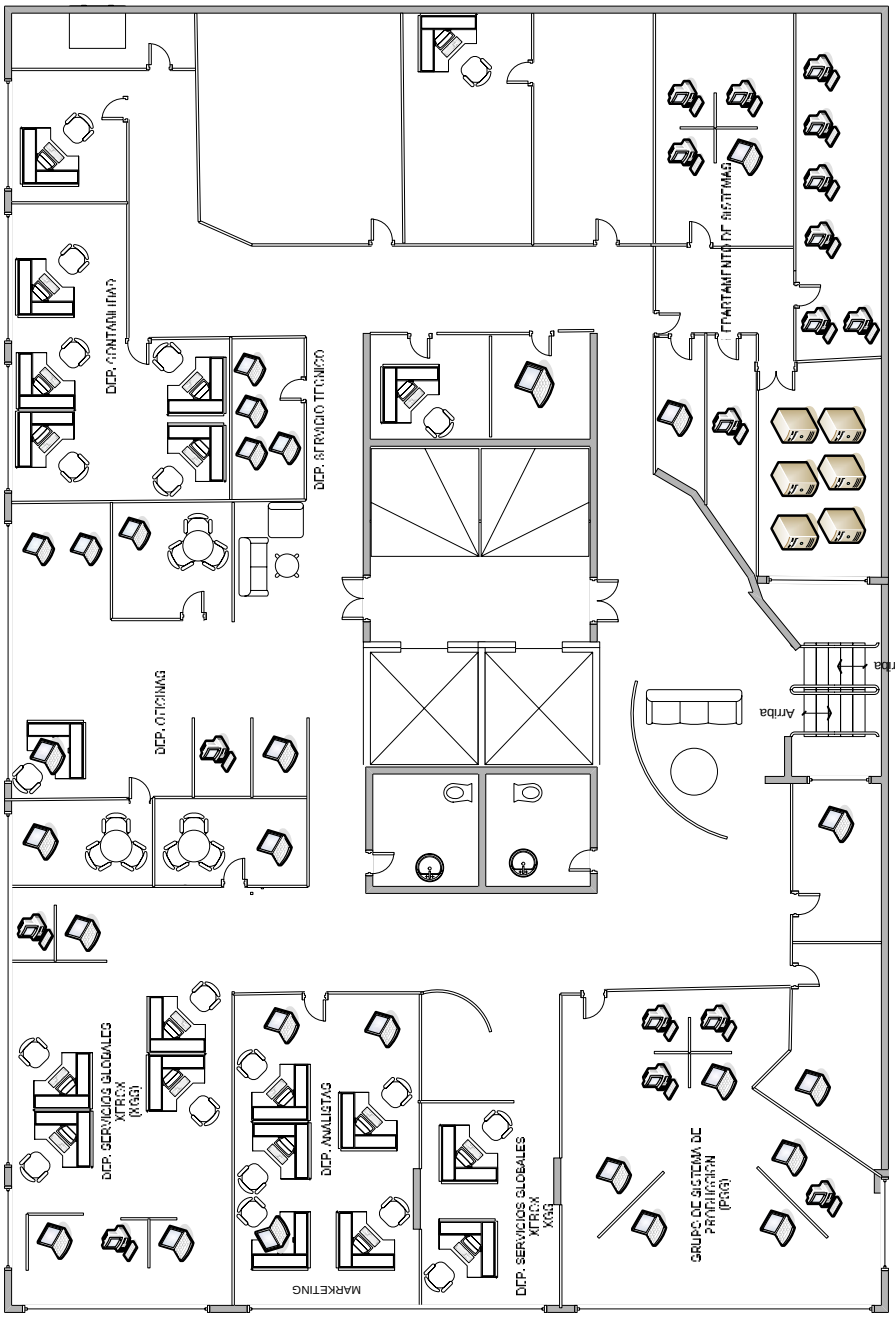


Figura 5.8 Plano del Mezanine

DÉCIMO PISO

Es la última planta del edificio que al igual que el mezanine presenta características similares en cuanto a obstáculos y usuarios como se muestra en la figura 5.9

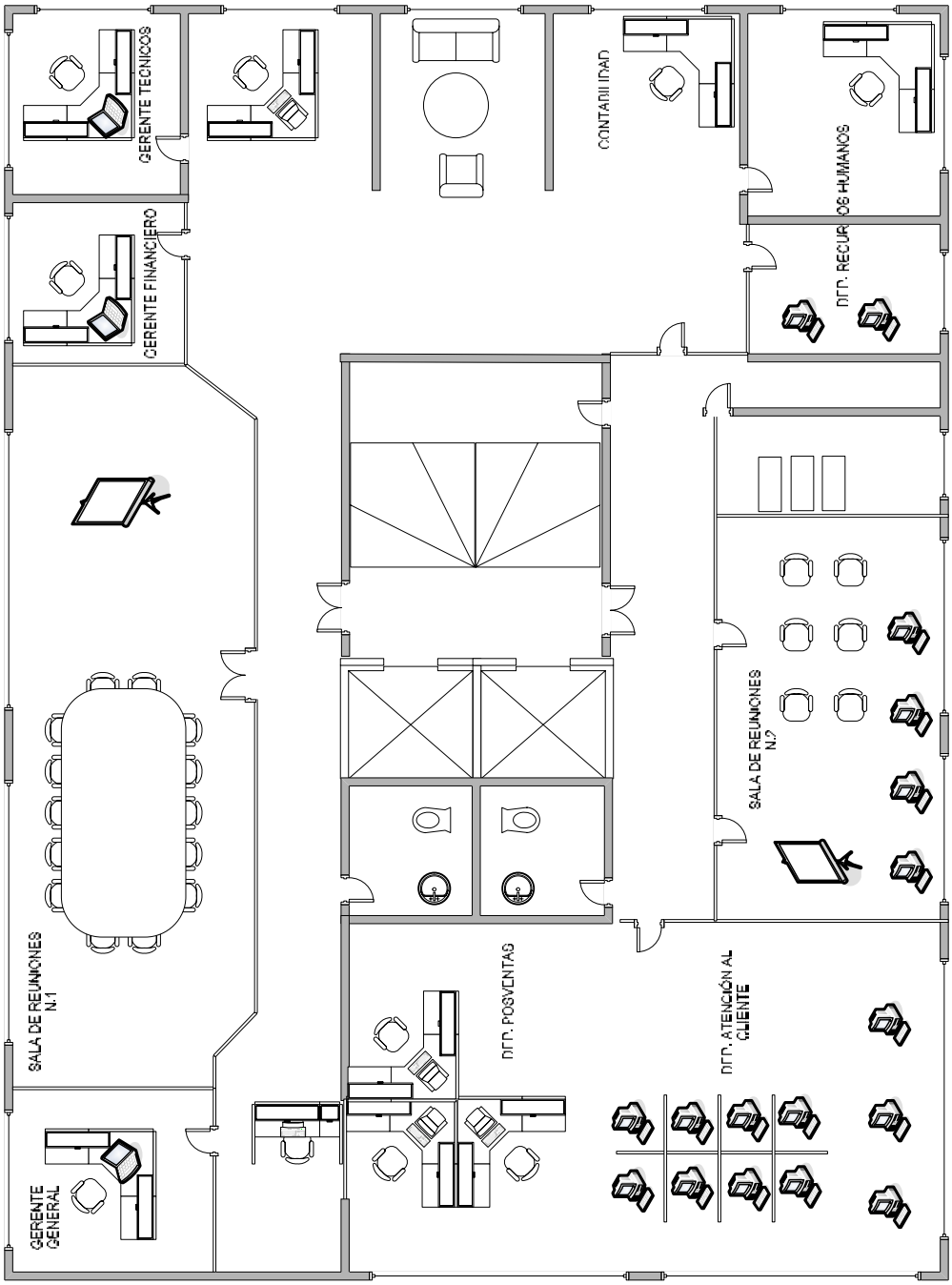


Figura 5.9 Plano del Décimo Piso

Para determinar el alcance de señal se realizarán varios cálculos teóricos con los equipos Wi-Fi (punto de accesos, antenas, cables y conectores) tomando en cuenta sus características técnicas.

En primera instancia se calculara la pérdida de propagación, que es la cantidad de señal necesaria para llegar de un extremo a otro de la transmisión; determinando si esta es suficiente para establecerse la comunicación, que está dada por la siguiente fórmula:

$$Pp = 20 \log (d) + 20 \log (f) + 32.4$$

Donde:

Pp = pérdida en dB.

d = distancia (Km)

f = frecuencia (MHz)

El valor de la frecuencia depende del canal en el que se tenga configurado el equipo, como referencia se utilizara la frecuencia 2.412 GHz (canal 1) en este caso, la formula anterior quedaría resumida en la siguiente:

$$Pp = 20 \log (d) + 100 \text{ dB}$$

$$Pp = 20 \log (0.10) + 100 \text{ dB}$$

$$Pp = - 20 \text{ dB} + 100 \text{ dB}$$

$$Pp = 80 \text{ dB}$$

Además del cálculo de la pérdida propagación, se requiere realizar el cálculo del alcance de la transmisión (S) que se basa en sumar todas las ganancias (radios, antenas y amplificadores) y restar las pérdidas que se producen (longitud de cable, conectores, pararrayos y similares). Se debe tener pendiente que no hay que sumar la ganancia de la antena en ambos extremos del enlace.

Para el presente proyecto se utilizará la tarjeta DLINK PCI DWL-G510 para el usuario cliente que tiene una potencia de transmisión de 15dB con una antena incorporada con ganancia de 2dB en el otro extremo se empleará un punto de acceso Linksys Wrt54g con una potencia de transmisión de 18dB con dos antenas incorporadas de 2dBi cada una, también se utilizará un conector con pérdida de

1dB, todas los valores están expresados en dB por tanto el cálculo es sencillo y hay que tomar en cuenta que se debe hacer en ambos sentidos.

CÁLCULO DEL ENLACE (ADAPTADOR CLIENTE – PUNTO DE ACCESO)

Sitio A (Lugar donde se encuentra el equipo cliente):

POTENCIA = Potencia de la tarjeta + Ganancia Antena

= 15 dB + 2dB

= 17dB

Sitio A = 17 dB

Sitio B (Lugar donde se encuentra el punto de acceso)

POTENCIA = Conector + Ganancia Antena

= -1dB + 4dB

Sitio B = 3 dB

Sitio A + Sitio B = 20 dB de ganancia

Luego se resta la perdida de la propagación y tomando en cuenta las condiciones ambientales, se pueden estimar unas pérdidas adicionales de 20 dB

S = 20dB - 80 dB – 20dB

S= **- 80 dB**

Donde:

S=Alcance de Transmisión

CÁLCULO DEL ENLACE (PUNTO DE ACCESO – ADAPTADOR CLIENTE)

Sitio A (Lugar donde se encuentra el punto de acceso)

POTENCIA = AP - Conector + Ganancia. Antena

= 18 dB-1 dB+4 dB

Sitio A = 21 dB

Sitio B (Lugar donde se encuentra el equipo cliente)

POTENCIA = Ganancia Antena

= 2 dB

Sitio B = 2 dB

Sitio A + Sitio B = 23 dB de ganancia

Luego se resta la perdida de la propagación y tomando en cuenta las condiciones ambientales, se pueden estimar unas pérdidas adicionales de 20 dB

S = 23 dB - 80 dB – 20dB

S = **- 77 dB**

Donde:

S = Alcance de Transmisión

Teóricamente la comunicación inalámbrica entre el equipo trasmisor y receptor en ambos sentidos, va a ser posible ya que el nivel de la señal obtenido (-80 dB y -77 dB), es igual y mayor a la especificación de sensibilidad de recepción (-80dB a 11Mbps) del equipo receptor dado por el fabricante. Estos cálculos corresponden a la señal de los equipos que se encuentran ubicados al interior del mezanine como del décimo piso.

Para la comunicación entre el mezanine y el décimo piso se utilizara dos puntos de acceso Linksys Wrt54g con una potencia de transmisión de 18dB y una antena incorporada de 2dB cada uno, conectados a la red Ethernet existente

Los canales que se utilizaran son: 1,6 y 11. La asignación de estos canales se realiza en base a la ubicación de los Access Point. La idea es no tener dos áreas contiguas con canales cercanos, para evitar interferencia en la transmisión de clientes cercanos como se indica en la figura 5.10

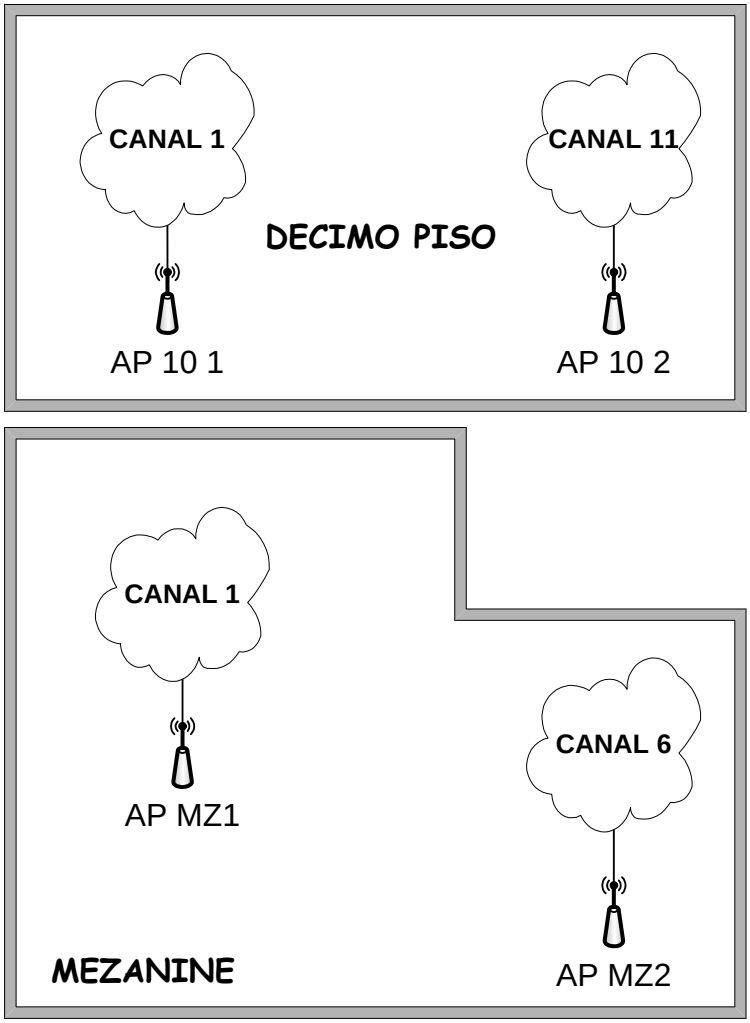


Figura 5.10 Distribución de los canales

5.6 CÁLCULO Y UBICACIÓN DE LOS PUNTOS DE ACCESO

Como parte de este proyecto de tesis se requiere calcular el número de puntos de acceso capaces de cubrir todas las áreas de la red inalámbrica. No existe un método exacto para determinar el número de puntos de acceso pero como referencia se utilizará la siguiente fórmula cuyo resultado será únicamente una aproximación.

$$N_{AP} = \frac{BW \times N_{USR} \times n_{USR}}{V_{EST}}$$

Donde:

N_{AP} = Número de Puntos de acceso

BW = Ancho de Banda por usuario

N_{USR} = Número de Usuarios

n_{USR} = Utilización Promedio de la red

V_{EST} = Velocidad Estimada

Las características de los servicios que se pretenden ofrecer a los usuarios de la red inalámbrica de Xerox, no exigen grandes cantidades de ancho de banda, esto se determino luego de un análisis de tráfico de la red actual con el administrador de la red y que se resume en el cuadro 5.3

TRAFICO DE LA RED LAN XEROX HORAS PICO	
NOMBRE DEL SERVICIO	VALOR (Kbps)
SMTP	250
http	150
FTP	220
Varios	200
TOTAL	820

Tabla 5.3 Tráfico de la red LAN Xerox[30]

[30] Datos proporcionados por el departamento de sistemas de Xerox.

Haciendo referencia al cuadro anterior, el valor total de 820 Kbps corresponde al tráfico de la red por cada usuario que para el cálculo siguiente con respecto al ancho de banda por usuario sería más que suficiente con 1 Mbps.

Cálculo:

$$N_{AP} = \frac{1\text{Mbps} \times 100 \times 0.25}{10}$$

$$N_{AP} = 2.5 \quad \text{Puntos de Acceso}$$

Con este resultado (2.5) se concluye que para la red inalámbrica del edificio Xerox se debería utilizar tres puntos de acceso pero se ha considerado que se deben utilizar cuatro puntos de acceso para evitar futuras interferencias ya que es posible una remodelación al interior de los pisos que influiría en la calidad de la señal inalámbrica

Para la ubicación de los puntos de acceso se ha tomado en cuenta el mejor ángulo de vista donde la calidad de la señal inalámbrica sea la óptima en cada uno de los pisos.

Con respecto al mezanine se ha considerado ubicar el primer punto de acceso (AP MZ-1) en la ZONA 1, brindando la cobertura inalámbrica a los sectores que corresponden a los departamentos de PSG, Analistas, XGS, Oficinas y parte de Servicio Técnico; el segundo punto de acceso (AP MZ-2) se ubica en la ZONA 2, el cual brinda la cobertura inalámbrica a los sectores que corresponden a los departamentos de Sistemas, Servicio Técnico, Contabilidad y parte de Oficinas, como se muestra en la figura 5.11.

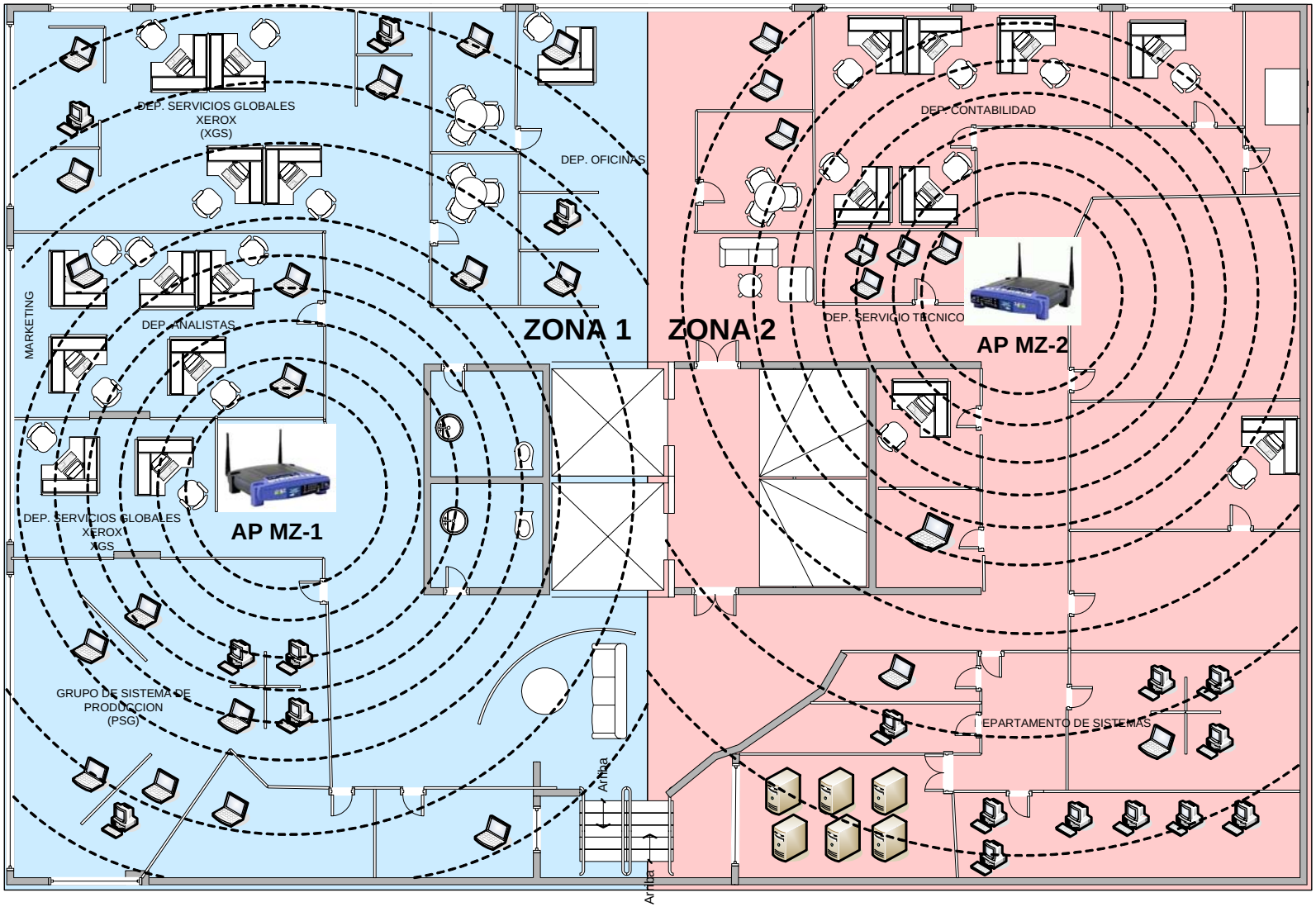


Figura 5.11 Ubicación de los puntos de acceso Mezanine

Para lo que corresponde al décimo piso se ha considerado ubicar el primer punto de acceso (AP 10-1) en la ZONA 3, brindando la cobertura inalámbrica a los sectores que corresponden a los departamentos de Atención al Cliente, Posventas, Gerencia General, Sala de Reuniones N 1 y parte de Sala de Reuniones N 2; el segundo punto de acceso (AP 10-2) se ubica en la ZONA 4, el cual brinda la cobertura inalámbrica a los sectores que corresponden a los departamentos Recursos Humanos, Contabilidad, Gerencia Financiera, Gerencia Técnica y parte de Sala de Reuniones N 1, como se muestra en la figura 5.12.

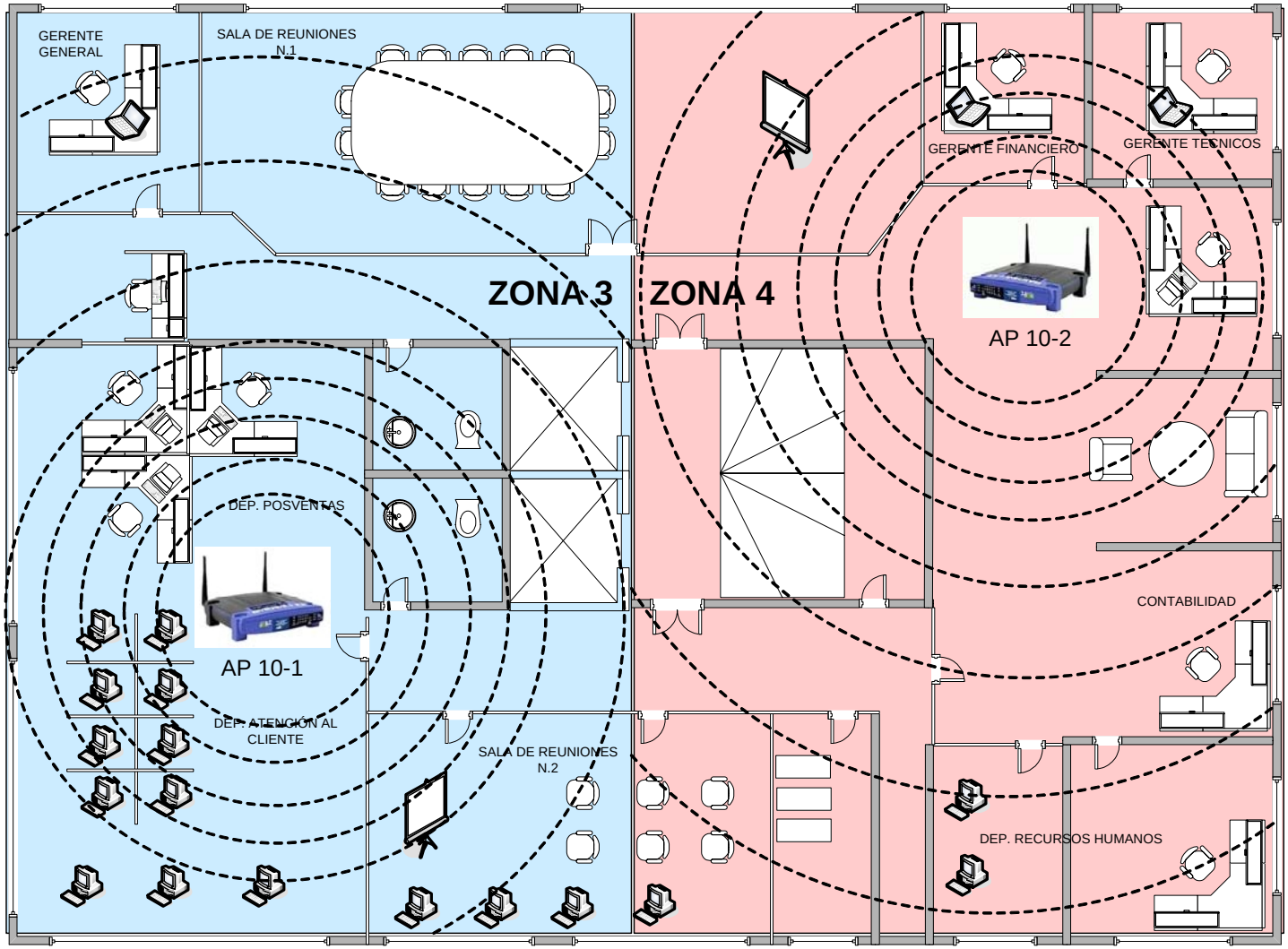


Figura 5.12 Ubicación de los puntos de acceso Décimo Piso

5.7 DIRECCIONAMIENTO IP

La información sobre las direcciones IP de la red Ethernet actual de Xerox no fue proporcionada por seguridad interna de la compañía por tal razón, se realizará un esquema de direccionamiento IP para la red Ethernet actual, la red inalámbrica y el sistema de control de acceso de Xerox.

Para iniciar la asignación de direcciones IP primero se debe tomar en cuenta el número de computadores portátiles y de escritorio, switch, router, servidores, punto de acceso y convertidores (113 Equipos) y segundo la tasa de crecimiento de usuarios proyectada a diez años (Df), para la cual se aplica la siguiente fórmula:

$$Df = Do\ (1+ r)^n$$

Donde,

Df = Demanda Final

Do = Demanda Inicial

r = Porcentaje Estimado

n = Número de Años

Siendo:

$$Df = 113\ (1+0,05)^{10}$$

$$Df = 184,06 \text{ equipos}$$

Obtenida la demanda final (Df) se tiene que la red de Xerox tendrá un crecimiento aproximado del 62.88 por ciento, lo que indica que en diez años la red ocupara cerca de 184 direcciones IPs, que con un direccionamiento IP de clase C sería suficiente ya que esta abarca hasta 254 direcciones IP a ser asignadas a las máquinas para lo cual se partirá de la IP privada 192.168.10.0/24 con una máscara de red 255.255.255.0, cuya forma binaria es:

11000000 . 10100000 . 00001010 . 00000000 / 24

RED HOST

Para empezar la división en subredes se aplica la formula $2^n - 2$, tomando en cuenta la mayor cantidad de usuarios por piso siendo el Mezanine con 74 host:

$$2^n - 2$$

n = número de bits para host

$$2^7 - 2 = 126 \text{ direcciones}$$

Donde las 126 direcciones abastecen a los 74 host requeridos en el mezanine, De este resultado se procede asignar las direcciones para las subredes, recorriendo el número de bits de derecha a izquierda del último octeto de bits de la dirección:

Primera subred (Mezanine):

192 . 168 . 10 . **0** 0000000 / 25

RED HOST

/ 25 hace referencia a un bit adicional para la subred, con una máscara:

255.255.255.128

Los rangos de direcciones IP para la primera subred van desde:

192.168.10.0 hasta 192.168.10.127

Segunda subred (Décimo Piso):

192 . 168 . 10 . **0**1 111110 / 26

RED HOST

/ 26 hace referencia a dos bits adicionales para la subred, con una máscara:

255.255.255.192

Los rangos de direcciones IP para la segunda subred van desde:

192.168.10.128 hasta 192.168.10.191

La comunicación entre el mezanine y el décimo piso se hará a través una VLAN (tercera subred).

Tercera Subred (VLAN entre Mezanine y Décimo Piso)

192.168.10.192 / 26

/ 26 hace referencia a dos bits adicionales para la subred, con una máscara:

255.255.255.192

Los rangos de direcciones IP para la tercera subred van desde:

192.168.10.192 hasta 192.168.10.255

En la tabla 5.4 se describen cada una de las direcciones IP a asignarse a los host, puntos de acceso, servidores, switches y convertidores con su respectiva mascara de subred y Gateway requeridos en cada subred, además la cantidad de direcciones reservadas en algunas subredes.

DIRECCIONAMIENTO IP				
SUBRED	**NOMBRE HOST**	**DIRECCION IP**	**MASCARA**	**GATEWAY**
1	S1B (GATEWAY)	192.168.10.1	255.255.255.128	
1	R1A	192.168.10.2	255.255.255.128	192.168.10.1
1	AP MZ-1	192.168.10.3	255.255.255.128	192.168.10.1
	AP MZ-2	192.168.10.4	255.255.255.128	192.168.10.1
1	EZL-PB	192.168.10.5	255.255.255.128	192.168.10.1
1	EZL-MZ	192.168.10.6	255.255.255.128	192.168.10.1
1	ECUQUIMDWH	192.168.10.7	255.255.255.128	192.168.10.1
1	XDORINET	192.168.10.8	255.255.255.128	192.168.10.1
1	XDORQSQL	192.168.10.9	255.255.255.128	192.168.10.1
1	XEROX10 WS1-F	192.168.10.10	255.255.255.128	192.168.10.1
1	XEROX MZ	192.168.10.11	255.255.255.128	192.168.10.1
1	AS/400	192.168.10.12	255.255.255.128	192.168.10.1
1	63 HOST	192.168.10.13 - 192.168.10.76	255.255.255.128	192.168.10.1
1	DIRECCIONES IP LIBRES SUBRED 1	192.168.10.77 a 192.168.10.127	255.255.255.128	192.168.10.1
	S1C (GATEWAY)	192.168.10.129	255.255.255.192	
2	S2C	192.168.10.130	255.255.255.192	192.168.10.129
2	AP 10-1	192.168.10.131	255.255.255.192	192.168.10.129
2	AP 10-2	192.168.10.132	255.255.255.192	192.168.10.129
2	EZL-10P	192.168.10.133	255.255.255.192	192.168.10.129
2	27 HOST	192.168.10.134 a 192.168.10.161	255.255.255.192	192.168.10.129
2	DIRECCIONES IP LIBRES SUBRED 2	192.168.10.162 A 192.168.10.191	255.255.255.192	192.168.10.129
3	S1B	192.168.10.193	255.255.255.192	192.168.10.194
3	S1C	192.168.10.194	255.255.255.192	192.168.10.193

Tabla 5.4 Tabla de distribución del direccionamiento IP

5.8 INTEGRACIÓN DEL SISTEMA DE CONTROL DE ACCESO A LA RED INALÁMBRICA

El sistema de control de acceso se comunica con la red inalámbrica a través de los conversores inalámbricos (EZL-300W Lite) como se explica en el capitulo anterior y cuyas direcciones IP fueron asignadas en la tabla 5.4.

Esta integración tiene la ventaja de facilitar el manejo del sistema de control (Administración) como parte de la red inalámbrica.

CAPÍTULO VI

ANÁLISIS DE COSTOS Y RENTABILIDAD DEL PROYECTO

6.1 COSTOS DE LA RED INALÁMBRICA Y DEL SISTEMA DE CONTROL DE ACCESO.

Este capítulo hace referencia a costos de equipos requeridos en hardware y software tanto para el sistema de control de acceso como para la red inalámbrica, a fin de determinar la rentabilidad del proyecto en base a una evaluación financiera del mismo, es importante aclarar que este capítulo es referencial en caso de querer ejecutar el proyecto a futuro, ya que el objetivo inicial de esta tesis no contempla el aspecto de implementación.

Para la realización del diseño de la red inalámbrica y del sistema de control de acceso del edificio matriz Xerox, se realizó previamente un estudio de la LAN actual, se recopiló información de la infraestructura física, planos, y distribución del espacio físico en cada planta del edificio, y de los requerimientos de red en cada departamento.

Con la información recopilada, se realizaron los diseños de la red y del sistema de control, en el que se incluyen esquemas, políticas de seguridad, y calidad de servicio; además, se investigó los equipos disponibles en el mercado que cumplen con los requerimientos del diseño. Se calcula que este proyecto, en el mercado tendría un costo aproximado de 2000 dólares americanos.

En los siguientes cuadros se detallan los costos de inversión, costos de instalación y configuración y costos de operación de los equipos que fueron seleccionados en

el capítulo IV correspondiente al sistema de control de acceso y capítulo V correspondiente al diseño de la red inalámbrica local.

Los costos correspondientes a la mano de obra están incluidos en los costos de instalación y configuración de los equipos tanto para la red inalámbrica como para el sistema de control.

6.1.1 COSTOS DE LA RED INALÁMBRICA

En las tablas 6.1, 6.2, 6.3 y 6.4 se muestran los costos para la red inalámbrica:

- ✓ Costos de inversión de equipos.
- ✓ Costos de instalación y configuración de equipos
- ✓ Costos de operación

COSTOS DE INVERSIÓN EN EQUIPOS			
DESCRIPCIÓN	**CANTIDAD**	**COSTO UNITARIO (USD)**	**COSTO TOTAL (USD)**
Punto de acceso Lynksys Wrt54g	4	130	520,00
Tarjeta de red cliente DLINK PCI DWL-G510	63	100	6300,00
TOTAL COSTOS DE INVERSION			**6820,00**

Tabla 6.1 Costos de inversión en equipos para la red inalámbrica

COSTOS DE INSTALACIÓN Y CONFIGURACIÓN DE EQUIPOS				
DESCRIPCIÓN	**CANTIDAD**	**COSTO /h CONFIGURACIÓN**	**TIEMPO ESTIMADO**	**COSTO TOTAL (USD)**
Punto de acceso Lynksys Wrt54g	4	35	1.5 horas	210,00
Tarjeta de red cliente DLINK PCI DWL-G510	63	15	0.5 horas	472.50
TOTAL COSTOS INSTALACIÓN Y CONFIGURACIÓN				**682.50**

Tabla 6.2 Costos de instalación y configuración de equipos

COSTOS DE OPERACIÓN		
DESCRIPCIÓN	**COSTO MENSUAL (USD)**	**COSTO ANUAL (USD)**
Mantenimiento	1000	12000,00
Administración de la red	2000	24000,00
TOTAL COSTOS DE OPERACIÓN	**3000**	**36000,00**

Tabla 6.3 Costos de operación para la red inalámbrica

COSTO TOTAL DE LA RED INALÁMBRICA	
DESCRIPCIÓN	**COSTO (USD)**
Costos de inversión en equipos	6820,00
Costos de instalación y configuración de equipos	682,50
TOTAL	**7502,50**

Tabla 6.4 Costo total de la red inalámbrica.

Se debe señalar que la red inalámbrica no requiere de autorización, ni de pago de una licencia por el uso del espectro, ya que según la "Norma para la implementación y operación de sistemas de espectro ensanchado" este diseño es considerado como un sistema de reducido alcance.

6.1.2 COSTOS DEL SISTEMA DE CONTROL DE ACCESO

En las tablas 6.5, 6.6, 6.7 y 6.8 se indican los costos para el sistema de control de acceso:

- ✓ Costos de inversión de equipos.
- ✓ Costos de instalación y configuración de equipos
- ✓ Costos de operación

COSTOS DE INVERSIÓN DE EQUIPOS			
DESCRIPCIÓN	**CANTIDAD**	**COSTO UNITARIO (USD)**	**COSTO TOTAL (USD)**
Panel de control ZEBRA ZC500	3	600	1800,00
Conversor serie a Wireless EZL-300W Lite	3	150	450,00
Lector de proximidad ZEBRA ZL50	5	58	290,00
Tarjeta de proximidad Kimaldi EM4102	150	3,5	525,00
Cerradura magnética C-600 F	5	60	300,00
Cable FTP CAT 6	80	0,44	35,20
Software Sistema de control de Acceso ZEBRA SV200	1	600	600,00
		TOTAL DE INVERSIÓN	**4000.20**

Tabla 6.5 Costos de inversión para el sistema de control de acceso

COSTOS DE INSTALACIÓN Y CONFIGURACIÓN DE EQUIPOS				
DESCRIPCIÓN	**CANTIDAD**	**COSTO /h CONFIGURACIÓN**	**TIEMPO ESTIMADO**	**COSTO TOTAL (USD)**
Panel de control ZEBRA ZC500	3	40	2 horas	240,00
Conversor serie a Wireless EZL-300W Lite	3	20	1 hora	60,00
			TOTAL DE INVERSIÓN	**300,00**

Tabla 6.6 Costos de instalación y configuración del sistema de control de acceso

COSTOS DE OPERACIÓN			
DESCRIPCIÓN	**CANTIDAD**	**COSTO MENSUAL (USD)**	**COSTO ANUAL (USD)**
Administración	1	1000	12000,00
Guardia	1	320	3840,00
TOTAL COSTO DE OPERACIÓN		**1700**	**15840,00**

Tabla 6.7 Costos de operación para el sistema de control de acceso.

COSTO TOTAL DEL SISTEMA DE CONTROL DE ACCESO	
DESCRIPCIÓN	**COSTO PRIMER AÑO (USD)**
Costos de inversión en equipos	4000,20
Costos de instalación y configuración de equipos	300,00
TOTAL	**4300,20**

Tabla 6.8 Costo total del sistema de control de acceso.

6.2 PROYECCIÓN DE COSTOS DE LA RED INALÁMBRICA Y DEL SISTEMA DE CONTROL DE ACCESO.

La red inalámbrica y el sistema de control de acceso se han proyectado para cinco años de la siguiente forma:

El primer año corresponde a la inversión inicial de todo el proyecto, que está compuesta por el costo total de la red inalámbrica, el costo total del sistema de control de acceso y el costo del diseño del proyecto, como se muestra en la tabla 6.9.

INVERSIÓN INICIAL DEL PROYECTO	
DESCRIPCIÓN	**COSTO (USD)**
Costos total de la red inalámbrica	7502,50
Costos total del sistema de control de acceso	4300,20
Costo diseño del proyecto	2000,00
TOTAL	**13802,70**

Tabla 6.9 Inversión inicial del proyecto

El segundo, tercero, cuarto, y quinto años los costos a tomar en cuenta son los costos de operación de todo el proyecto que implican el mantenimiento y la administración de la red inalámbrica y del sistema de control, como se muestra en la tabla 6.10

COSTO DE OPERACIÓN DEL PROYECTO	
DESCRIPCIÓN	**COSTO (USD)**
Costos de operación de la red inalámbrica	36000,00
Costos de operación del sistema de control de acceso	15840,00
TOTAL	**51840,00**

Tabla 6.10 Costo de operación del proyecto

En la tabla 6.11 se muestra la proyección de las inversiones para los cinco años.

INVERSIÓN POR AÑO PARA LA IMPLEMENTACIÓN	
AÑO	INVERSIÓN (USD)
0	13802,70
1	51840
2	51840
3	51840
4	51840
5	51840

Tabla 6.11 Costo total del proyecto por año.

6.3 REDUCCIÓN DE COSTOS CON LA RED INALÁMBRICA Y EL SISTEMA DE CONTROL DE ACCESO

Actualmente todas las organizaciones cambian continuamente su infraestructura, obligando a los encargados de la red a modificar los puntos de cableado, e incluso a realizar un nuevo tendido de cableado. Xerox del Ecuador, no es la excepción, sus departamentos han sufrido cambios en su ubicación física; por esta razón, el personal del departamento de sistemas, estima que de los 90 puntos de cableado para empleados, un promedio de 15% de ellos son trasladados mensualmente, y un 7% necesita un nuevo tendido de cableado; para satisfacer las necesidades de

los usuarios en los distintos departamentos; es decir que de los 90 puntos de cableado, alrededor de 14 puntos son trasladados mensualmente, y 7 son re-cableados. Esta situación representa un problema constante para Xerox, no solo por los gastos que implica, sino también por las molestias a los usuarios. En la tabla 6.12 se indica el ahorro en cableado estructurado según proformas de empresas dedicadas a brindar este servicio.

REDUCCIÓN DE COSTOS CON LA RED INALÁMBRICA				
DESCRIPCIÓN	**CANTIDAD**	**COSTO UNITARIO (USD)**	**COSTO MENSUAL (USD)**	**COSTO ANUAL (USD)**
Movimiento de puntos de cableado	14	20	280	3360
Nuevo tendido de cableado	7	120	840	10080
			TOTAL REDUCCIÓN DE COSTOS	**13440**

Tabla 6.12 Reducción de costos con la red inalámbrica.

Los movimientos o cambios de puntos de red generan pérdida de tiempo laboral llamados también tiempos muertos, con la red inalámbrica habría un ahorro de tiempo aproximado de una a dos horas por semana por cada usuario, que multiplicado por 52 semanas al año, por el valor de la hora de trabajo, y por el número de empleados significaría un ahorro económico para Xerox.

Con el siguiente cálculo se indica el ahorro por año en costos por puntos muertos, considerando un valor de cinco dólares aproximadamente por cada hora de trabajo de un empleado de Xerox:

$$1\frac{hora}{seana} * 52\frac{semanas}{año} * 5\frac{dolares}{hora - usuario} * 90\ usuarios = 23400\frac{dolares}{año}$$

Al igual que en la red inalámbrica, el sistema de control de acceso también genera una reducción de costos, es así que Xerox actualmente contrata el servicio de seis guardias, esto implica salarios mensuales, con el sistema de control de acceso Xerox reduciría a un solo empleado de seguridad. En la tabla 6.13 se indica el ahorro anual en personal de seguridad.

REDUCCIÓN DE COSTOS CON EL SISTEMA DE CONTROL DE ACCESO				
DESCRIPCIÓN	**CANTIDAD**	**COSTO UNITARIO (USD)**	**COSTO MENSUAL (USD)**	**COSTO ANUAL (USD)**
Salario Guardias	6	320	1920	23040
			TOTAL REDUCCIÓN DE COSTOS	**23040**

Tabla 6.13 Reducción de costos con el sistema de control acceso.

6.4 EVALUACIÓN DEL PROYECTO

Para evaluar la viabilidad de este proyecto vamos a utilizar el indicador de flujo de caja y periodo de recuperación de la inversión.

6.4.1 FLUJO DE EFECTIVO O CAJA

El flujo de caja o de efectivo son los ingresos y gastos relacionados con el proyecto con el fin de determinar si son suficientes para soportar la deuda anual y retribuir adecuadamente el capital aportado por la empresa.

Tomando en cuenta los valores indicados en la tablas 6.1, 6.2, 6.3, 6.5, 6.6, 6.7, 6.12 y 6.13 en la tabla 6.14 se presenta el flujo de caja del proyecto

SIGNO	FLUJO DE EFECTIVO O CAJA	AÑO 0	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
-	Costos de operación de la red inalámbrica		36000	36000	36000	36000	36000
-	Costos de operación del sistema de control de acceso		15840	15840	15840	15840	15840
-	Costos de inversión de la red inalámbrica	6820					
-	Costos de inversión del sistema de control de acceso	4000.20					
-	Costos de instalación y configuración de la red inalámbrica	682.50					
-	Costos de instalación y configuración del sistema de control de acceso	300					
-	Costos de diseño de la red inalámbrica y del sistema de control de acceso	2000					
+	Reducción de costos de la red inalámbrica		13440	13440	13440	13440	13440
+	Reducción de costos del sistema de control		23040	23040	23040	23040	23040
+	Ahorro por tiempos muertos		23400	23400	23400	23400	23400
	FLUJO DE EFECTIVO O CAJA NETA	-13802.70	8040	8040	8040	8040	8040

Tabla 6.14 Flujo de efectivo o caja neta

En el siguiente ítem se determinan el periodo de recuperación de la inversión en base a los resultados obtenidos con el flujo de efectivo o caja neta, resumido en la tabla 6.14.

6.4.2 PERIODO DE RECUPERACIÓN DE LA INVERSIÓN

Consiste en medir el plazo de tiempo que se requiere para que los flujos de caja de una inversión recuperen su costo.

El periodo de recuperación de la inversión es un factor que determina el tiempo requerido para que Xerox pueda recuperar su inversión en el caso de llevar a cabo este proyecto. Para calcular este periodo se utiliza la siguiente fórmula:

$$PRI = Año\ anterior\ recuperacion\ total + \frac{Costo\ no\ recuperado\ principio\ de\ año_5}{Flujo\ de\ caja\ durante\ el\ año}$$

Año anterior a la recuperación total:

Se suman los Flujos de Caja a partir del año 0, hasta que el valor obtenido sea positivo:

-13802.70 +8040 + 8040 = 2277.30

Como el valor obtenido se hace positivo al segundo año, se tiene que el año anterior a la recuperación total va a ser el primer año.

Costo no recuperado al principio del año:

Como el año anterior a la recuperación total es el primer año, se va a tener un costo acumulado no recuperado a partir del año 0, tal como se muestra a continuación:

-13802.70 + 8040= -5762.70

Flujo de Caja durante el año:

Siendo el flujo de caja anual de: $ 8040, como se indica en la tabla 6.10, y aplicando la fórmula del PRI, se tiene que el período de recuperación de la inversión, es:

$$PRI = 1 + \frac{5762.70}{8040} = 1.71\ años$$

Con el resultado obtenido, se concluye que los costos generados por la implementación serán recuperados por Xerox en un tiempo aproximado de 1 año, 7 meses y 1 día.

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1 CONCLUSIONES

- ✓ Actualmente, dada la nueva tendencia en la que los empleados, pasan la mayor parte de su tiempo en movimiento trabajando con portátiles y PDAs, la tecnología inalámbrica se posiciona como una herramienta fundamental para mejorar la productividad en las empresas de hoy. Una red inalámbrica se caracteriza por su flexibilidad y movilidad, aspectos que benefician a los usuarios que laboran alejados de sus sitios de trabajo, permitiéndoles desplazarse fácilmente por las oficinas, ahorrando tiempo y complicaciones si disponen de un acceso transparente a la red de área local (LAN). La conexión es prácticamente instantánea y está disponible desde cualquier lugar con cobertura inalámbrica.

- ✓ Además con una conexión inalámbrica la información en línea está siempre disponible, la integración de nuevos dispositivos y aplicaciones en el entorno de la tecnología inalámbrica también mejora considerablemente y por último el tamaño de la red se puede modificar con facilidad, en respuesta a los distintos niveles de demanda conforme al crecimiento de la empresa.

- ✓ Debido a la gran cantidad de información relacionada con las redes inalámbricas y puesto que es difícil abarcar todas sus áreas, así como estándares y profundizar en cada una de ellos, en este trabajo fueron expuestos sus conceptos básicos y fundamentos, para de esta manera cumplir con el objetivo del presente proyecto, que es el brindar un aporte

que permita familiarizarse con este tipo de redes, su diseño, costos referenciales y los beneficios que aportan.

- ✓ El análisis de la situación actual de la red de Xerox del Ecuador constituye el referente a partir del cual se puede partir, pues al tener una visión general de su condición y parámetros de funcionamiento, permitió establecer las consideraciones de diseño y los requerimientos de la nueva red.

- ✓ El sistema de red actual, enfrenta un problema con respecto a la movilidad de usuarios, y escalabilidad. La posible integración de nuevos usuarios, y las cambiantes necesidades departamentales, que eventualmente modifican la ubicación física de los empleados (tiempos muertos), generan un gran problema en la creación de nuevos puntos de red, o movimiento de los mismos. Sin embargo, todos los dispositivos que conforman una red inalámbrica pueden ser trasladados sin ningún tipo de problema, por lo que no volverá a tener que realizar ese gasto.

- ✓ En una entidad privada, los datos con los que se trabajan son confidenciales, por lo que es primordial considerar el aspecto de la seguridad de esta información, si bien la desventaja fundamental de las redes inalámbricas es la seguridad, se han tomado las medidas de seguridad básicas.

- ✓ Como esquema básico de seguridad se plantea cambiar el SSID por default a uno que no tenga relación con el nombre de la institución y restringir su broadcast, esto hará a la red difícilmente identificable, luego se propone el filtrado de direcciones MAC y por último el método de encriptación WPA2.

- ✓ El estándar empleado para el diseño de la red inalámbrica es IEEE 802.11b puesto que especifica características adecuadas para el diseño, no obstante se deben tener en cuenta varios aspectos que hacen que dichas

características se vean limitadas y no se cumpla estrictamente lo que la teoría define. Por el efecto de atenuación causada por los materiales de los que está hecho el edificio, se considero necesario utilizar cuatro puntos de acceso, es decir, dos por planta para garantizar un acceso seguro y sin interrupciones a la red y calidad de la señal en la red inalámbrica de Xerox.

- ✓ Para el diseño se consideró las diferentes aplicaciones que utilizarán los usuarios de la red, basados en estadísticas del ancho de banda requerido por cada aplicación, con base en estos resultados, se concluye que al utilizar 802.11b, el ancho de banda supera lo necesario y se está garantizando un correcto desempeño de la red y de las aplicaciones que sobre esta correrán.

- ✓ Para el diseño de la red inalámbrica se realizó un análisis de diferentes tipos de equipos existentes en el mercado y se procedió a la elección de la mejor alternativa tomando en cuenta aspectos técnicos y económicos (Lynksys y DLINK), para lo cual se comparó sus características técnicas y se realizó un análisis de los precios del mercado actual y el costo que presenta el proyecto.

- ✓ El Edificio Matriz de Xerox del Ecuador al poseer un Sistema de Control de acceso monitoreado desde un computador central se beneficiará con una administración ágil, eficiente y costos de operación más bajos.

- ✓ Para el sistema de control de acceso se diseñaron dos soluciones utilizando la tecnología de identificación por radio frecuencia, pero optimizando el número de equipos empleados y disminuyendo así el costo de implementación sólo en una de ellos (opción dos, ver figura 4.9).

- ✓ La comunicación entre el sistema de Control de accesos y la red Inalámbrica no presenta complicaciones ya que se maneja a base de direcciones IP que se configura en el conversor EZL-300W Lite que integra

la tecnología RFID del sistema de control de acceso con la tecnología inalámbrica de la red.

- ✓ Finalmente se concluye que el presente proyecto brinda soluciones a los problemas existentes en la red actual y en el control de ingreso a las instalaciones del edificio Xerox, con costos de inversión admisibles, satisfaciendo a los usuarios y permitiéndole a la empresa en la medida de lo posible, ir a la par de los desafíos que representan los nuevas tendencias tecnológicas.

7.2 RECOMENDACIONES

Para un conveniente funcionamiento de la red y del Sistema de Control se realizan las siguientes recomendaciones:

- ✓ Antes de una futura implementación es importante revisar que los equipos adquiridos estén en óptimo funcionamiento (fallas de fábrica) tanto para la red inalámbrica como para el sistema de control de acceso, además la instalación y configuración de los equipos deben ser realizadas por personal capacitado.

- ✓ Previo a la instalación de la red inalámbrica, se deben realizar pruebas de campo en el lugar, ya que pueden existir factores que obliguen a efectuar correcciones en el diseño. Es recomendable verificar que no existan interferencias principalmente entre oficinas o edificios que se encuentran contiguos y comprobar si es factible hacer uso de los canales que se sugirieron.

- ✓ Dar capacitación técnica a los administradores de la red inalámbrica y del sistema de control de acceso, para que estos puedan dar un mejor mantenimiento y soporte a los usuarios. Informar a los usuarios de los servicios y beneficios de los sistemas, así como de sus funcionamientos;

además solicitar que se enmarquen en las políticas de seguridad establecidas.

- ✓ Implementar un sistema de procedimientos estandarizados para la configuración de los Puntos de Acceso y demás dispositivos inalámbricos instalados.

- ✓ Realizar un “Plan de Contingencias”, que contenga los procedimientos necesarios que se deben tomar cuando exista alguna falla en la red inalámbrica y/o en el sistema de control de acceso.

- ✓ Realizar pruebas comparativas al adquirir nuevos equipos inalámbricos, una vez escogida alguna marca o modelo tratar en lo posible que sea compatible con la infraestructura tecnológica ya instalada y evitar posibles caídas de la red inalámbrica.

- ✓ Crear manuales de configuración y administración para todos los dispositivos de la infraestructura inalámbrica y del sistema de control de acceso: switches, puntos de acceso, tarjetas, convertidores RS232 a RS485, etc. Además, en lo posible sería conveniente disponer de un punto de acceso como backup ya configurado.

- ✓ Dar a los usuarios capacitación sobre el uso de la tecnología inalámbrica Wi-Fi para crear una “cultura tecnología”; de tal forma que se ejecuten actividades que tengan relación con el mantenimiento de la red inalámbrica, como por ejemplo desconectar de la red inalámbrica cuando el equipo no se lo esté utilizando; es decir establecer políticas de uso y seguridad, puesto que son factores importantes tanto para la red inalámbrica como para el sistema de control de accesos.

- ✓ Es recomendable en el futuro la instalación y configuración de un servidor RADIUS para fortalecer la seguridad de la red inalámbrica.

- ✓ En el sistema de control de acceso es imprescindible mantener restringido el acceso a la base de datos del personal no autorizado, puesto que en estas se almacenan los códigos de las tarjetas RFDI

Todas estas recomendaciones se realizan con el objeto de garantizar el buen funcionamiento de la red y el sistema de control en conjunto en caso de ser implementado a futuro en la Compañía Xerox del Ecuador.

GLOSARIO

A

AC*K*. (Acuse de recibo). En comunicaciones entre computadores, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado. Si el terminal de destino tiene capacidad para detectar errores, el significado de ACK es “ha llegado y además ha llegado correctamente”.

Algoritmo. Una regla bien definida o proceso para llegar a la solución de un problema

Amplitud de la señal. Es una medida de la variación máxima del desplazamiento de onda electromagnética y en el tiempo

Ancho de banda. Es la longitud, medida en Hz, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal

Ancho de haz. Se refiere a la capacidad de direccionamiento de una antena, se usa de una manera específica respecto a una antena parabólica o Yagi y se define como el ángulo entre dos puntos de energía intermedia (-3dB) en cada extremo del lóbulo principal de radiación

API. (Application Programming Interface), Interfaz de Programación de Aplicaciones. Interfaz que permite la comunicación entre programas, redes y bases de datos.

B

Banda estrecha. Tipo de conexión que utiliza un ancho de banda muy reducido. La conexión más típica de banda estrecha que existe es la conexión por módem

telefónico (Dial-up). Un módem adapta las señales informáticas producidas por la computadora a otro tipo de señal que se puede introducir por la línea telefónica; así mismo, convierte la señal que llega a través de la línea telefónica en información comprensible para el ordenador.

Banda ISM (Industrial,Scientific and Medical). Son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. En la actualidad estas bandas han sido popularizadas por su uso en comunicaciones Wi-Fi y Bluetooth

Baudios. Es una unidad de medida, usada en telecomunicaciones, que representa el número de símbolos transmitidos por segundo en una red análoga.

Biometría. Es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. El término se deriva de las palabras griegas “bios” de vida y “metron” de medida

Bit de parada o paridad. Usado para indicar el fin de la comunicación de un solo paquete. Los valores típicos son 1, 1.5 o 2 bits

Bit. Es la unidad mínima de información empleada en informática, en cualquier dispositivo digital, o en la teoría de la información. Con él, podemos representar dos valores cuales quiera, como verdadero o falso,

Bluetooth. Es una especificación industrial para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,5 GHz.

Broadcast. Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Búfer. Es un espacio de memoria, en el que se almacenan datos para evitar que el programa o recurso que los requiere, ya sea hardware o software, se quede en algún momento sin datos

Bus de datos. En arquitectura de computadores, el bus es un sistema digital que transfiere datos entre los componentes de un ordenador o entre ordenadores. Está formado por cables o pistas en un circuito impreso, dispositivos como resistencias y condensadores además de circuitos integrados.

C

Campo eléctrico. Describe la interacción entre cuerpos y sistemas con propiedades de naturaleza eléctrica. Los campos eléctricos pueden tener su origen tanto en cargas eléctricas como en campos magnéticos variables.

Campo eléctrico. Es un ente físico que es representado mediante un modelo que describe la interacción entre cuerpos y sistemas con propiedades de naturaleza eléctrica

Canal de comunicación. El canal de comunicación es el medio de transmisión por el que viajan las señales portadoras de la información que pretenden intercambiar emisor y receptor. Es frecuente referenciarlo también como canal de datos.

CDMA, (Code Division Multiple Access). Acceso múltiple de división de código. La multiplexación por división de código, acceso múltiple por división de código. Es un término genérico para varios métodos de multiplexación o control de acceso al medio basados en la tecnología de espectro expandido.

Cisco. Es una empresa multinacional con sede en California - Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

Cobertura. Es el área geográfica que cubre una estación específica. Las estaciones transmisoras y las compañías de telecomunicaciones generan mapas de cobertura que le indican a sus usuarios el área en la ofrecen sus servicios.

Codificar. Aplicación de un algoritmo específico a los datos de forma que se altera la apariencia de estos, lo que los hace incomprensibles para las personas que no tienen autorización para ver la información.

Colisiones. Situación que ocurre cuando dos o más dispositivos intentan enviar una señal a través de un mismo canal al mismo tiempo. El resultado de una colisión es generalmente un mensaje confuso

Cortafuegos. Es un dispositivo de seguridad hardware o software que controla los accesos a la red local desde el exterior (típicamente internet).

D

dBi. Abreviatura para los decibeles de ganancia de la antena en referencia a la ganancia de una antena isotrópica. Una antena isotrópica es una antena teorica que radia con una simetría perfecta en las tres direcciones.

dBm. Abreviaturas para decibeles de energía en referencia a un miniwatt;0 dBm es 1 mW

Decibelios (dB). Abreviatura para decibel. Una unidad que expresa la relación de energía o voltaje en términos de ganancia o pérdida.

DHCP. Acrónimo del protocolo de configuración dinámica del Anfitrión. Proporciona un mecanismo para asignar direcciones IP en forma dinámica de manera que las direcciones se puedan reciclar cuando el equipo anfitrión ya no las necesite.

Dirección MAC. Dirección estandarizada de la capa enlace de datos que se requiere para cada puerto o dispositivo que se conecte a una LAN. Se las conoce también como direcciones de hardware, direcciones de capa MAC y direcciones físicas.

Dispersión. Es el fenómeno por el cual un conjunto de partículas que se mueve en una dirección determinada rebota sucesivamente con las partículas del medio por el que se mueve hasta perder una dirección privilegiada de movimiento.

Display. Es un dispositivo de ciertos aparatos electrónicos que permite mostrar información al usuario, creado a partir de la aparición de calculadoras, cajas registradoras e instrumentos de medida electrónicos en los que era necesario hacerlo.

E

Encoder. Es un codificador, también llamado codificador del eje, suele ser un dispositivo electromecánico usado para convertir la posición angular de un eje a un código digital,

Enrutador. (**direccionador**, **ruteador** o **encaminador**). Es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un router es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

ESS (Conjunto de servicios extendidos, Extended Service Set). Es una de las modalidades en las que se puede configurar una red local inalámbrica Wi-FI. Reciben este nombre las redes inalámbricas que están formadas por mas de un punto de acceso.

Estándar 100BaseT. Es el estándar de la red Ethernet que permite velocidades de transmisión de100 Mbps. Conocida también como Fast Ethernet.

Estándar 802.11. Conjunto de estándares de red de área local inalámbrica definidos por el IEEE. Entre estos estándares se encuentra el 802.11b, que es en el que se basa Wi-Fi.

Estándar 802.11i. Estándar IEEE que se enfoca en el mejoramiento de MAC 802.11 actual para mejorar la seguridad.

Estándar 802.1X. Estándar IEEE que define la operación de un puente MAC con el fin de proporcionar la capacidad de acceso a la red basado en puertos. Este estándar usa el protocolo de autenticación extensible (EAP) y se relaciona con el medio físico, ya sea Ethernet, Token Ring o una LAN inalámbrica.

Ethernet. Red de área local, que utiliza el protocolo TCP/IP

ETSI .Instituto Europeo de Normas de Telecomunicaciones. Organización creada para proponer estándares de comunicaciones

F

FCC. Comisión general de comunicaciones de los Estados Unidos que controla los estándares de transmisión electrónica y electromagnética

Frecuencia. Numero de ciclos, medidos en herts (1 por segundo), de la señal de corriente alterna por unidad de tiempo

H

Hertzio. Unidad de frecuencia

Hotspot. Es una zona de cobertura Wi-Fi, en el que un punto de acceso o varios proveen servicios de red a través de un Proveedor de Servicios de Internet Inalámbrico (WISP)

Hub. Es un equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás.

I

IAS de Microsoft (Internet Authentication Service). Servicio de autentificación de Internet es un componente del sistema operativo Windows Server que proporciona autentificaciónes de usuario, autorizaciones, contabilidad y auditoría.

Interferencia. Ruido indeseable en la comunicación que disminuye el desempeño de un enlace o evita que se pueda establecer el enlace.

IP Protocolo de Internet. Protocolo de nivel de red utilizado tanto por internet como por la mayoría de redes LAN cableadas e inalámbricas

IPSec. Es un protocolo de redes privadas virtuales que, aunque forma parte de la recomendación IPv6, es ampliamente utilizado también en las redes IPv4

IPX. Protocolo Novell o simplemente IPX es una familia de protocolos de red desarrollados por Novell y utilizados por su sistema operativo de red NetWare.

ISI, Inter-Symbol Interference. La distorsión causada por la energía de la señal en uno o más intervalos, que interfiere con la recepción de la señal en otro intervalo de modulación.

J

Jumper. Es un elemento para interconectar dos terminales de manera temporal sin tener que efectuar una operación que requiera herramienta adicional. Dicha unión de terminales cierra el circuito eléctrico del que forma parte.

L

Longitud de onda. Es la distancia que recorre la onda en el intervalo de tiempo

M

MAC. Control de acceso al medio. Es un conjunto de protocolos de las redes inalámbricas que controla como los distintos dispositivos se comparten el uso del espectro radioeléctrico

Modulación. Se llama modulación al hecho de distorsionar una señal eléctricao radioeléctrica para que contenga la información a transmitir. Al proceso contrario, extraer la información de una señal modulada se le llama demodulación

N

NAT. Acrónimo de traducción de direcciones de red. Mecanismo para reducir la necesidad de direcciones IP únicas globalmente. NAT permite que una organización que tiene direcciones que no son únicas globalmente se conecten a Internet, mediante la traducción de esas direcciones en direcciones direccionables en el espacio global.

NIS, (Network Information System). Sistema de Información de Red, es el nombre de un protocolo de servicios de directorios cliente-servidor desarrollado por Sun Microsystems para el envío de datos de configuración en sistemas

distribuidos tales como nombres de usuarios y hosts entre computadoras sobre una red.

Nodo. Cada una de las máquinas dentro de una red es un nodo, y si la red es Internet, cada servidor constituye también un nodo.

O

OSI (Open System Interconnection). Modelo de referencia de Interconexión de Sistemas Abiertos, fue el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, fue un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

P

PAM, Pluggable Authentication Modules). Es un mecanismo de autenticación flexible que permite abstraer las aplicaciones y otro software del proceso de identificación.

Paridad. Es una forma sencilla de verificar si hay errores en la transmisión serial. Existen cuatro tipos de paridad: par, impar, marcada y espaciada**.**

Pigtail. Un pigtail o latiguillo es un trozo de cable que lleva en cada uno de sus extremos un conector. Su utilidad es la de unir un dispositivo wireless (punto de acceso, tarjeta pcmcia, tarjeta pci, etc) a una antena wireless

PoE. (Power over). Ethernet La alimentación a través de Ethernet, es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre al dispositivo de red como, por ejemplo, un teléfono IP o una cámara de red, usando el mismo cable que se utiliza para una conexión de red.

Propagación. Se llama propagación al conjunto de fenómenos físicos que conducen a las ondas del transmisor al receptor.

Proxy. Referente a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP

Puerto de comunicaciones. Interfaz de comunicación de datos

Punto de acceso (AP). Un punto de acceso inalámbrico en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos

Q

QoS o Calidad de Servicio (Quality of Service,). Son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado. Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de video o voz.

R

Rack. Un rack es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones. Sus medidas están normalizadas para que sea compatible con equipamiento de cualquier fabricante.

Radio frecuencia. Se refiere a las comunicaciones inalámbricas con frecuencias por debajo de los 300Ghz.

RC4. Algoritmo de seguridad que usa WEP.

Red troncal. Parte de una red que actúa como la ruta principal del tráfico que con frecuencia se origina en una red y está destinado para otras redes**.**

Reset. Se conoce como reset a la puesta en condiciones iniciales de un sistema.

S

Sensor. Es un aparato capaz de transformar magnitudes físicas o químicas, llamadas variables de instrumentación, en magnitudes eléctricas.

Servidor. Se trata de un software que permite ofrecer servicios remotos a sus usuarios. También puede recibir el nombre de servidor el propio computador donde esta instalado el software de servidor

SNMP. Protocolo de administración de red que se usa casi exclusivamente en las redes TCP/IP. SNMP proporciona los medios para supervisar y controlar los dispositivos de red, además de manejar las configuraciones, la recolección de estadísticas el desempeño y la seguridad.

SNR, (Signal-To-Noise Ratio). La relación señal/ruido se define como el margen que hay entre la potencia de la señal que se transmite y la potencia del ruido que la corrompe. Este margen es medido en decibelios.

Spoofing. Técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

SSL. Secure Sockets Layer .Protocolo de Capa de Conexión Segura. Protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

T

Thinkpad. Es una marca de computadoras portables Laptops originalmente diseñada, manufacturada y vendida por IBM.

Transceptores. Dispositivo que realiza, dentro de una misma caja o chasis, funciones tanto de trasmisión como de recepción, utilizando componentes de circuito comunes para ambas funciones.

U

UDP. Protocolo de datagramas de usuario a nivel de capa transporte

V

VLAN. Red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local.

VPN. Virtual Private Network, Red Privada Virtual. Hace referencia a las soluciones que permite crear redes completamente privadas en cuanto a seguridad y confidencialidad utilizando para ello infraestructuras como Internet o redes inalámbricas.

W

WECA. (Wireless Ethernet Compatibility Alliance).Wireless Ethernet Compability Alliance, Alianza de Compatibilidad Ethernet Inalámbrica. Es una asociación de fabricantes de equipos de red con el objetivo de fomentar la tecnología inalámbrica y asegurar la compatibilidad de equipos

Wiegand. Tecnología que permite transmitir datos de un identificador (tarjeta) a otro dispositivo alejados entre si, como, por ejemplo, un lector y la central de control de accesos. El protocolo Wiegand es ampliamente utilizado por la mayor parte de los fabricantes porque permite la transmisión de información a través de un par de cobre que se acompaña de la alimentación para el dispositivo de lectura si afectar por ello a los dato

Wi-Fi (Wireless Fidelity), Fidelidad Inalámbrica. Es una marca creada por WECA con el objetivo de fomentar la tecnología inalámbrica

REFERENCIAS BIBLIOGRÁFICAS

TEXTOS

- ✓ CABALLAR JOSÉ A., “Wi-Fi ¿Cómo construir una red inalámbrica?”, 2ª ed., México, Ed. Alfaomega Grupo editor, 2005.
- ✓ GAST MATTHEW S., “Redes Wireless 802.11”, 1ª ed., Español, Anayamultimedia, España 2006.
- ✓ REID NEIL, SEIDE RON, “802.11 (Wi-Fi)”, 1ª ed., Español, McGraw-Hill Interamericana Editores, S.A., 2004
- ✓ VLADIMIROV ANDREW A., GAVRILENKO KONSTANTIN V., MIKHAILOVSKY ANDREI A., “Hacking Wireless”, 1ª ed., Ed. Anayamultimedia, España 2004.

INTERNET

- ✓ www.cinit.org.mx/articulo.php?idArticulo=29
- ✓ www.configurarequipos.com/doc331.html
- ✓ www.ds3comunicaciones.com/sectorial.html
- ✓ www.e-advento.com/tecnologia/wlan_intro.php
- ✓ www.jantek.com/Spanish/overviewjas.htm
- ✓ www.kimaldi.com/
- ✓ www.larepublica.com/internet/inalambrica

- ✓ www.lat.3com.com/lat/technology/technnical.papers/wireless.
- ✓ www.linksysbycisco.com/EU/es/support/WRT54G/download
- ✓ www.tdsi.co.uk/es/about_access.htm
- ✓ www.wikipedia.org/wiki/Antena