

# **ESCUELA POLITÉCNICA NACIONAL**

## **FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA**

**“DISEÑO E IMPLEMENTACION DE UN SISTEMA DE SEGURIDAD  
CONTRA INTRUSOS PARA EL LABORATORIO DE INFORMATICA  
UTILIZANDO EL ESTANDAR IEEE 802.15.4 ZIGBEE COMO  
TECNOLOGIA DE COMUNICACIÓN”**

**PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN  
ELECTRÓNICA Y TELECOMUNICACIONES**

**CEPEDA ORTIZ GABRIELA ROCIO**

**[gabriela.cepeda@hotmail.com](mailto:gabriela.cepeda@hotmail.com)**

**GUERRA CHICANGO JORGE ESTEBAN**

**[kdtguerrag@gmail.com](mailto:kdtguerrag@gmail.com)**

**DIRECTOR: DR. LUIS CORRALES**

**[luisco5049@yahoo.com](mailto:luisco5049@yahoo.com)**

**Quito, Julio 2009**

## DECLARACIÓN

Nosotros, Gabriela Rocío Cepeda Ortiz y Jorge Esteban Guerra Chicango, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he 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 Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normativa institucional vigente.

---

Gabriela Rocío Cepeda Ortiz

---

Jorge Esteban Guerra Chicango

## CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Gabriela Roció Cepeda Ortiz y Jorge Esteban Guerra Chicango, bajo mi supervisión.

---

Dr. Luis Corrales

DIRECTOR DEL PROYECTO

## AGRADECIMIENTO

Mi gran agradecimiento va para todos los miembros de mi familia: mi mamá, mi abuelita, mis hermanos y mis dos tías queridas, que siempre han aportado con su gran sabiduría, amor, comprensión, cariño, fuerza y sobre todo siempre han sabido darme el aliento necesario para dar cada paso y cosechar cada éxito en mi vida.

Quiero agradecer a mi compañero de tesis, más que un compañero un gran amigo, que me ha dado siempre una mano en todo. Gracias George por compartir conmigo el trabajo para sacar adelante este proyecto y hoy disfrutar del fruto del mismo.

Agradezco a todos, todos mis amigos, perdón por no poner cada uno de sus nombres, no se me puede escapar ninguno y no me alcanzaría una sola página para nombrarlos, pero los llevo en las páginas imborrables de la memoria y del corazón. A ustedes AMIGOS que me han dado la fuerza para continuar cuando sentía que quería desmayar antes de llegar a la meta, gracias por hacer de la poli un lugar muy querido, gracias por estar a mi lado, por ser la mano extendida, la sonrisa, la confianza y por ser el complemento que endulza la vida.

A todos aquellos buenos maestros, esos que saben sembrar y dejar huellas en la mente y en el corazón. Gracias por dar todo su conocimiento y experiencia en contribución a mi formación personal y profesional. Y en especial al Doctor Luis Corrales por su acertada dirección en este proyecto, por ser más que un gran profesional una gran persona.

Y finalmente agradezco a todas las personas especiales que han estado presentes en mi vida mientras liberaba cada batalla que me acercaba más hacia esta gran meta trazada.

No sé si este es el fin o el principio pero siempre espero tenerlos a mi lado, mil gracias a todos.

Gabriela R. Cepeda Ortiz

## AGRADECIMIENTO

Mi agradecimiento con todo el corazón a aquel quien es rey de reyes y señor de señores, a aquel cuyo nombre es sobre todo nombre, Yeshua, quien me ha enseñado a ser esforzado y valiente, y por su voluntad perfecta me ha permitido culminar este pequeño sueño de ser un profesional. Gracias mi señor.

Agradezco a mis padres Jorge y Judith por haberme brindado su apoyo totalmente incondicional, por sus consejos, sus enseñanzas, por su constancia para guiarme y por su amor para comprenderme, gracias por estar a mi lado. A mis hermanos Nelson, Cristi y Mishel por estar también junto a mí en todos los momentos en los cuales reímos y también en los que lloramos, gracias siempre estarán en mis pensamientos.

Mi agradecimiento a mi gordita quien estuvo desde el principio hasta el final de mi carrera, apoyándome, levantando mi ánimo en esos momentos difíciles, orando y sobre todo por su amor puro, sincero y verdadero.

A todos mis amigos con quienes he compartido y he disfrutado momentos muy hermosos de la vida, por sus consejos y fuerzas para continuar, muchas gracias por sus oraciones, no me olvidare nunca de todo lo que vivimos.

Agradezco a Gaby por trabajar a mi lado en este último proyecto como compañeros universitarios, su esfuerzo nos ha llevado a terminar exitosamente y orgullosamente este trabajo, al Dr. Luis Corrales por su guía invaluable en este proyecto como director, profesor y gran profesional.

Tal vez yo no pueda recompensar su ayuda pero muchas gracias a todos.

Jorge E. Guerra Chicango

## DEDICATORIA

Este Proyecto de Titulación va dedicado a mi mamita, por su lucha incondicional de toda una vida, por los grandes sacrificios, por el apoyo, por la comprensión, por sus desvelos y sobre todo por el gran amor de siempre que me ha regalado a lo largo de este sinuoso camino que conduce a mis sueños. Mamita, espero siempre tenerte a mi lado dándome aliento y luz para seguir adelante.

A mi abuelita por todo el cariño y preocupación.

A mis tías (Patricia y Jenny) que han cuidado de mi desde pequeña y aún están a mi lado para ayudarme. Las quiero mucho y a sus familias

A Isabel, mi hermana, mi mejor amiga, mi cómplice, mi confidente y todo y a Francisco, mi pequeño hermano, gracias a los dos por la compañía, la paciencia y por creer siempre en mí.

A mis dos grandes amores con quienes caminaré el resto de mi vida y quienes estoy segura que me traerán tantas alegrías como la que estoy cosechando ahora. Gracias por estar dándome tanto cariño y felicidad.

A todos ustedes, de todo corazón, les dedico este fruto del esfuerzo y la constancia. Espero que sigan siendo las luces que me guían por el gran sendero de la vida. Los quiero mucho.

Gabriela R. Cepeda Ortiz

## DEDICATORIA

Este proyecto de titulación va dedicado a mi familia, quienes permitieron que lo pueda culminar pues me brindaron todo su amor y ayuda.

Papis lo que anhelaron esta cumplido, ya soy ingeniero.

A mi gordita que también esperaba el día de mi graduación, el tiempo se ha cumplido.

Quisiera dedicárselo a Dios pero esto ya fue suyo desde antes, gracias, este es el final de esta bendición tuya.

Jorge E. Guerra Chicango

## CONTENIDO

DECLARACION.....	I
CERTIFICACION.....	II
AGRADECIMIENTO.....	III
DEDICATORIA.....	V
CONTENIDO.....	VII
FIGURAS.....	XIV
TABLAS.....	XIX
RESUMEN.....	XXI
PRESENTACION.....	XXII
CAPITULO 1 .....	1
INTRODUCCION AL ESTANDAR IEEE 802.15.4 ZIGBEE .....	1
1.1  ESPECIFICACIONES DEL ESTANDAR IEEE 802.15.4.....	1
1.1.1  CARACTERISTICAS GENERALES DE REDES LR-WPANS:.....	1
1.1.2  COMPONENTES DEL ESTANDAR IEEE 802.15.4 .....	2
1.1.3  TOPOLOGIAS DE RED.....	3
1.1.3.1  Formación de una red con topología en estrella .....	4
1.1.3.2  Formación de una red punto a punto .....	4
1.1.4  ARQUITECTURA.....	6
1.1.4.1  Capa PHY .....	8
1.1.4.1.1  ED (Energy Detection) .....	9
1.1.4.1.2  LQI (Link Quality Indicator) .....	9
1.1.4.1.3  CCA (Clear Channel Assessment) .....	9
1.1.4.1.4  Rango operativo de frecuencias .....	10
1.1.4.1.5  Canales.....	10
1.1.4.1.6  Períodos LIFS (Minimum Long Interframe Spacing) y SIFS (Short Interframe Spacing) .....	11
1.1.4.1.7  Potencia.....	12
1.1.4.1.8  Formato PPDU .....	12

1.1.4.2	Subcapa MAC .....	14
1.1.4.2.1	Administración de Beacons .....	15
1.1.4.2.2	Acceso al canal.....	17
1.1.4.2.3	Asociación y Desasociación .....	19
1.1.4.2.4	Transferencia de datos .....	19
1.1.4.2.5	Consumo de potencia.....	21
1.1.4.2.6	Seguridad .....	21
1.1.4.2.7	Periodos LIFS Y SIFS .....	22
1.1.4.2.8	Estructura de tramas .....	23
1.1.4.2.9	Formación de una PAN .....	25
1.2	ESPECIFICACIONES DE LA ALIANZA ZIGBEE.....	26
1.2.1	ARQUITECTURA.....	26
1.2.2	CAPA DE APLICACION .....	27
1.2.2.1	Subcapa de Soporte.....	27
1.2.2.1.1	Formato de las Tramas PDU APS.....	28
1.2.2.2	Estructura de Aplicación (AF).....	28
1.2.2.2.1	Servicio de Parejas Clave-Valor .....	29
1.2.2.2.2	Servicio de Mensajes .....	29
1.2.2.3	Objetos de dispositivos ZigBee .....	29
1.2.2.3.1	Gestión de Descubrimiento.....	29
1.2.2.3.2	Gestión de Enlace .....	30
1.2.2.3.3	Gestión de Seguridad.....	30
1.2.3	FUNDAMENTOS DE COMUNICACIÓN DE LA CAPA DE APLICACIÓN .....	31
1.2.3.1	Perfiles .....	31
1.2.3.2	Objeto (Endpoint) .....	31
1.2.3.3	Atributo .....	31
1.2.3.4	Clusters .....	32
1.2.3.5	Enlace (Binding) .....	32
1.2.4	CAPA DE RED.....	32
1.2.4.1	Formato de las tramas PDU NWK.....	33
1.2.4.2	Funcionalidades .....	33

1.2.4.2.1	Formación de la red .....	34
1.2.4.2.2	Modelo de transferencia de tramas.....	35
CAPITULO 2 .....		38
DISEÑO E IMPLEMENTACION DEL HARDWARE DEL SISTEMA.....		38
2.1	TOPOLOGIA FISICA .....	38
2.2	TOPOLOGIA LOGICA .....	39
2.3	LUGAR DE INSTALACION DE LOS EQUIPOS .....	39
2.4	CARACTERISTICAS DE LOS ELEMENTOS UTILIZADOS .....	41
2.4.1	DISPOSITIVOS XBEE .....	41
2.4.1.1	Especificaciones.....	42
2.4.1.1.1	Características generales.....	42
2.4.1.1.2	Performance .....	43
2.4.1.1.3	Seguridad y Networking .....	43
2.4.1.1.4	Requerimientos de energía.....	43
2.4.1.1.5	Antena.....	43
2.4.1.1.6	Aprobaciones regulatorias .....	44
2.4.1.1.7	Dimensiones.....	44
2.4.1.2	Descripción de los pines .....	45
2.4.1.3	Notas de diseño .....	45
2.4.1.4	Kit de desarrollo .....	46
2.4.1.5	Software y hardware para la configuración de los dispositivos Xbee	47
2.4.2	MICROCONTOLADOR PIC 16F877A .....	48
2.4.2.1	Especificaciones.....	49
2.4.2.2	Software y hardware para programación del PIC 16F877A .....	51
2.5	DISEÑO DEL HARDWARE .....	52
2.5.1	DISEÑO DEL CEREBRO DEL SISTEMA.....	52
2.5.1.1	Construcción del cerebro del sistema .....	54
2.5.1.1.1	PIC 16F877A .....	56
2.5.1.1.2	Dispositivo Xbee .....	59
2.5.1.2	Ruteo del cerebro del sistema.....	60

2.5.1.3	Construcción de la interfaz de usuario .....	61
2.5.1.4	Ruteo de la interfaz de usuario.....	63
2.5.2	PERIFERICOS DEL SISTEMA .....	64
2.5.2.1	Construcción de los periféricos del sistema .....	65
2.5.2.1.1	Dispositivo Xbee .....	66
2.5.2.2	Ruteo de los periféricos del sistema.....	70
2.6	FUENTE DE ENERGIA.....	71
2.7	IMPLEMENTACION DEL HARDWARE .....	73
CAPITULO 3.....		77
DESARROLLO DEL SOFTWARE DE SOPORTE.....		77
3.1	DISEÑO DEL SOFTWARE DEL CEREBRO DEL SISTEMA.....	77
3.1.1	MICROCONTROLADOR PIC 16F877A.....	77
3.1.2	PERIFERICOS.....	81
3.1.2.1	LCD.....	81
3.2	DISEÑO DEL SOFTWARE DE LA CENTRAL DE CONTROL “SECURITY SOFT”82	
3.2.1	DESCRIPCIÓN .....	82
3.2.2	LENGUAJE DE PROGRAMACIÓN .....	82
3.2.3	COMUNICACIÓN SERIAL.....	83
3.2.3.1	Conexión del Microcontrolador PIC al Puerto Serie del PC .....	84
3.2.3.2	El Cableado .....	84
3.2.4	EMPAQUETAMIENTO DEL SOFTWARE .....	85
3.2.4.1	Instalación del Software.....	86
3.2.5	FUNCIONAMIENTO Y CODIGO DEL SOFTWARE DE MONITOREO .....	87
3.2.6	SEGURIDADES.....	100
CAPITULO 4 .....		101
PRUEBAS Y RESULTADOS.....		101

4.1	PRUEBAS DE COMUNICACIÓN DE DATOS .....	101
4.1.1	PRUEBA BÁSICA DE COMUNICACIÓN PC-XBEE .....	102
4.1.2	PRUEBA DE COMUNICACIÓN XBEE-XBEE.....	103
4.1.2.1	Prueba con línea de vista (Outdoor).....	103
4.1.2.2	Prueba sin línea de vista (Indoor).....	106
4.2	PRUEBAS DE PROCESAMIENTO DE DATOS .....	113
4.2.1	PRUEBA DE FUNCIONAMIENTO DE PERIFERICOS .....	114
4.2.2	PRUEBA DE FUNCIONAMIENTO DEL CEREBRO DEL SISTEMA 115	
4.3	PRUEBAS DE CONSUMO DE CORRIENTE .....	118
4.3.1	CONSUMO DE CORRIENTE DEL CEREBRO DEL SISTEMA....	119
4.3.2	CONSUMO DE CORRIENTE DEL INTERFAZ DE USUARIO.....	119
4.3.3	CONSUMO DE CORRIENTE DE LOS PERIFERICOS DEL SISTEMA .....	119
4.4	DETALLE DE COSTOS QUE INCURRIERON EN LA IMPLEMENTACIÓN DEL PROYECTO.....	120
4.4.1	COSTO DE CONSTRUCCION DEL CEREBRO DEL SISTEMA (Tabla 4.1):.....	121
4.4.2	COSTO DE CONSTRUCCION DEL INTERFAZ DE USUARIO (Tabla 4.2):.....	121
4.4.3	COSTO DE CONSTRUCCION DE LOS PERIFERICOS DEL SISTEMA (Tabla 4.3): .....	122
4.4.4	COSTO DE CONSTRUCCION DE LA FUENTE DE ENERGIA (Tabla 4.4):.....	122
4.4.5	COSTOS VARIOS (Tabla 4.5): .....	123
CAPITULO 5 .....		124
POSIBILIDADES DE AMPLIACIÓN A OTROS AMBIENTES CERCANOS ...		124
5.1	DESCRIPCIÓN .....	124
5.2	TOPOLOGIA FISICA DEL SISTEMA.....	126

5.3	TOPOLOGIA LOGICA DEL SISTEMA.....	126
5.4	REQUERIMIENTOS DE HARDWARE.....	126
5.4.1	DISPOSITIVOS ZIGBEE .....	126
5.4.1.1	Dispositivos Router .....	126
5.4.1.1.1	Especificaciones .....	127
5.4.1.2	Dispositivos Terminales .....	129
5.5	ANALISIS DE LOS SITIOS .....	129
5.5.1	CENTRO DE MONITOREO (GARITA DE LOS GUARDIAS) .....	130
5.5.1.1	Lugar de instalación de los equipos .....	130
5.5.2	LABORATORIO DE INSTRUMENTACION .....	131
5.5.2.1	Topología Física.....	131
5.5.2.2	Topología Lógica.....	131
5.5.2.3	Lugar de instalación de los equipos .....	131
5.5.3	LABORATORIO DE TRANSMISIÓN Y SISTEMAS RADIANTES	132
5.5.3.1	Topología Física.....	132
5.5.3.2	Topología Lógica.....	132
5.5.3.3	Lugar de instalación de los equipos .....	133
5.6	CAMBIOS EN EL SISTEMA DE MONITOREO .....	133
5.6.1	REQUERIMIENTOS DE SOFTWARE .....	133
5.7	COSTO DE LA AMPLIACION DEL SISTEMA DE SEGURIDAD .....	136
5.7.1	COSTO DE CONSTRUCCION DEL CEREBRO DEL SISTEMA..	137
5.7.2	COSTO DE CONSTRUCCION DEL INTERFAZ DE USUARIO ...	137
5.7.3	COSTO DE CONSTRUCCION DE LOS PERIFERICOS DEL SISTEMA .....	138
5.7.4	COSTO DE CONSTRUCCION DE LA FUENTE DE ENERGIA ...	139
5.7.5	COSTOS VARIOS .....	140

CAPITULO 6 .....	141
CONCLUSIONES Y RECOMENDACIONES .....	141
6.1    CONCLUSIONES .....	141
6.2    RECOMENDACIONES .....	142
REFERENCIAS BIBLIOGRAFICAS.....	143
ANEXOS.....	144

## FIGURAS

Figura 1.1 Topología en estrella.....	4
Figura 1.2 Topología Punto a Punto.....	6
Figura 1.3 Red Multicluster.....	6
Figura 1.4 Arquitectura IEEE 802.15.4.....	7
Figura 1.5 Componentes e interfaces de la capa PHY.....	8
Figura 1.6 Períodos LIFS y SIFS.....	11
Figura 1.7 Paquete PPDU.....	13
Figura 1.8 Componentes de la subcapa MAC.....	15
Figura 1.9 Supertrama IEEE 802.15.4.....	16
Figura 1.10 Supertrama con porción activa e inactiva.....	16
Figura 1.11 CAP y CFP.....	17
Figura 1.12 Ejemplo de supertrama.....	17
Figura 1.13 Transferencia de datos a un coordinador Beacons-enable.....	19
Figura 1.14 Transferencia de datos a un coordinador Nonbeacon-enable.....	20
Figura 1.15 Transmisión de datos desde un coordinador Beacons-Enable.....	20
Figura 1.16 Transmisión de datos desde un coordinador Nonbeacons-Enable...	21
Figura 1.17 Períodos SIFS y LIFS.....	22
Figura 1.18 Estructura de trama beacon.....	23
Figura 1.19 Estructura de trama de datos.....	24
Figura 1.20 Estructura de trama de confirmación.....	24
Figura 1.21 Estructura de trama de comando MAC.....	25
Figura 1.22 Arquitectura ZigBee.....	27
Figura 1.23 Formato de Trama APS.....	28
Figura 1.24 Formato de la Trama NWK.....	33

Figura 1.26 Transferencia de datos hacia el coordinador (CSMA/CA).....	36
Figura 1.27 Transferencia de datos desde el coordinador (beacon-enable) .....	36
Figura 1.28 Transferencia de datos desde el coordinador (CSMA/CA).....	37
Figura 2.1 Topología física en estrella .....	38
Figura 2.2 Lugar de instalación de los equipos .....	40
Figura 2.3 Lugar de instalación del sensor de movimiento 1 .....	40
Figura 2.4 Lugar de instalación del sensor de movimiento 2 .....	41
Figura 2.5 Dimensiones de los dispositivos Xbee .....	44
Figura 2.6 Kit de desarrollo Xbee .....	46
Figura 2.7 Software X-CTU .....	47
Figura 2.8 Módulo de desarrollo USB .....	48
Figura 2.9 Distribución de pines del microcontrolador PIC 16F877A .....	49
Figura 2.10 Conexión del cristal externo para el microcontrolador 16F877A.....	50
Figura 2.11 Software para la programación del PIC 16F877A .....	51
Figura 2.12 Hardware para la programación del PIC 16F877A.....	51
Figura 2.13 Esquema de diseño del cerebro del sistema.....	55
Figura 2.14 Esquema del circuito del cerebro del sistema .....	56
Figura 2.15 Circuito básico de reset para el microcontrolador PIC16F877A.....	59
Figura 2.16 Esquema de conexión Xbee-PIC16F877A.....	59
Figura 2.17 Ruteo del cerebro del sistema.....	61
Figura 2.18 Esquema de diseño para controlar contraste y baklite del LCD.....	62
Figura 2.19 Conexión en modo directo de cable multipar .....	62
Figura 2.20 Esquema del circuito de la interfaz de usuario.....	63
Figura 2.21 Ruteo de la interfaz de usuario .....	64
Figura 2.22 Esquema de diseño de los periféricos del sistema.....	65
Figura 2.23 Esquema del circuito de los periféricos del sistema.....	66

Figura 2.24 Ruteo de los periféricos del sistema.....	71
Figura 2.25 Esquema del circuito de la fuente de energía .....	72
Figura 2.26 Ruteo de la fuente de energía .....	73
Figura 2.27 Cajas metálicas portadoras de los circuitos .....	73
Figura 2.28 Circuito y caja del cerebro del sistema.....	74
Figura 2.29 Circuito y caja del interfaz de usuario.....	75
Figura 2.30 Circuito y caja de los periféricos del sistema.....	75
Figura 3.1 Diagrama del funcionamiento del Microcontrolador .....	79
Figura 3.2 Esquema general del proyecto.....	82
Figura 3.3 Conexión del microcontrolador al PC .....	84
Figura 3.4 Distribución de pines en el conector DB9.....	85
Figura 3.5 Proceso de Instalación del Software en la PC .....	87
Figura 3.6 Pantalla Principal del Software de Monitoreo .....	88
Figura 3.7 Formulario Splash .....	88
Figura 3.8 Cuadro de Autenticación para inicio de sesión .....	90
Figura 3.9 Mensaje de error en la autenticación .....	90
Figura 3.10 Cambio de clave.....	91
Figura 3.11 Ingreso de la nueva clave .....	91
Figura 3.12 Diagrama de la Pantalla de Autenticación.....	92
Figura 3.13 Entorno del software “Security Soft”.....	93
Figura 3.14 Sistema de Monitoreo Alarmado .....	94
Figura 3.15 Menú Opciones .....	95
Figura 3.16 Menú Vista .....	95
Figura3.17 Opción Activar Sistema .....	96
Figura 3.18 Opción desactivar Sistema de Monitoreo.....	97
Figura 3.19 Cerrar puerto Comm .....	97

Figura 3.20 Diagrama de la pantalla de monitoreo.....	98
Figura 4.1 Placa de desarrollo USB .....	101
Figura 4.2 Placa de desarrollo RS-232 .....	101
Figura 4.3 Configuración modulo de PC del software X-CTU .....	102
Figura 4.4 Proceso Test/Query .....	102
Figura 4.5 Diagrama para prueba con línea de vista.....	103
Figura 4.6 Medida de recepción de paquetes y RSSI a 30 m .....	104
Figura 4.7 Medida de recepción de paquetes y RSSI a 60 m .....	104
Figura 4.8 Medida de recepción de paquetes y RSSI a 200 m .....	105
Figura 4.9 Lugar de instalación de los equipos para Prueba 1.....	106
Figura 4.10 Medida de recepción de paquetes y RSSI para Prueba 1.....	107
Figura 4.11 Lugar de instalación de los equipos para Prueba 2.....	108
Figura 4.12 Medida de recepción de paquetes y RSSI para Prueba 2.....	108
Figura 4.13 Lugar de instalación de los equipos para Prueba 3.....	109
Figura 4.14 Medida de recepción de paquetes y RSSI para Prueba 3.....	109
Figura 4.15 Lugar de instalación de los equipos para Prueba 4.....	110
Figura 4.16 Medida de recepción de paquetes y RSSI para Prueba 4.....	111
Figura 4.17 Lugar de instalación de los equipos para Prueba 5.....	112
Figura 4.18 Medida de recepción de paquetes y RSSI para Prueba 5.....	112
Figura 4.19 Cadena de caracteres enviados por un periférico .....	114
Figura 4.20 Sistema de monitoreo activado .....	118
Figura 5.1 Diagrama General del Sistema de Seguridad Extendido .....	125
Figura 5.2 Red Malla que forman los dispositivos .....	127
Figura 5.3 Dimensiones de los dispositivos Xbee-PRO .....	129
Figura 5.4 Centro de monitoreo (garita entrada Eléctrica-Química) .....	130
Figura 5.5 Diagrama del Laboratorio de Instrumentación .....	131

Figura 5.6 Diagrama del Laboratorio de Transmisión .....	132
Figura 5.7 Diagrama de flujo del funcionamiento del programa "Security Soft..."	134
Figura 5.8 Vista de los diferentes laboratorios .....	136

## TABLAS

Tabla 1.1 Rango operativo de frecuencias .....	10
Tabla 1.2 Canales .....	11
Tabla 1.3 Periodos mínimos LIFS y SIFS .....	12
Tabla 1.4 Longitud del campo preámbulo .....	13
Tabla 1.5 Longitud de campo SFD .....	14
Tabla 1.6 Longitud del campo longitud trama .....	14
Tabla 2.1 Especificaciones generales de los dispositivos Xbee .....	42
Tabla 2.2 Descripción de los pines de los dispositivos Xbee .....	45
Tabla 2.3 Especificaciones básicas del microcontrolador PIC 16F877A .....	49
Tabla 2.4 Osciladores externos para el microcontrolador PIC 16F877A .....	50
Tabla 2.5 Programación del dispositivo Xbee del cerebro del sistema .....	60
Tabla 2.6 Programación en común para los dispositivos Xbee de los periféricos .....	68
Tabla 2.7 Programación Xbee para el sensor de movimiento 1 .....	69
Tabla 2.8 Programación Xbee para el sensor de movimiento 2 .....	69
Tabla 2.9 Programación Xbee para el sensor magnético 1 .....	69
Tabla 2.10 Programación Xbee para el sensor magnético 2 .....	70
Tabla 2.11 Programación Xbee para el sensor magnético 3 .....	70
Tabla 2.12 Medias de las cajas portadoras de los circuitos .....	74
Tabla 3.1 Tabla de comandos más utilizados para manejar un LCD .....	81
Tabla 3.2 Propiedades del Componente Serial .....	84
Tabla 3.3 Disposición de los pines en el ordenador .....	85
Tabla 4.1 Costo de construcción del cerebro del sistema .....	121
Tabla 4.2 Costo de construcción del interfaz de usuario .....	121
Tabla 4.3 Costo de construcción de los periféricos del sistema .....	122

Tabla 4.4 Costo de construcción de la fuente de energía .....	122
Tabla 4.5 Costos varios.....	123
Tabla 5.1 Especificaciones generales de los dispositivos ZigBee.....	127
Tabla 5.2 Costo de construcción del cerebro del sistema .....	137
Tabla 5.3 Costo de construcción del interfaz de usuario .....	137
Tabla 5.4 Costo de construcción de circuito para puerta .....	138
Tabla 5.5 Costo de construcción circuito para pasillo .....	138
Tabla 5.6 Costo de construcción circuito para ventana .....	139
Tabla 5.7 Costo de construcción de la fuente de energía .....	139
Tabla 5.8 Costos varios.....	140

## RESUMEN

En este trabajo se diseña y construye un sistema de seguridad para el laboratorio de informática del Departamento de Electrónica, Telecomunicaciones y Redes de Información, ubicado en el sexto piso del edificio de Eléctrica-Química de la EPN. Se ha escogido este laboratorio por la cantidad de equipos que posee y por el sinnúmero de servicios que presta a los estudiantes y consecuentemente de gran afluencia de gente.

Para realizar el diseño se revisó las diferentes tecnologías y sistemas de seguridad que hay en la actualidad, para determinar aquella que mejor se adapte a las necesidades del Laboratorio a protegerse. Luego de realizar un análisis comparativo se optó por una opción de bajo consumo de potencia, menos vulnerable a ataques de intrusos y que sea competitiva en costos. El sistema cuenta con sensores ubicados en puertas y pasillos, comandados mediante una central de control que consta de un microcontrolador programado para cubrir a todo el laboratorio. El sistema puede dar un aviso inmediato a una aplicación que permite identificar al dispositivo activado así como su ubicación. Puesto que la aplicación debe en el futuro permitir el control de varios sitios a la vez, el sistema cuenta con un sistema de comunicación basado en el estándar Zigbee (IEEE 802.15.4) que le proveería de versatilidad para la interconexión.

Luego de haber implementado el sistema de seguridad anti intrusos y haber realizado las pruebas respectivas se demostró que el sistema cumple con las expectativas planteadas.

## **PRESENTACION**

En la actualidad y debido a la inseguridad que existe, todos los lugares que cuentan con equipos de valor son protegidos utilizando sistemas anti intrusos.

Los sistemas anti intrusos son una herramienta que brinda confiabilidad a los usuarios que se encargan de la seguridad. Los sistemas de seguridad anti intrusos evolucionan cada día y su sistema de comunicación alámbrico ha sido paulatinamente sustituido por sistemas inalámbricos dentro de los cuales están incluidos los sistemas Zigbee.

El presente diseño utiliza un sistema Zigbee de corto alcance y punto a punto para cumplir con las necesidades de comunicación.

Los sistemas Zigbee están difundidos a nivel mundial en diversas aplicaciones de seguridad para casas, edificios, oficinas, etc. Además de estas aplicaciones de seguridad, los sistemas Zigbee son usados en una infinidad de proyectos y en la domótica de última tecnología.

El presente diseño también utiliza un microcontrolador PIC16F877A que sirve para cumplir con las necesidades de procesamiento de datos. Este microcontrolador fue escogido por su facilidad de instalación y programación.

## **CAPITULO 1**

### **INTRODUCCION AL ESTANDAR IEEE 802.15.4 ZIGBEE**

#### **1.1 ESPECIFICACIONES DEL ESTANDAR IEEE 802.15.4**

El estándar IEEE 802.15.4 pertenece al grupo de las redes LR-WPAN (Low Rate Wireless Personal Area Networks). Estas redes son redes de comunicación de bajo costo que permiten conectividad inalámbrica para aplicaciones donde la potencia es limitada. Los principales objetivos de estas redes son: la fácil instalación, confiabilidad de transferencia de datos, cortos rangos de operación, bajo costo y un razonable tiempo de vida de las baterías manteniendo un protocolo simple y flexible.

##### **1.1.1 CARACTERISTICAS GENERALES DE REDES LR-WPANs:**

- Velocidades de transmisión inalámbricas de 250 kbps, 100 kbps, 40 Kbps y 20 Kbps
- Operación en estrella o punto a punto
- Direcciones cortas de 16 bits o de 64 bits
- GTSs (Guaranteed time slots)
- Acceso al canal con CSMA-CA
- Protocolo con confirmación para transferencia confiable
- Consumo bajo de potencia
- Detección de energía (ED-Energy Detection)
- Indicador de calidad de enlace (LQI-Link Quality Indication)
- 16 canales en los 2450 MHz, 30 canales en los 915 MHz y 3 canales en los 868 MHz

En las redes 802.15.4 existen dos tipos de dispositivos:

1. FFD (Full Function Device): Estos dispositivos, conocidos como nodos activos, tienen gran capacidad de procesamiento.
2. RFD (Reduced Function Device): Estos dispositivos, conocidos como nodos pasivos, tienen capacidades limitadas de procesamiento.

Un dispositivo FFD puede operar como:

1. Coordinador: Es el dispositivo más completo, existe por lo menos uno por cada red, controla la red y el camino que sigue cada dispositivo para comunicarse entre ellos.
2. Router: Es el dispositivo que interconecta dispositivos separados en la topología de red.
3. Dispositivo final: Es el dispositivo que tiene la funcionalidad de comunicarse con su nodo coordinador pero no puede comunicarse con otros dispositivos.

Por otro lado, un dispositivo RFD solo puede operar como dispositivo final y es utilizado para aplicaciones bastantes simples, como por ejemplo en interruptores de luz o en un sensor. Estos dispositivos no tienen la necesidad de transmitir grandes cantidades de datos y pueden asociarse con un solo FFD a la vez. Consecuentemente, un dispositivo RFD puede ser implementado usando un mínimo de recursos y mínimo de capacidad de memoria.

### **1.1.2 COMPONENTES DEL ESTANDAR IEEE 802.15.4**

Un sistema conformado con este estándar se compone de algunos componentes, el más general de estos componentes es el dispositivo que puede ser FFD o RFD. Dos o más dispositivos comunicándose en el mismo canal físico constituyen y forman una red WPAN, sin embargo esta WPAN debe incluir por lo menos un dispositivo FFD operando como coordinador WPAN. El área de cobertura de la red no existe en realidad para un dispositivo, debido a que las características de propagación son dinámicas e inciertas. Pequeños cambios en la posición o

dirección pueden ocasionar drásticas diferencias en el enlace de comunicaciones. Estos efectos pueden ocurrir en dispositivos estacionarios y en móviles.

### **1.1.3 TOPOLOGIAS DE RED**

Dependiendo de la aplicación de la red, el estándar IEEE 802.15.4 puede operar en dos topologías:

1. Estrella
2. Punto a punto

En la topología de estrella las comunicaciones son establecidas entre equipos con un controlador central llamado el coordinador WPAN. Este coordinador puede tener una aplicación específica pero generalmente es usado como inicio, como fin o como dispositivo de ruteo. Todos los equipos que operan en una red con cualquiera de las dos topologías tienen una dirección única de 64 bits. Esta dirección puede ser usada para las comunicaciones directas entre dispositivos. Una dirección pequeña de 16 bits también puede ser usada por el coordinador.

En la topología punto a punto también se tiene un coordinador WPAN con la diferencia, ante la topología en estrella, de que cualquier dispositivo puede comunicarse con otro siempre que se encuentre dentro del rango del anterior. La topología punto a punto requiere más complejidad para la implementación. Dentro de las aplicaciones más comunes para esta topología está la industria en el control y monitoreo de sensores inalámbricos, en la agricultura inteligente y en la seguridad. Una red con esta topología puede ser:

1. Ad hoc
2. Self-organizig
3. Self-healing

Esta topología también permite múltiples saltos para enrutar mensajes desde un dispositivo hacia otro en la red. Funciones adicionales pueden ser añadidas en capas superiores, pero no son parte del estándar IEEE 802.15.4. Cada red WPAN es independiente y tiene un único identificador. Este identificador permite

comunicarse entre dispositivos usando direcciones cortas de 16 bits y habilitando transmisiones entre dispositivos a través de redes independientes.

### 1.1.3.1 Formación de una red con topología en estrella

La estructura básica para una red en estrella se puede observar en la Figura 1.1. Luego de que el dispositivo FFD es activado este puede establecer su propia red y llegar a ser el coordinador PAN. Todas las redes en estrella operan independientemente de otras redes en estrella que estén en operación. Esto se realiza escogiendo un identificador PAN el cual no sea usado por ninguna otra red que este dentro del radio de influencia. Cuando el identificador PAN es escogido, el coordinador PAN permite a otros dispositivos sean estos FFD o RFD acceder a la red.

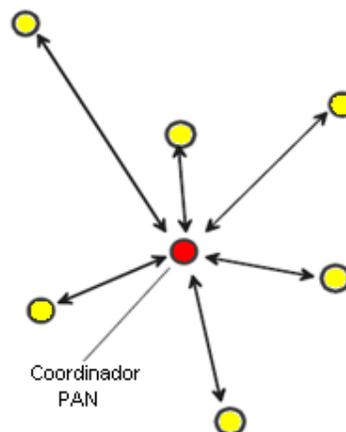


Figura 1.1 Topología en estrella

### 1.1.3.2 Formación de una red punto a punto

La estructura básica para una red en punto a punto se puede observar en la Figura 1.2. En una red punto a punto cada dispositivo está en la capacidad de comunicarse con otro dispositivo que se encuentre en su radio de cobertura. Un

dispositivo es denominado el coordinador PAN, el cual tuvo la virtud de ser el primer dispositivo en comunicarse en el canal.

Un claro ejemplo de una red punto a punto es una red "cluster tree". Esta red contiene una gran mayoría de dispositivos FFD. Un dispositivo RFD se conecta a una red cluster tree como una hoja al final de una rama porque los dispositivos RFD no permiten a otros equipos asociarse. Algunos dispositivos FFD pueden actuar como coordinadores y proveer servicios de sincronización a otros dispositivos o hacia otros coordinadores. Solo uno de estos coordinadores puede ser el coordinador general WPAN, el cual debe tener grandes recursos computacionales, mejores a los de cualquier otro dispositivo en la red. El coordinador WPAN forma el primer grupo escogiendo identificadores WPAN no usados y enviando mensajes de broadcast en tramas beacon a dispositivos vecinos. El mecanismo de contención es requerido si dos o más dispositivos FFD simultáneamente intentan establecerse como coordinadores WPAN.

Un dispositivo candidato recibe una invitación (trama beacon) a la cual debe contestar para unirse a la red. Si el coordinador WPAN permite a este dispositivo unirse a la red lo añade en su lista de vecinos, luego el nuevo dispositivo unido al coordinador WPAN empieza una transmisión periódica de beacons, y nuevos dispositivos candidatos pueden unirse al coordinador WPAN.

Si el dispositivo original que estaba como candidato no está disponible para unirse a la red, el coordinador WPAN buscara otro dispositivo. La forma más simple de una red cluster tree es una simple red cluster, pero redes más grandes son posibles formando una malla de múltiples clusters. Una vez conocidos los requerimientos de la red, el primer coordinador WPAN puede instruir a un dispositivo para que pueda ser un coordinador WPAN de un nuevo cluster añadido al primero. Otros dispositivos gradualmente se conectan y forman una estructura de red multicluster, parecida a la que se encuentra en la Figura 1.3. La ventaja de tener un multicluster es el incremento del área de cobertura pero la desventaja es el incremento de la latencia en los mensajes.

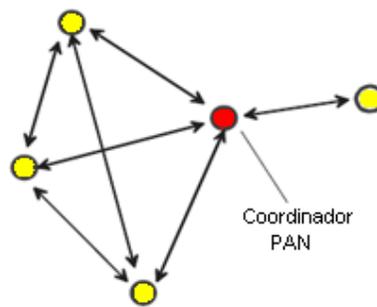


Figura 1.2 Topología Punto a Punto

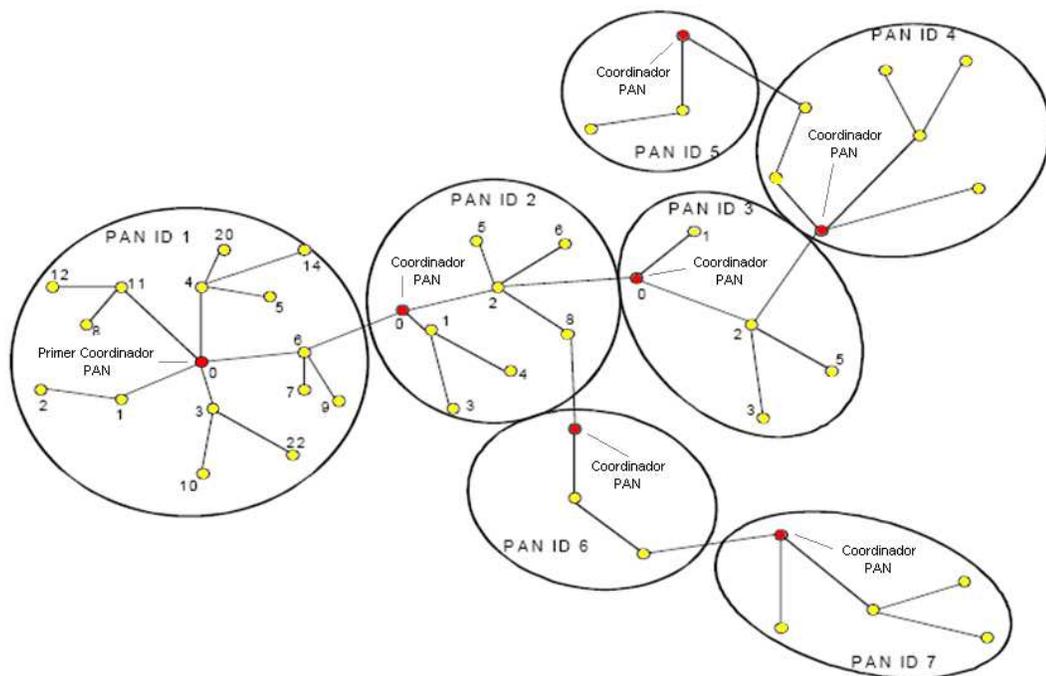


Figura 1.3 Red Multicluster

#### 1.1.4 ARQUITECTURA

La arquitectura del estándar IEEE 802.15.4 está definida en términos del número de componentes que simplifiquen el estándar. Estos componentes son llamados capas, cada capa es responsable por una parte del estándar y ofrece servicios a las capas superiores. La estructura de las capas está basada en el sistema OSI

de siete capas. Las interfaces entre las capas sirven para definir los enlaces lógicos descritos en este estándar. Un dispositivo LR-WPAN está provisto de una capa PHY la cual contiene un transceiver de radio frecuencia (RF) el cual es un mecanismo de control de bajo nivel, y una subcapa MAC la cual provee acceso al canal físico para todo tipo de transferencias. En la Figura 1.4 se puede observar de una forma grafica lo descrito anteriormente.

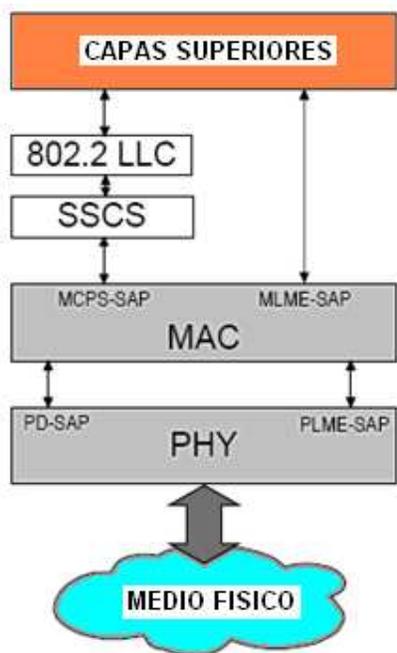


Figura 1.4 Arquitectura IEEE 802.15.4

Las capas superiores a la subcapa MAC consisten de una capa de red, la cual provee la configuración, manipulación y ruteo de los mensajes de la red, y una capa de aplicación, la cual provee las funciones del dispositivo. Estas capas se describen en el estándar ZigBee que se explicará luego. La capa LLC (Logical Link Control) puede acceder a la subcapa MAC a través de una subcapa de convergencia SSCS (Service-Specific Convergence Sublayer). La arquitectura LR-WPAN puede ser implementada para dispositivos embebidos como para dispositivos que requieren del soporte de un equipo externo, como una PC. Los servicios MCPS-SAP y MLME-SAP son proveídos por la subcapa MAC para realizar la interfaz hacia el SSCS (Service-Specific Convergence Sublayer). Esta es una capa de convergencia que realiza la interfaz hacia la subcapa 802.2 LLC

(Logical Link Control). Los servicios PD-SAP y PLME-SAP realizan la interfaz entre la subcapa MAC y la capa PHY.

#### 1.1.4.1 Capa PHY

La capa PHY realiza un interfaz entre la capa física y la subcapa MAC. Esta capa incluye una entidad de administración llamada PLME. La PLME es responsable por mantener una base de datos de administración de objetos correspondientes a la capa PHY. Esta base de datos es referida como PIB (PAN Information Database). La Figura 1.5 muestra los componentes e interfaces de la capa PHY.

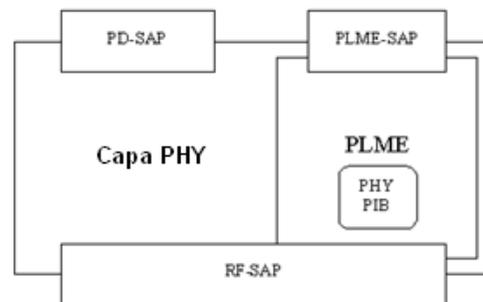


Figura 1.5 Componentes e interfaces de la capa PHY

La capa PHY provee dos servicios:

1. Servicio de datos PHY (PHY Data Services): Este servicio habilita la transmisión y recepción de las PDUs (Protocol Data Units) a través del canal físico de radio. Este servicio es accedido a través de PD-SAP.
2. Servicio de administración PHY (PHY Management Service): Este servicio realiza un interfaz hacia PLME (Physical Layer Management Entity). Este servicio es accedido a través de PLME-SAP.

La capa PHY es responsable de:

1. Activación y desactivación del tranciver de radio
2. ED (Energy Detection)
3. LQI (Link Quality Indicator)
4. Selección de frecuencia del canal
5. CCA (Clear Channel Assessment) para CSMA-CA
6. Trasmisión y recepción de datos

#### *1.1.4.1.1 ED (Energy Detection)*

La medida de Energy Detection es usada por la capa red como parte de la selección de canales. Esta medida es un estimado de la potencia de la señal recibida.

#### *1.1.4.1.2 LQI (Link Quality Indicator)*

La medida de Link Quality Indicator indica la calidad de los paquetes recibidos.

#### *1.1.4.1.3 CCA (Clear Channel Assessment)*

Se realiza por tres diferentes métodos:

1. CCA modo 1: Se reporta un medio ocupado cuando se detecta energía por encima del umbral.
2. CCA modo 2: Se reporta un medio ocupado cuando se detecta una portadora.
3. CCA modo 3: Se reporta un medio ocupado con la combinación de CCA modo 1 y CCA modo2.

#### 1.1.4.1.4 Rango operativo de frecuencias

Los dispositivos pueden trabajar en una de muchas bandas de frecuencia usando modulación y formatos de propagación mostrados en la Tabla 1.1

PHY (MHz)	Banda de frecuencia (MHz)	Parámetros de propagación		Parámetros de datos		
		Chip rate (kchip/s)	Modulación	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Símbolos
868/915	868-868.6	300	BPSK	20	20	Binario
	902-928	600	BPSK	40	40	Binario
868/915 (opcional)	868-868.6	400	ASK	250	12.5	20 bits PSSS
	902-928	1600	ASK	250	50	5 bits PSSS
868/915 (opcional)	868-868.6	400	O-QPSK	100	25	16-ario orthogonal
	902-928	1000	O-QPSK	250	62.5	16-ario orthogonal
2450	2400-2483.5	2000	O-QPSK	250	62.5	16-ario orthogonal

Tabla 1.1 Rango operativo de frecuencias

#### 1.1.4.1.5 Canales

El estándar IEEE 802.15.4 define un número de 32 canales. Para soportar el crecimiento del número de canales se realiza una combinación entre números de canales y paginas de canales. Esta combinación se realiza utilizando los 5 bits más significantes de los bitmaps para especificar 32 posibles páginas de canales. Los 27 bits menos significantes especifican los 27 canales dentro de la página de canal. En la Tabla 1.2 se puede observar las páginas y números de canales asociados.

Página de canal (decimal)	Página de canal (binario)	Número de canal (decimal)	Descripción del número de canal
0	00000	0	Canal 0 está en la banda 868 MHz usando BPSK
		1-10	Canales 1-10 están en la banda 915 MHz usando BPSK
		11-26	Canales 11-26 están en la banda 2.4 GHz usando O-QPSK
1	00001	0	Canal 0 está en la banda 868 MHz usando ASK
		1-10	Canales 1-10 están en la banda 915 MHz usando ASK
		11-26	Reservado
2	00010	0	Canal 0 está en la banda 868 MHz usando O-QPSK
		1-10	Canales 1-10 están en la banda 915 MHz usando O-QPSK
		11-26	Reservado
3-31	00011-1111	Reservado	Reservado

Tabla 1.2 Canales

#### 1.1.4.1.6 Períodos LIFS (Minimum Long Interframe Spacing) y SIFS (Short Interframe Spacing)

Los tiempos LIFS y SIFS se ilustran en la Figura 1.6

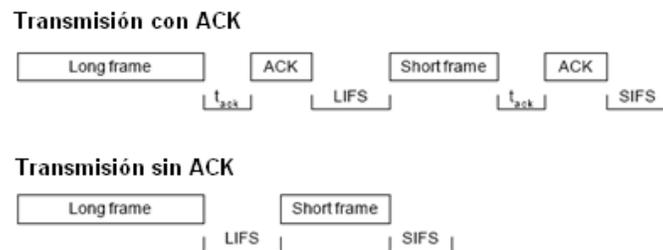


Figura 1.6 Períodos LIFS y SIFS

Los períodos mínimos LIFS y SIFS para cada PHY se muestran en la Tabla 1.3

PHY	macMinLIFSPeriod	macSIFSPeriod	Unidades
868-868.6 MHz BPSK	40	12	Símbolos
902-928 MHz BPSK	40	12	Símbolos
868-868.6 MHz ASK	40	12	Símbolos
902-928 MHz ASK	40	12	Símbolos
868-868.6 MHz O-QPSK	40	12	Símbolos
902-928 MHz O-QPSK	40	12	Símbolos
2400-2483.5 MHz O-QPSK	40	12	Símbolos

Tabla 1.3 Periodos mínimos LIFS y SIFS

#### 1.1.4.1.7 Potencia

La potencia máxima de transmisión debe estar conforme a las regulaciones locales. De la misma forma las emisiones espurias deben estar en conformidad con las regulaciones locales. La sensibilidad del receptor se mide de acuerdo al PER (Packet Error Rate). El PER es un promedio de paquetes transmitidos los cuales no han sido correctamente recibidos.

#### 1.1.4.1.8 Formato PPDU

La estructura del paquete se presenta de tal forma que el campo que se encuentra a la izquierda es el primero que se transmite. De la misma forma el bit menos significativo es el primero que se transmite.

Cada paquete PPDU consiste de tres componentes básicos como se puede ver en la Figura 1.7

1. Una cabecera de sincronización (SHR), la cual permite al equipo receptor sincronizarse.
2. Una cabecera PHY (PHR), la cual contiene la información de longitud de trama.

3. Un payload de longitud variable el cual contiene la trama de la subcapa MAC.

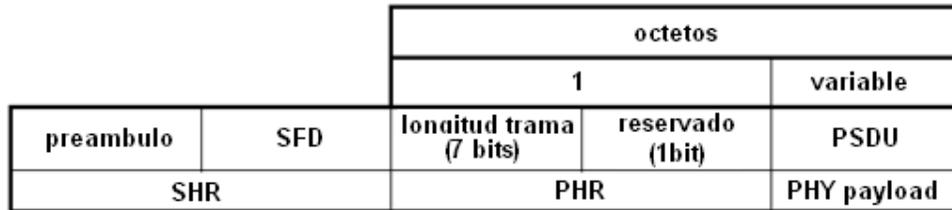


Figura 1.7 Paquete PDU

El preámbulo es usado por el transmisor para obtener la sincronización de un mensaje entrante. En la Tabla 1.4 se muestra la longitud del campo.

PHY	Longitud		Duración (us)
868-868.6 MHz BPSK	4 octetos	32 símbolos	1600
902-928 MHz BPSK	4 octetos	32 símbolos	800
868-868.6 MHz ASK	5 octetos	2 símbolos	160
902-928 MHz ASK	3.75 octetos	6 símbolos	120
868-868.6 MHz O-QPSK	4 octetos	8 símbolos	320
902-928 MHz O-QPSK	4 octetos	8 símbolos	128
2400-2483.5 MHz O-QPSK	4 octetos	8 símbolos	128

Tabla 1.4 Longitud del campo preámbulo

El campo SFD indica el final del campo SHR y el comienzo del paquete de datos. La longitud de este campo se muestra en la Tabla 1.5. El valor excepto para ASK es de 11100101.

PHY	Longitud	
868-868.6 MHz BPSK	1 octeto	8 símbolos
902-928 MHz BPSK	1 octeto	8 símbolos
868-868.6 MHz ASK	2.5 octetos	1 símbolo
902-928 MHz ASK	0.625 octetos	1 símbolo
868-868.6 MHz O-QPSK	1 octeto	2 símbolos
902-928 MHz O-QPSK	1 octeto	2 símbolos
2400-2483.5 MHz O-QPSK	1 octeto	2 símbolos

Tabla 1.5 Longitud de campo SFD

El campo de longitud de trama tiene una longitud de siete bits. Este campo especifica el número total de octetos contenidos en el PSDU. La Tabla 1.6 muestra los valores de longitud frente al tipo de payload.

Longitud de trama	Payload
0-4	Reservado
5	MPDU (ACK)
6-8	Reservado
9 a aMaxPHYPacketSize	MPDU

Tabla 1.6 Longitud del campo longitud trama

El campo PSDU tiene una longitud variable y contiene el paquete de datos de la PHY.

#### 1.1.4.2 Subcapa MAC

La subcapa MAC provee un interfaz entre la SSCS y la PHY. Esta subcapa incluye una entidad de administración llamada MLME. Esta entidad provee un servicio de interfaces a través de los cuales las funciones de administración de capa deben ser invocadas. La MLME también es responsable del mantenimiento de la base de datos de los objetos relacionados administrados en la subcapa

MAC. Esta base de datos es referida como PIB. En la Figura 1.8 se muestra los componentes de la subcapa MAC.

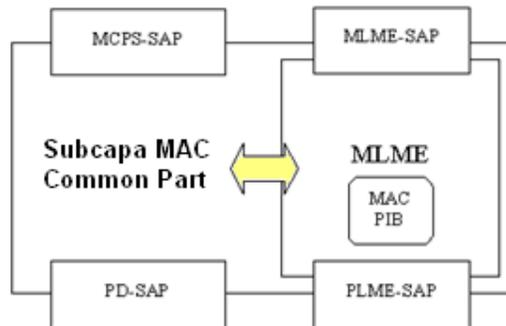


Figura 1.8 Componentes de la subcapa MAC

La subcapa MAC es responsable de:

1. Administración de beacons
2. Acceso al canal
3. Administración GTS
4. Validación de trama
5. Entrega de trama conocida
6. Asociación y Desasociación

#### 1.1.4.2.1 Administración de Beacons

El estándar IEEE 802.15.4 permite el uso de una supertrama. Esta supertrama tiene un formato el cual lo define el coordinador. La supertrama es delimitada por beacons que son enviados por el coordinador y está dividida en 16 slots de igual tamaño como se observa en la Figura 1.9

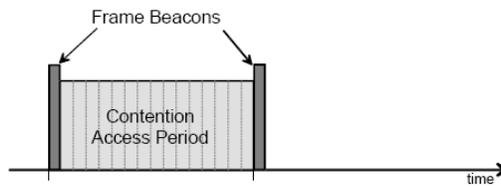


Figura 1.9 Supertrama IEEE 802.15.4

La supertrama puede tener una porción activa y otra inactiva como se observa en la Figura 1.10

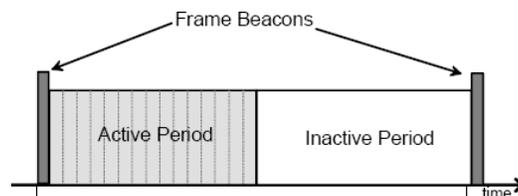


Figura 1.10 Supertrama con porción activa e inactiva

Durante la porción de inactividad el coordinador puede entrar en un estado de bajo consumo de potencia. La trama beacon es transmitida en el primer slot de cada supertrama. Si el coordinador no desea usar la estructura de supertrama este apagará las transmisiones de beacons.

Los beacons son usados para sincronizar los dispositivos de la red para identificar la PAN, y para describir la estructura de la supertrama. Cuando un dispositivo desea comunicarse durante el periodo de acceso de contención (CAP-Contention Access Period), entre dos beacons, compete con otros dispositivos usando el mecanismo CSMA-CA.

Para aplicaciones de baja latencia o aplicaciones que requieren un ancho de banda específico, el coordinador PAN debe dedicar porciones activas de la supertrama para dicha aplicación. Estas porciones son llamadas GTS

(Guaranteed Time Slots). Los GTS forman el periodo libre de contención (CFP-Contention Free Period), el cual siempre aparece al final de la supertrama activa, como se muestra en la Figura 1.11

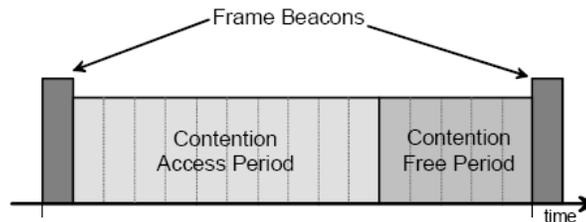


Figura 1.11 CAP y CFP

El coordinador PAN puede asignar siete GTS. Un GTS puede ocupar más de un slot, pero siempre queda una porción de CAP para el acceso por contención. Cada dispositivo en un GTS debe estar seguro de completar su transacción antes del siguiente GTS o antes del fin del periodo CFP. En la Figura 1.12 se puede observar un ejemplo de supertrama.

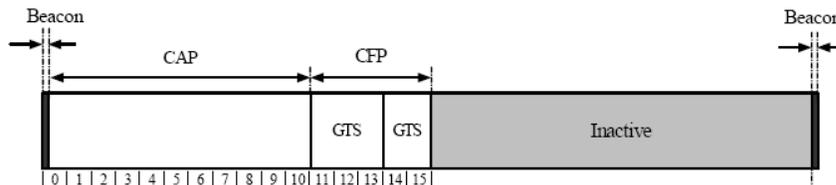


Figura 1.12 Ejemplo de supertrama

#### 1.1.4.2.2 Acceso al canal

Para acceder al canal el estándar IEEE 802.15.4 utiliza dos tipos de mecanismos que dependen de la configuración de la red.

1. Nonbeacons-Enabled
2. Beacons-Enabled

Una PAN con Nonbeacons-Enable utiliza el mecanismo CSMA-CA unslotted. Cuando un dispositivo desea transmitir tramas de datos o comandos MAC, este espera un periodo aleatorio. Si el canal se encuentra desocupado luego del periodo aleatorio, el dispositivo transmite los datos. Si el canal se encuentra ocupado luego del periodo aleatorio el dispositivo espera otro tiempo aleatorio antes de tratar nuevamente de acceder al canal. Las tramas de confirmación son enviadas sin usar el mecanismo CSMA-CA.

Una PAN con Beacons-Enable usa el mecanismo de acceso slotted. Este mecanismo alinea los slots con el inicio del beacon de transmisión. Cuando un dispositivo desea transmitir tramas de datos durante el periodo CAP, este localiza la frontera del siguiente slot y luego espera por un número aleatorio de slots antes de tratar de acceder al canal nuevamente. Si el canal esta libre el dispositivo empieza la transmisión en el siguiente limite de un slot disponible.

El algoritmo CSMA-CA se utiliza antes de la transmisión de datos en una red Nonbeacons-enabled y no se utiliza en tramas de confirmación o datos transmitidos en un periodo CFP. Si se utiliza beacons periódicos se emplea la versión CSMA-CA slotted.

Cada dispositivo mantiene tres variables por cada intento de transmisión:

1. NB: Numero de veces que el algoritmo CSMA-CA fue requerido para la transmisión.
2. CW: Longitud de la ventana de contención la cual define el numero de periodos backoff que son necesarios para acceder a un canal limpio antes de transmitir, se usa solo para CSMA-CA slotted.
3. BE: Exponente de backoff que define el numero de periodos backoff que un dispositivo espera antes de accesar a un canal.

### 1.1.4.2.3 Asociación y Desasociación

Un dispositivo se asocia luego de haber realizado un reset de la subcapa MAC y un completo escaneo activo o pasivo del canal. Los resultados del escaneo del canal deben servir para luego escoger una adecuada PAN.

La desasociación se inicia por la capa superior cuando un coordinador requiere que un dispositivo asociado salga de la red PAN.

### 1.1.4.2.4 Transferencia de datos

El estándar IEEE 802.15.4 ofrece tres tipos de transferencias de datos:

1. Transferencia de datos a un coordinador
2. Transferencia de datos desde un coordinador
3. Transferencia de datos entre dispositivos

Para la transferencia de datos a un coordinador en una PAN Beacons-enable se escucha los beacons y cuando se encuentra uno, el dispositivo sincroniza la estructura de la supertrama. El dispositivo transmite su trama de datos usando CSMA-CA hacia el coordinador. Este puede confirmar la exitosa recepción de los datos transmitiendo una trama adicional de confirmación como se observa en la Figura 1.13

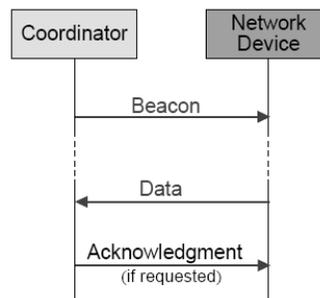


Figura 1.13 Transferencia de datos a un coordinador Beacons-enable

Para la transferencia de datos a un coordinador en una red Nonbeacons-enabled, se transmite los datos usando CSMA-CA hacia el coordinador. Este confirma la exitosa recepción de los datos con una transmisión opcional de una trama de confirmación como se observa en la Figura 1.14

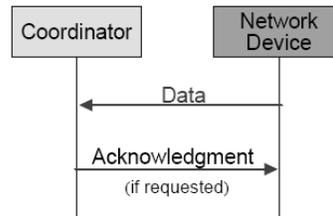


Figura 1.14 Transferencia de datos a un coordinador Nonbeacon-enable

Para la transferencia de datos desde un coordinador en una red Beacons-enabled, este indica a la red que un mensaje está en espera. Los dispositivos escuchan periódicamente beacons en la red para verificar si hay mensajes pendientes. El coordinador confirma la exitosa recepción de los datos enviando una trama de confirmación. La trama pendiente se envía luego de la confirmación. El dispositivo debe confirmar la recepción de los datos transmitiendo una trama de confirmación. Luego de la transmisión de los datos el mensaje es removido de la lista de mensajes pendientes como se ve en la Figura 1.15

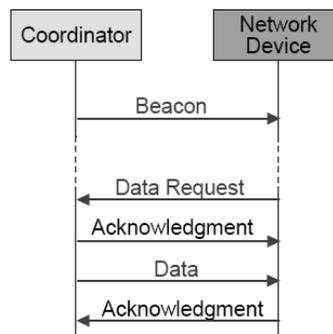


Figura 1.15 Transmisión de datos desde un coordinador Beacons-Enable

Para la transferencia de datos desde un coordinador en una red Nonbeacons-enabled, este guarda los datos para contactar al dispositivo apropiado y transmitirlos. El dispositivo debe solicitar los datos al coordinador. El coordinador confirma la recepción de los datos transmitiendo una trama de confirmación. Si la trama de datos está pendiente, el coordinador transmite la trama usando acceso CSMA-CA hacia el dispositivo. Si la trama no está pendiente el coordinador indica este hecho en la trama de confirmación luego de la solicitud de los datos, o en una trama de datos con un payload de longitud cero. Luego el dispositivo envía una trama de confirmación como se ve en la Figura 1.16

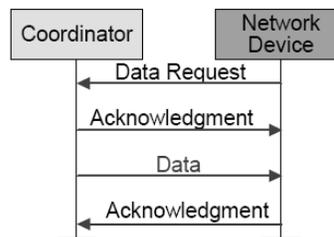


Figura 1.16 Transmisión de datos desde un coordinador Nonbeacons-Enable

Para la transferencia de datos en una red punto a punto los dispositivos que desean comunicarse necesitan sincronizarse los unos con los otros.

#### 1.1.4.2.5 Consumo de potencia

El estándar IEEE 802.15.4 ha sido desarrollado para ser utilizado en dispositivos con baterías, sin embargo en ciertas aplicaciones se utilizan dispositivos alimentados directamente, sin baterías.

#### 1.1.4.2.6 Seguridad

El estándar IEEE 802.15.4 es vulnerable a los ataques Eavesdropping. Los dispositivos IEEE 802.15.4 son de bajo costo y no poseen una base computacional confiable. Estas restricciones limitan la elección de algoritmos criptográficos y protocolos e influyen en la arquitectura de la seguridad. Los

mecanismos criptográficos se basan en llaves simétricas las cuales son provistas por procesos de capas superiores. El mecanismo asume una implementación segura de operaciones criptográficas y el almacenamiento seguro y autenticado del material de llaves. El mecanismo criptográfico provee combinaciones particulares de los siguientes servicios de seguridad:

1. Confidencialidad de datos: Seguridad en la transmisión de información. Esta información es solo para quien debe recibirla.
2. Autenticidad de datos: Seguridad de la fuente que transmite la información.
3. Protección Replay: Seguridad en la duplicidad de información, es detectada.

#### 1.1.4.2.7 Periodos LIFS Y SIFS

La subcapa MAC necesita un periodo de tiempo para procesar los datos recibidos desde la capa PHY. Dos tramas sucesivas transmitidas desde un dispositivo deben ser separadas por lo menos por un periodo IFS. Si la primera transmisión requiere acuse de recibo, la separación entre la trama de acuse y la segunda transmisión deber ser de al menos un periodo IFS. La longitud del periodo IFS es dependiente del tamaño de la trama que ha sido transmitida. Tramas mayores al tamaño SIFS máximo en octetos deben ser seguidas por un SIFS. Tramas más grandes que el tamaño SIFS máximo en octetos deben ser seguidas por un periodo LIFS como se muestra en la Figura 1.17

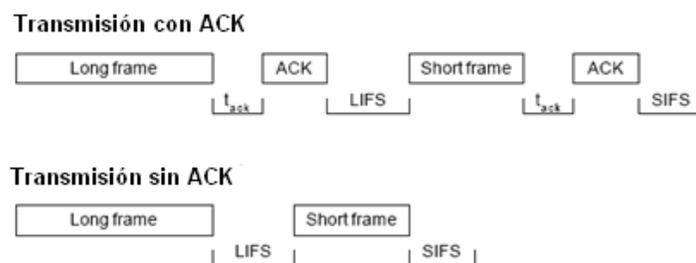


Figura 1.17 Períodos SIFS y LIFS

### 1.1.4.2.8 Estructura de tramas

La estructura de trama ha sido diseñada para mantener una complejidad mínima y una buena robustez para la transmisión en un canal ruidoso. El estándar IEEE 802.15.4 define cuatro estructuras de trama:

1. Una trama beacon usada por el coordinador
2. Una trama de datos
3. Una trama de confirmación
4. Una trama command MAC, usada para manejar el control de transferencias entre entidades pares

La estructura de la trama beacon se puede observar en la Figura 1.18. Un coordinador puede transmitir beacons en una PAN Beacons-enabled.

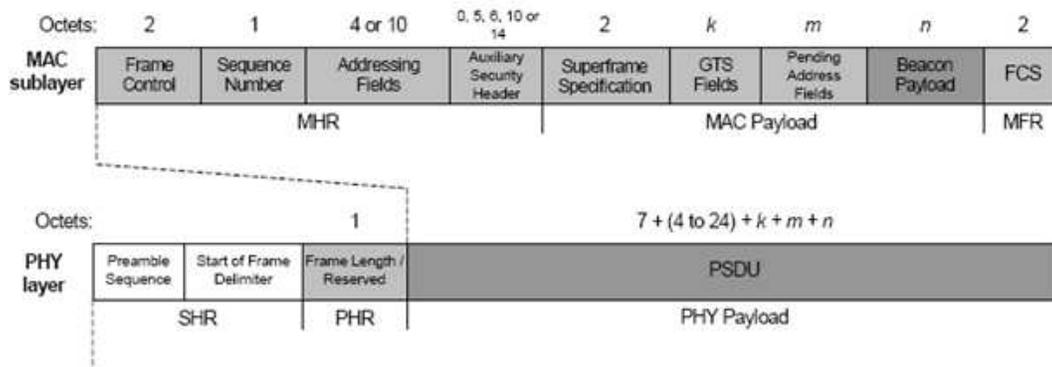


Figura 1.18 Estructura de trama beacon

La trama beacon es enviada a la capa física como PSDU (PHY Service Data Unit).

La estructura de la trama de datos se puede observar en la Figura 1.19. El payload de datos que pasa a la subcapa MAC se denomina MSDU (MAC Service Data Unit). La MPDU pasa a la capa PHY como la PSDU, la cual se convierte en

el payload PHY. La secuencia de preámbulo y los datos SFD activan la recepción para lograr la sincronización de símbolo.

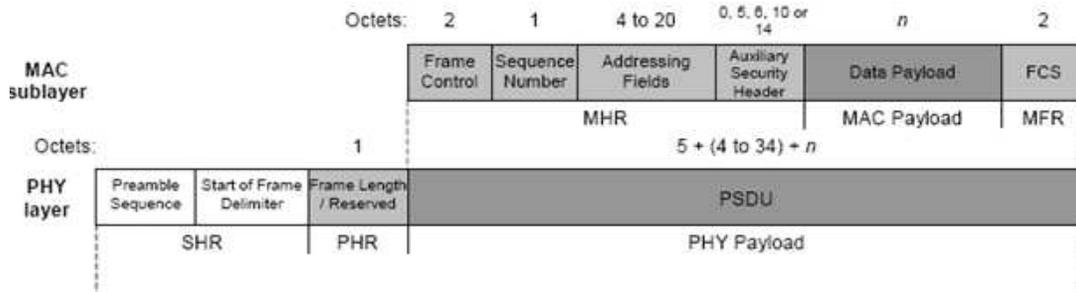


Figura 1.19 Estructura de trama de datos

La estructura de la trama de confirmación se puede observar en la Figura 1.20. La trama de confirmación no tiene payload MAC. La MPDU pasa a la capa PHY como el PSDU, el cual se convierte en el payload PHY.

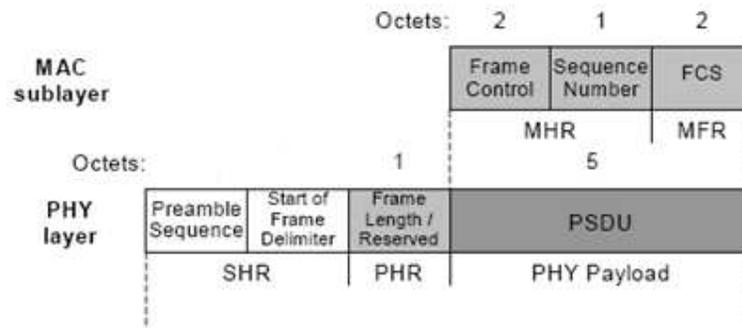


Figura 1.20 Estructura de trama de confirmación

La estructura de la trama de comando MAC se puede observar en la Figura 1.21. La MPDU luego pasa a la capa PHY como el PSDU, el cual se convierte en el payload PHY. La secuencia de preámbulo activa la recepción para lograr la sincronización de símbolo.

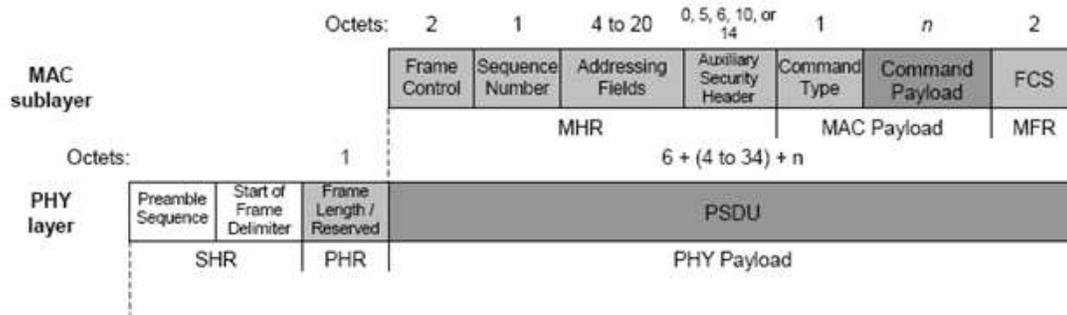


Figura 1.21 Estructura de trama de comando MAC

En orden de detectar errores en los bits el estándar IEEE 802.15.4 emplea el mecanismo FCS el cual utiliza CRC (Cyclic Redundancy Check).

#### 1.1.4.2.9 Formación de una PAN

Para empezar todos los dispositivos deben ser capaces de realizar escaneos a través de una lista de canales especificados.

El escaneo de canal ED permite a un dispositivo obtener una medida del pico de energía en cada solicitud de canal.

Se pueden realizar tres tipos de escaneos:

1. Escaneo de canal activo
2. Escaneo de canal pasivo
3. Escaneo de canal huérfano

El escaneo de canal activo permite a un dispositivo localizar alguna transmisión de tramas beacon de algún coordinador. Puede ser utilizado por un coordinador PAN prospecto para seleccionar un identificador PAN o para usarse antes de la asociación.

El escaneo de canal pasivo permite localizar la transmisión de tramas beacon de algún coordinador. Sin embargo el Beacon Request Command no es transmitido. Puede ser utilizado por un dispositivo antes de la asociación.

El escaneo de canal huérfano permite a un dispositivo intentar reubicar su coordinador luego de una pérdida de sincronización. Durante este escaneo la subcapa MAC debe descartar todas las tramas recibidas sobre el servicio de datos PHY.

Cuando dos PANs existen dentro de la misma cobertura con el mismo identificador PAN, se sigue un procedimiento de resolución. Este procedimiento es opcional para un RFD. El procedimiento de resolución genera un conflicto PAN ID el cual notifica a la siguiente capa superior para realizar un escaneo activo y usar la información del escaneo para seleccionar un nuevo identificador PAN.

Una PAN debe ser iniciada solo por un dispositivo FFD luego de haber realizado un reset de subcapa MAC, un escaneo activo y la elección del identificador PAN.

Para el descubrimiento de un dispositivo el coordinador PAN indica su presencia en la PAN por medio de la transmisión de tramas beacons. Luego se realiza la asociación del dispositivo.

## **1.2 ESPECIFICACIONES DE LA ALIANZA ZIGBEE**

### **1.2.1 ARQUITECTURA**

La arquitectura Zigbee está basada en el modelo de referencia OSI (Open Systems Interconnection), definiendo solamente aquellas capas relevantes para lograr la funcionalidad deseada y garantizar la compatibilidad entre los dispositivos.

El estándar IEEE 802.15.4 define dos capas base: la física (PHY) y la de control de acceso al medio (MAC). La Alianza ZigBee diseñó sobre ellas, la capa Red (NWK) y la capa Aplicación (APL).

A continuación se describen las características de las capas definidas por la Alianza ZigBee.



enlace de dispositivos y mantiene una base de datos de los objetos llamado “APS Information Base (AIB)”.

La responsabilidad de la APS es brindar un conjunto general de servicios para el uso de las subcapas AF, incluyendo servicios para el mantenimiento de tablas para ‘binding’, que es la habilidad para relacionar dos dispositivos basados en sus servicios y necesidades, y el envío de mensajes entre ellos.

#### 1.2.2.1.1 Formato de las Tramas PDU APS

Está compuesto por una cabecera y un payload. Los campos de la cabecera aparecen en un orden fijo, pudiendo el de dirección no ser incluido en todas las tramas. Las PDUs pueden ser datos, comando y ACK. El campo de dirección incluye identificadores para los endpoints (objetos), el clúster, y el perfil; al recibir un mensaje, la aplicación procesa esta información y determina a que endpoint notificar.

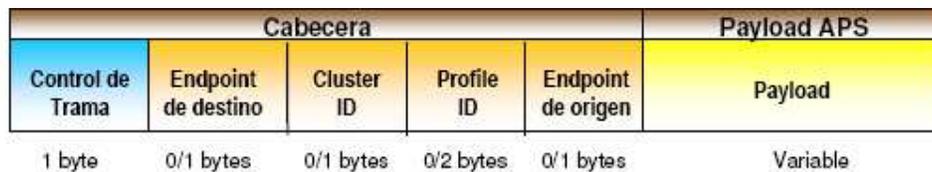


Figura 1.23 Formato de Trama APS

#### 1.2.2.2 Estructura de Aplicación (AF)

Dentro de la estructura de aplicación, los objetos envían y reciben datos a través del APSDE-SAP. El control y la gestión de los objetos de aplicación, es llevada a cabo por los interfaces de los ZDO. El servicio de datos ofrecido por el APSDE-SAP, incluye primitivas de petición, confirmación, respuesta e indicación (request, confirm, response, indication) para la transferencia de datos. Se pueden definir más de 240 objetos de aplicación llamados terminales, con interfaces que para cada uno de los terminales se enumeran del 1 al 240.

#### *1.2.2.2.1 Servicio de Parejas Clave-Valor*

El servicio de pares key-valor (KVP) permite a los atributos definidos, que en los objetos de aplicación se puedan utilizar primitivas como *get*, *get response*, *set* y *set response*.

KVP está diseñado para transferir información asociada a un atributo utilizando una estructura estricta. Además, KVP utiliza estructuras de datos de marcado XML en una versión más reducida.

#### *1.2.2.2.2 Servicio de Mensajes*

Existen varias áreas de aplicación en ZigBee, se tiene protocolos de direccionamiento propietarios y que no funcionan bien con KVP. Por tanto, este servicio MSG transfiere información mediante una estructura de formato libre.

### **1.2.2.3 Objetos de dispositivos ZigBee**

Las responsabilidades del ZDO son definir el rol de un dispositivo en la red (como coordinador o dispositivo final), iniciar y responder a un "*binding request*"(requerimiento de relación) y establecer vínculos seguros entre los elementos de la red. El ZDO es también responsable de descubrir dispositivos en la red y determinar qué servicios proveen.

Las interfaces públicas proporcionan la gestión de las direcciones de dispositivos, el descubrimiento, el enlace (binding) y las funciones de seguridad incluidos en la capa del framework de aplicación de la pila de protocolo de ZigBee.

#### *1.2.2.3.1 Gestión de Descubrimiento*

El descubrimiento se gestiona dependiendo de los objetos de aplicación. Cuando se solicita, la dirección IEEE de la petición del dispositivo tiene que ser devuelta (si el dispositivo es un dispositivo final) o bien con las direcciones de los dispositivos de todas las asociaciones (si el dispositivo es un dispositivo

coordinador o router). Todo esto se produce por un dispositivo que se encarga del descubrimiento de los dispositivos ZigBee.

Un dispositivo puede descubrir terminales activos, además puede descubrir servicios específicos que coincidan con un criterio dado (como pueden ser los identificadores de perfiles y de clusters).

#### *1.2.2.3.2 Gestión de Enlace*

La gestión del enlace la proporcionan los objetos de aplicación, de manera que estos objetos en cada uno de los dispositivos ZigBee puedan conectar todas las capas de la pila de protocolo a través de varias conexiones, que puedan proporcionar varios nodos en la red ZigBee. Las tablas de enlace se construyen y se publican en las peticiones de enlace y sus respuestas resultantes. Los dispositivos finales y las instrucciones tanto de enlace como de desenlace (abandono de la red) entre los dispositivos se soportan a través de los perfiles ZigBee

#### *1.2.2.3.3 Gestión de Seguridad*

La gestión de seguridad la proporcionan también los objetos de aplicación para habilitar o deshabilitar la parte de seguridad en el sistema. Si está habilitada, la gestión de claves se lleva a cabo haciendo el uso de lo que se conoce como claves maestras (master keys), claves de red (network keys) que permiten establecer una clave de enlace (link key).

## **1.2.3 FUNDAMENTOS DE COMUNICACIÓN DE LA CAPA DE APLICACIÓN**

### **1.2.3.1 Perfiles**

Los perfiles son acuerdos a los que se llega por mensajes. El formato de estos mensajes, y las acciones producidas, permiten a las aplicaciones residir en cada uno de los dispositivos individuales para enviar instrucciones, realizar peticiones de datos o procesar instrucciones para crear así una aplicación distribuible e interoperable. Por ejemplo, un interruptor en un nodo puede comunicarse con una lámpara en otro nodo. Juntos, son parte de un perfil para “control de iluminación”. Los perfiles son desarrollados por cada uno de los fabricantes ZigBee, que en base a las necesidades que existen en el mercado, proporcionan soluciones tecnológicas específicas.

### **1.2.3.2 Objeto (Endpoint)**

Es un elemento particular dentro de un dispositivo. Cada dispositivo Zigbee dispone de una única dirección de red, por lo tanto se requiere de una dirección de “endpoint” que diferencie cada componente (interruptores, lámparas, sensores, etc).

Cada dispositivo Zigbee puede soportar hasta 240 de tales componentes. El endpoint 0 está reservado para la administración del dispositivo (subcapa ZDO).

### **1.2.3.3 Atributo**

Es una entidad de datos que representa una cantidad física o un estado. El dato es comunicado a otro utilizando comandos (los más conocidos set, get, event).

### **1.2.3.4 Clusters**

Están formados por uno o más atributos. Los clusters se diferencian entre ellos mediante un identificador de cluster (Cluster ID), el cual está asociado con el flujo de datos saliente o entrante del dispositivo. Los identificadores de clusters son únicos dentro de un mismo perfil. Los enlaces se producen por la relación existente entre identificadores de clusters de salida y de entrada, asumiendo que ambos clusters están dentro de un mismo perfil.

### **1.2.3.5 Enlace (Binding)**

Creación de un enlace lógico unidireccional entre terminales/interfases/ clusters, de un nodo destino y otro de origen. Este enlace se puede establecer con uno o más dispositivos. Los dispositivos son vinculados basados en los servicios que ofrecen y sus necesidades.

La información de cómo los clusters se emparejan con los nodos se indica en una tabla de enlace (binding table).

La tabla de enlace se implementa en el coordinador ZigBee. Esto es porque se necesita que la red esté continuamente operativa y disponible, con lo que es más probable que el coordinador sea el que pueda ofrecer este servicio.

## **1.2.4 CAPA DE RED**

La capa de red hace de interfaz entre la capa de Aplicación y la capa MAC. Para esto, la capa de red dispone en esta interfaz de dos servicios: el Servicio de Datos y Servicio de Control. La comunicación entre la capa de Aplicación y la sub-capas MAC, se lleva a cabo en el SAP de la capa de Red.

Entre sus responsabilidades incluye mecanismos para unirse y dejar una red. Además, tiene como tarea el descubrimiento y mantenimiento de rutas entre los dispositivos de la red. Adicionalmente, está a cargo de la labor de descubrimiento de vecinos y memorización de dicha información. En esta capa, el coordinador es responsable de iniciar una nueva red, cuando es necesario, y asignar direcciones

a los nuevos dispositivos. Si el coordinador deja la red, otro dispositivo de función completa (FFD) puede tomar su papel.

#### 1.2.4.1 Formato de las tramas PDU NWK

Cada trama consiste de los siguientes componentes básicos:

1. Cabecera NWK, que comprende la trama de control, direccionamiento y secuenciamiento de la información.
2. Payload NWK, de longitud variable, que contiene información específica del tipo de trama.

Las tramas en la capa red están descritas como una secuencia de campos en orden específico. Los formatos de las tramas se describen en el orden en que se transmiten por la subcapa MAC, de izquierda a derecha, donde el bit de la izquierda es el más significativo se transmite primero. La trama será estructurada como en la ilustración de la Figura 1.24

octetos: 2	2	2	1	1	0/8	0/8	0/1	variable	variable
control de trama	dirección de destino	dirección de origen	radius	numero de secuencia	Dirección de destino IEEE	Dirección de origen IEEE	control multicast	subtrama source rate	trama payload
cabecera NWK									payload

Figura 1.24 Formato de la Trama NWK

#### 1.2.4.2 Funcionalidades

Todos los dispositivos ZigBee disponen de dos funcionalidades:

1. Incorporación a una Red
2. Abandonar una red

Además de estas funcionalidades, los dispositivos Coordinadores y Routers disponen de una serie de funcionalidades adicionales:

1. Permitir a otros dispositivos incorporarse a la red de dos formas distintas:
  - a. Por indicaciones de la sub-capas de MAC
  - b. Por solicitud de incorporación desde la capa de Aplicación
  
2. Permitir a los dispositivos miembros de la red abandonarla. De la misma forma que sucedía en el caso anterior, dispone de dos posibilidades:
  - a. Por indicaciones de la sub-capas de MAC
  - b. Por solicitud de incorporación desde la capa de Aplicación
  
3. Asignación de direcciones de red lógicas
4. Mantenimiento de una tabla o lista de dispositivos cercanos o vecinos

Por último, los dispositivos Coordinadores disponen de una funcionalidad particular. Esta es la que les permite crear o establecer nuevas redes de datos entre dispositivos.

#### *1.2.4.2.1 Formación de la red*

Una nueva red Zigbee es establecida por un coordinador. Al inicializarse, el coordinador busca otros coordinadores en sus canales permitidos. Basado en la energía del canal y el número de redes encontradas en sus canales, establece su propia red y selecciona un identificador PAN único. Una vez que la nueva red ha sido establecida, los ruteadores y terminales son habilitados a unirse a red.

Los distintos dispositivos guardan información acerca de otros nodos de la red, en un área no volátil de memoria llamada tabla de vecindades. Al inicializarse, si un dispositivo determina a través de la tabla que fue parte de una red, puede ejecutar un procedimiento de notificación para localizarla. Los dispositivos (coordinadores o ruteadores) que reciban la notificación, verificarán sus tablas para cerciorarse de que el nuevo dispositivo pertenecía a su red. Si la notificación falla o el

dispositivo no se encuentra en las tablas de vecindad del resto, tratará de unirse a una de las redes como un nuevo dispositivo.

Una vez en la red, un dispositivo puede desasociarse ya sea por pedido del coordinador o router (dispositivos padres) o por sí mismo.

#### 1.2.4.2.2 Modelo de transferencia de tramas

La comunicación entre coordinador y un dispositivo puede darse de las siguientes formas:

1. Transferencia de datos hacia el coordinador
2. Transferencia de datos desde el coordinador

Para la transferencia de datos hacia el coordinador, en el caso de una red que utilice beacon-enable, el dispositivo busca el beacon o baliza para sincronizarse a la estructura de la supertrama.

Luego utiliza el método CSMA/CA con slots de tiempo para transmitir la información (Figura 1.25).

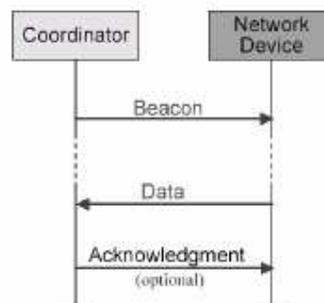


Figura 1.25 Transferencia de datos hacia el coordinador (beacon-enable)

Para una red que no utilice beacon-enable, el dispositivo utiliza el método CSMA/CA sin slots para transmitir la información (Figura 1.26).

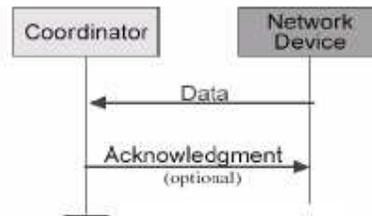


Figura 1.26 Transferencia de datos hacia el coordinador (CSMA/CA)

Para la transferencia de datos desde el coordinador, en una red beacon-enable (con balizas), el coordinador indica en el beacon que existen datos pendientes. El dispositivo periódicamente escucha el beacon y transmite un comando de pedido MAC usando la técnica CSMA/CA con slots de tiempo, si es necesario (Figura 1.27).

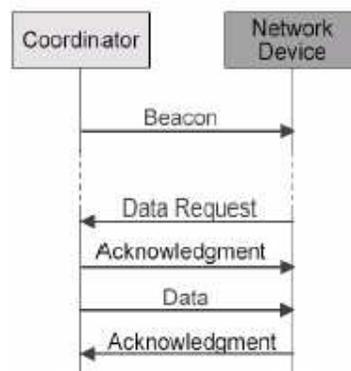


Figura 1.27 Transferencia de datos desde el coordinador (beacon-enable)

En una red sin beacon-enable, el dispositivo transmite un comando de pedido MAC usando CSMA/CA sin segmentación. Si el coordinador tiene datos pendientes, transmite sus datos bajo la misma técnica. En caso de no tener datos, el coordinador envía una trama de datos con un payload de longitud cero (Figura 1.28).

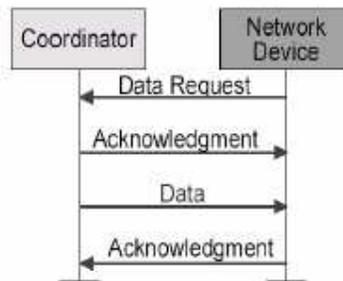


Figura 1.28 Transferencia de datos desde el coordinador (CSMA/CA)

En el presente capítulo se describió las especificaciones de la tecnología Zigbee. En el siguiente capítulo se describirá las topologías escogidas para el diseño e implementación del sistema. También se describirá el lugar específico de instalación de los equipos.

## CAPITULO 2

### DISEÑO E IMPLEMENTACION DEL HARDWARE DEL SISTEMA

En este capítulo se describirá las características de la topología física y lógica utilizadas y el lugar específico de instalación de los equipos en el laboratorio de informática. También se describirá las características de los elementos utilizados para el diseño, en donde constan como principales los elementos Zigbee y microprocesadores. Como parte final se describirá paso a paso la construcción de los módulos utilizados para la implementación del sistema.

#### 2.1 TOPOLOGIA FISICA

La topología física que se seleccionó es la topología en estrella. Esta topología permite cumplir con las necesidades de conexión física del presente proyecto. Estas necesidades de conexión física hacen referencia a la comunicación de los dispositivos finales con el coordinador, no existiendo forma de que los dispositivos finales se comuniquen entre sí. (Figura 2.1)

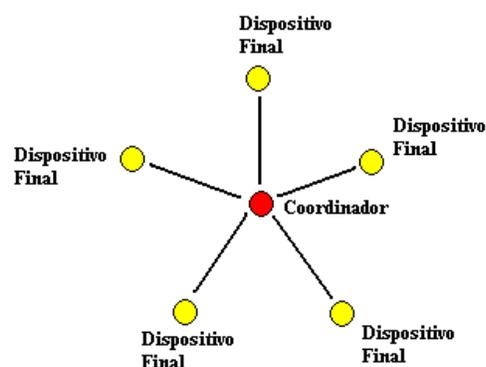


Figura 2.1 Topología física en estrella

El coordinador es un dispositivo del tipo FFD mientras que los dispositivos finales son del tipo RFD. El presente proyecto consta de un dispositivo FFD y cinco dispositivos RFD. La topología en estrella y los seis dispositivos Zigbee conforman la red WPAN.

## **2.2 TOPOLOGIA LOGICA**

La topología lógica que se seleccionó es la topología en estrella la cual permite la comunicación lógica entre dispositivos finales con el coordinador.

## **2.3 LUGAR DE INSTALACION DE LOS EQUIPOS**

El sistema de alarma consta de un modulo central (coordinador) y cinco dispositivos finales. Los dispositivos finales corresponden a los sensores y se dividen en dos tipos:

1. Sensores de movimiento
2. Sensores magnéticos

El sistema se diseñó con dos sensores de movimiento y tres sensores magnéticos.

El lugar de instalación de los equipos se observa en la Figura 2.2:

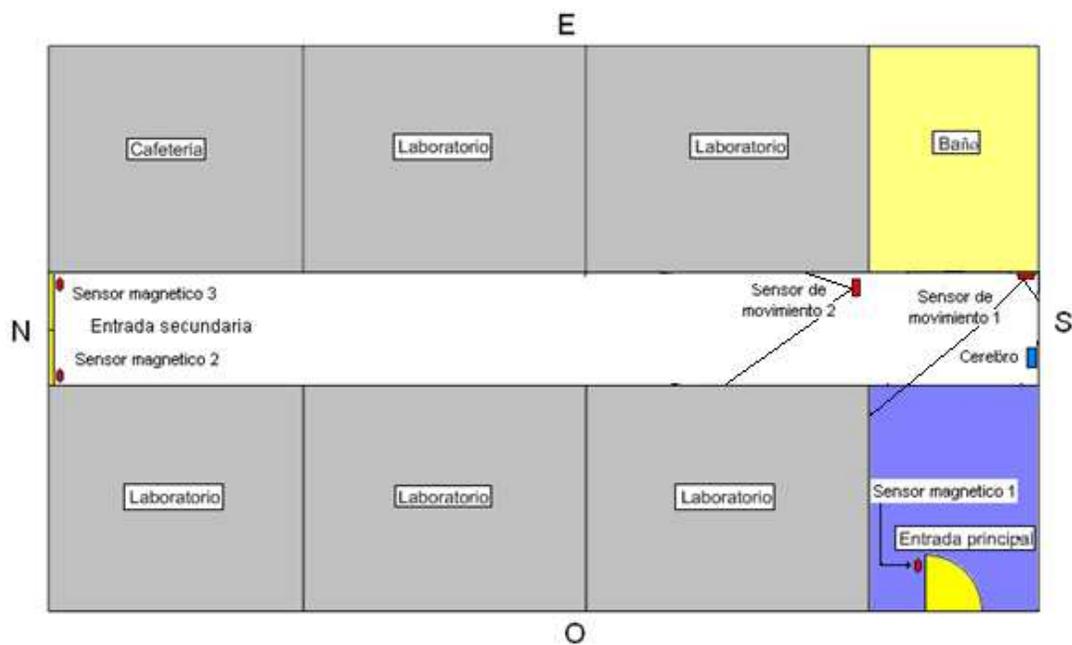


Figura 2.2 Lugar de instalación de los equipos

Los sensores magnéticos se instalaron tanto en la puerta principal como en las dos puertas secundarias (posteriores), mientras que los dos sensores de movimiento se instalaron de la siguiente forma:

Sensor de movimiento 1 (Figura 2.3)



Figura 2.3 Lugar de instalación del sensor de movimiento 1

Sensor de movimiento 2 (Figura 2.4)

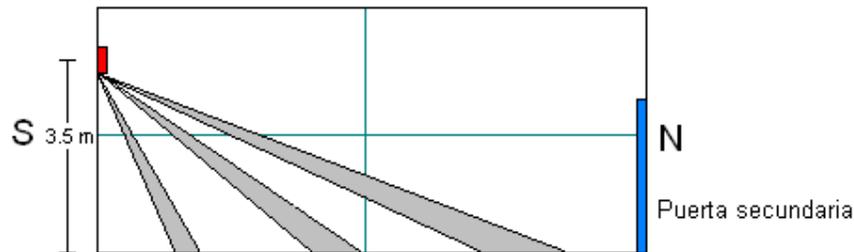


Figura 2.4 Lugar de instalación del sensor de movimiento 2

## 2.4 CARACTERÍSTICAS DE LOS ELEMENTOS UTILIZADOS

La red WPAN conforma el nivel de comunicaciones del sistema de alarma, por medio del estándar Zigbee (802.15.4) y utilizando dispositivos Xbee.

Bajo el nivel de comunicaciones existe un nivel que maneja el procesamiento de datos, con el uso de dispositivos microcontroladores del tipo PIC.

### 2.4.1 DISPOSITIVOS XBEE

“Los dispositivos Xbee proveen comunicaciones inalámbricas confiables sobre redes 802.15.4 Zigbee.”<sup>2.1</sup>

“De toda la serie de dispositivos Xbee disponibles se ha utilizado los de la serie 1 puesto que soportan topología en estrella, además estos dispositivos son de corto alcance y mantienen un performance inalámbrico excelente con un costo reducido y un tamaño pequeño.”<sup>2.1</sup>

“Estos dispositivos de la serie 1 están basados en un chip Zigbee 802.15.4 de Freescale donde las características del firmware cargado lo hacen ideal para comunicaciones punto a punto.”<sup>2.1</sup>

“Estos dispositivos dan al usuario un control máximo sobre la red y un mínimo de latencia.”<sup>2.1</sup>

#### 2.4.1.1 Especificaciones

Especificaciones generales	Series 1
Silicon	Freescale
Firmware	802.15.4
Topologías de red	Punto-punto; Punto-Multipunto
Rango urbano indoor	30 m
Rango con línea de vista outdoor	90 m

Tabla 2.1 Especificaciones generales de los dispositivos Xbee

##### 2.4.1.1.1 Características generales

- Interfaz de datos seriales  
3.3V CMOS UART
- Método de configuración  
Comandos AT o API, localmente o por aire
- Banda de frecuencia:  
2.4 GHz
- Inmunidad a interferencia  
Canales DSSS (Direct Sequence Spreads Spectrum)
- Velocidad de transmisión  
1200-250000 bps  
6 entradas ADC de 10 bits  
8 entradas/salidas digitales

#### *2.4.1.1.2 Performance*

- Potencia de transmisión de salida  
1 mW (0dBm)
- Sensibilidad de recepción  
-92 dBm

#### *2.4.1.1.3 Seguridad y Networking*

- Encriptación  
AES 128-bit
- Entrega confiable de paquetes  
Reintentos y acuses de recibo
- Identificador PAN  
Direcciones de 64 bits IEEE MAC
- Canales  
16

#### *2.4.1.1.4 Requerimientos de energía*

- Voltaje de alimentación  
2.8-3.4 VDC
- Corriente de transmisión  
45 mA @3.3V
- Corriente de recepción  
50 mA @3.3V
- Corriente Power-Down  
<10 uA

#### *2.4.1.1.5 Antena*

- Wire Whip Antena

### 2.4.1.1.6 Aprobaciones regulatorias

- U.S. (FCC part 15.247): OUR-XBEE/OUR-XBEEPRO
- Canada (IC): 4214A-XBEE/4214A-XBEEPRO
- Europa (CE): ETSI/ETSI
- Australia
- Japan

### 2.4.1.1.7 Dimensiones

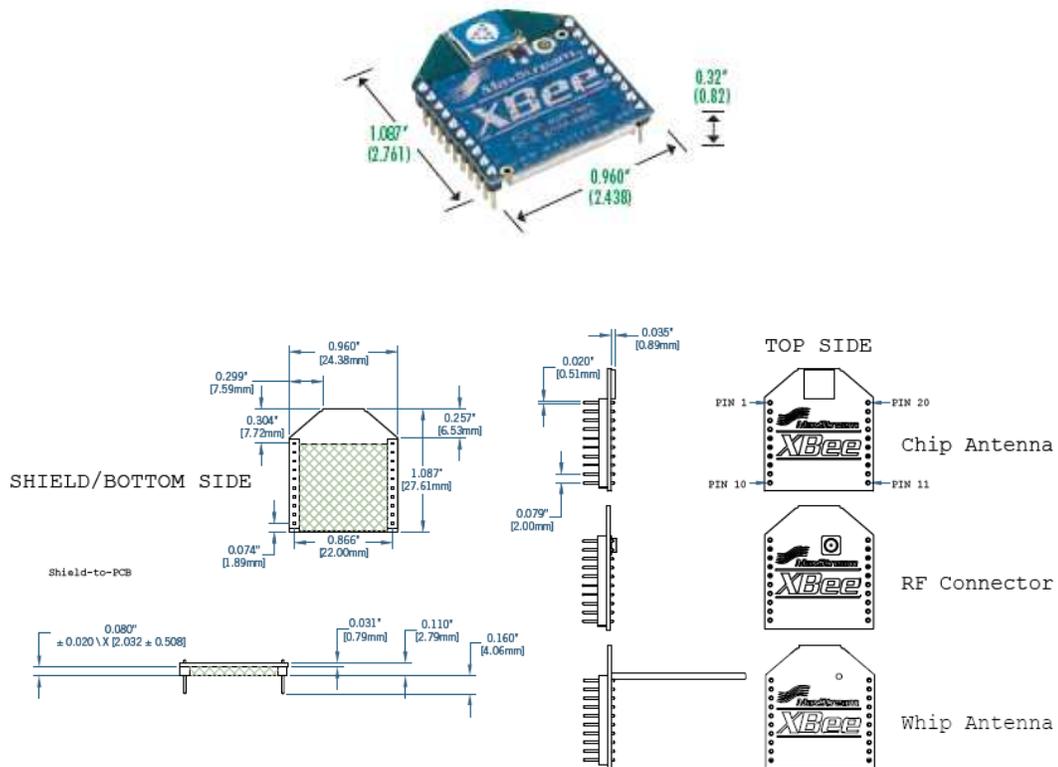


Figura 2.5 Dimensiones de los dispositivos Xbee

### 2.4.1.2 Descripción de los pines

PIN	NOMBRE	DIRECCION	DESCRIPCION
1	VCC	-	Power supply
2	DOUT	Output	UART Data out
3	DIN/ <i>CONFIG</i>	Input	UART Data in
4	DO8*	Output	Digital Output 8
5	<i>RESET</i>	Input	Module reset (200 ns)
6	PWM0/RSSI	Output	PWM output 0 / RX signal strength indicator
7	PWM1	Output	PWM output 1
8	Reserved	-	Do not connect
9	<i>DTR</i> /SLEEP_RQ/DI8	Input	Pin sleep control line or digital input 8
10	GND	-	Ground
11	AD4/DIO4	Either	Analog input or digital I/O 4
12	<i>CTS</i> /DIO7	Either	Clear to send flow control or digital I/O7
13	ON / <i>SLEEP</i>	Output	Module status indicador
14	VREF	Input	Voltage reference for A/D inputs
15	Associate/AD5/DIO5	Either	Associated indicator, analog input 5 or digital I/O 5
16	<i>RTS</i> /AD6/DIO6	Either	Request to send flow control, analog input 6 or digital I/O 6
17	AD3 / DIO3	Either	Analog input 3 or digital I/O 3
18	AD2 / DIO2	Either	Analog input 2 or digital I/O 2
19	AD1 / DIO1	Either	Analog input 1 or digital I/O 1
20	AD0 / DIO0	Either	Analog input 0 or digital I/O 0

Tabla 2.2 Descripción de los pines de los dispositivos Xbee

### 2.4.1.3 Notas de diseño

- Conexiones mínimas: VCC,GND,DOUT,DIN

- Conexiones mínimas para actualización de firmware:  
VCC,GND,DIN,DOUT,RTS,DTR
- El modulo incluye resistencia de pull-up al  $\overline{RESET}$
- Muchas de las entradas pull-ups pueden ser configuradas usando el comando PR
- Los pines no usados deben ser desconectados

#### 2.4.1.4 Kit de desarrollo

Para la inicialización en el modo de trabajo de los dispositivos Xbee se utilizo el kit de desarrollo Xbee (Figura 2.6) el cual contiene los siguientes elementos:

- (2) XBee 802.15.4 / Wire Antena
- Modulo de desarrollo RS-232
- Modulo de desarrollo USB
- Cable serial RS-232
- Cable USB
- Adaptador de poder
- Clip para batería de 9V
- Adaptador DB9



Figura 2.6 Kit de desarrollo Xbee

### 2.4.1.5 Software y hardware para la configuración de los dispositivos Xbee

El software que se utilizó para la configuración de los dispositivos Xbee es el X-CTU (Figura 2.7) proveído por la compañía Digi. El software X-CTU contiene cuatro módulos:

1. Módulo de configuración de PC: Utilizado para la configuración de los puertos seriales para la interfaz PC-Módulo Xbee.
2. Módulo de test: Utilizado para realizar pruebas de rango de señal de los módulos Xbee y monitorear paquetes enviados y recibidos.
3. Módulo terminal: Utilizado para configurar y leer los parámetros del modulo Xbee por medio de comandos AT.
4. Módulo de configuración modem: Utilizado para configurar y leer los parámetros del modulo Xbee por medio de una interfaz gráfica.

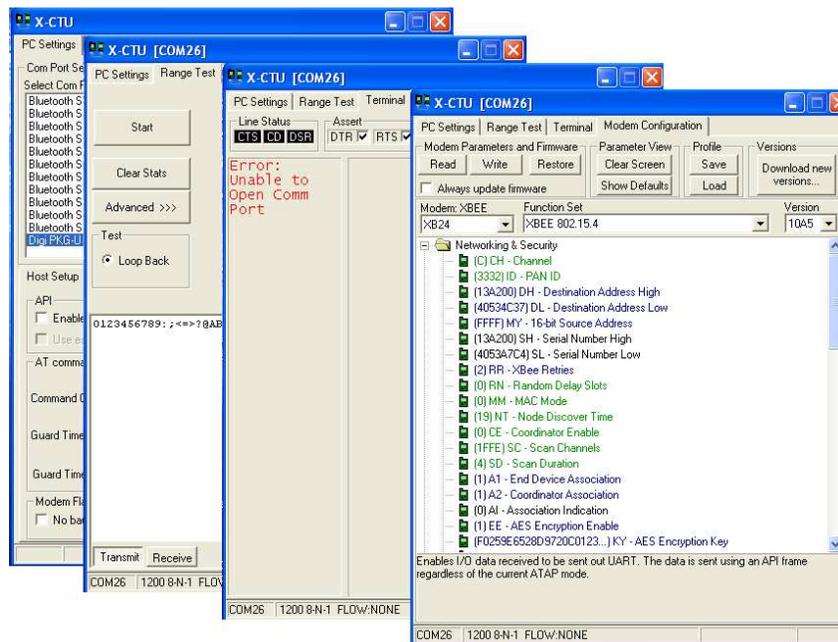


Figura 2.7 Software X-CTU

El hardware que se utilizó para la configuración de los dispositivos Xbee es el módulo de desarrollo USB (Figura 2.8) incluido en el kit de desarrollo Xbee.



Figura 2.8 Módulo de desarrollo USB

#### 2.4.2 MICROCONTROLADOR PIC 16F877A

El microcontrolador 16F877A pertenece a una gran familia de microcontroladores de 8 bits cuyas características de arquitectura Harvard, tecnología RISC y tecnología CMOS lo distinguen de los demás. Debido a estas características este dispositivo es altamente efectivo en el uso de memoria de datos y programa y por lo tanto en velocidad de ejecución.

### 2.4.2.1 Especificaciones

Especificaciones básicas	PIC 16F877A
Frecuencia de operación	DC-20 MHz
Memoria flash de programación( palabras de 14 bits)	8K
Memoria de datos (bytes)	368
Memoria de datos EEPROM (bytes)	256
Interrupciones	15
Puertos I/O	A,B,C,D,E
Timers	3
Comunicación serial	MSSP, USART
Comunicaciones paralelas	PSP
Modulo A/D 10 bits	8 canales de entrada
Comparadores analógicos	2
Set de instrucciones	35

Tabla 2.3 Especificaciones básicas del microcontrolador PIC 16F877A

El empaquetado del PIC que se utilizó es el PDIP (Plastic dual in line package) y la distribución de pines se observa en la Figura 2.9

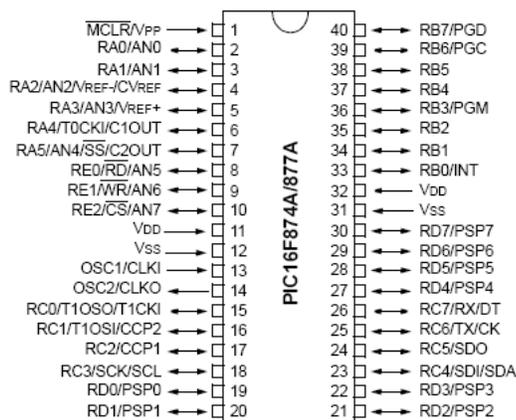


Figura 2.9 Distribución de pines del microcontrolador PIC 16F877A

El PIC 16F877A tiene una memoria flash con un rango de voltaje estándar de 4.5-6 V y tiene la posibilidad de configurar 8 diferentes tipos de osciladores, tres de los cuales trabajan con cristales externos y se muestran a continuación:

Modo	Frecuencia típica	Capacitores recomendados	
		C1	C2
LP	32 khz	68 a 100 pf	68 a 100 pf
	200 khz	15 a 30 pf	15 a 30 pf
XT	100 khz	68 a 150 pf	150 a 200 pf
	2 Mhz	15 a 30 pf	15 a 30 pf
HS	4 Mhz	15 a 30 pf	15 a 30 pf
	8 Mhz	15 a 30 pf	15 a 30 pf
	10 Mhz	15 a 30 pf	15 a 30 pf
	20 Mhz	15 a 30 pf	15 a 30 pf

Tabla 2.4 Osciladores externos para el microcontrolador PIC 16F877A

La conexión para el cristal externo se muestra en la Figura 2.10

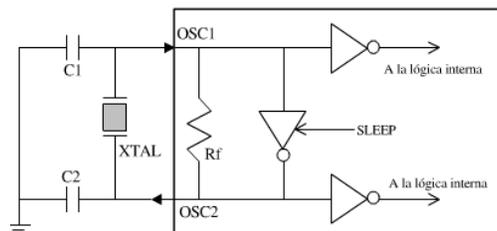


Figura 2.10 Conexión del cristal externo para el microcontrolador 16F877A

Las cinco opciones restantes de oscilador trabajan con un cristal interno de 4 MHz con un rango de error de  $\pm 1.5\%$ .

La memoria del PIC 16F877A está dividida en dos:

1. La memoria de programa
2. La memoria de datos

La memoria de datos a su vez está dividida en registros de propósito general y registros de propósito especial y está organizada en 4 bancos numerados 0, 1, 2 y 3, los cuales pueden ser accedidos por medio de direccionamiento directo e indirecto.

#### 2.4.2.2 Software y hardware para programación del PIC 16F877A

El software que se utilizó para la programación del PIC 16F877A es el WinPic800 (Figura 2.11)

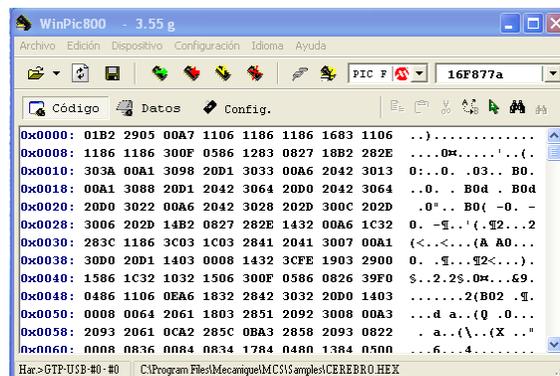


Figura 2.11 Software para la programación del PIC 16F877A

El hardware que se utilizó para la programación del PIC 16F877A es el programador universal de microcontroladores PIC (Figura 2.12)



Figura 2.12 Hardware para la programación del PIC 16F877A

## **2.5 DISEÑO DEL HARDWARE**

El hardware del sistema de alarma se divide en dos partes principales:

1. El cerebro del sistema
2. Los periféricos de sistema

El cerebro del sistema es el elemento que comanda el monitoreo anti-intrusos por medio de periféricos, los cuales básicamente son sensores anti-intrusos.

De acuerdo al diseño del sistema, al cerebro se lo ha dividido en dos partes:

1. Hardware para procesamiento de datos
2. Hardware para comunicación de datos

Mientras que para los periféricos solo existe:

1. Hardware para comunicación de datos

El hardware para procesamiento de datos está formado por el PIC 16F877A y su respectiva programación.

El hardware para comunicación de datos está formado por los dispositivos Xbee y su respectiva configuración.

### **2.5.1 DISEÑO DEL CEREBRO DEL SISTEMA**

El cerebro es la parte principal del sistema de alarma. En el diseño se consideró que el cerebro realice diversas actividades de control, dentro de las cuales las más importantes son:

1. Control de activación y desactivación del sistema de alarma

2. Control del sistema de mando para usuario
3. Control de activación y desactivación del sistema de monitoreo

La activación y desactivación del sistema de alarma se realiza por instrucción de los periféricos quienes envían una señal hacia el cerebro del sistema. Este activa la sirena y envía la señal de intruso al sistema de monitoreo.

El sistema de mando se complementa con un LCD que recibe datos del cerebro y un teclado que envía datos hacia el cerebro.

La activación y desactivación del sistema de monitoreo se realiza por instrucción del cerebro, el cual, luego de recibir una señal de cualquier periférico, activa el sistema de alarma e informa al sistema de monitoreo.

El cerebro del sistema se compone de un microcontrolador PIC 16F877A. Este microcontrolador ha sido tomado como base del hardware de procesamiento de datos debido a su robustez y facilidad de programación e instalación. Además, sus puertos posibilitan la conexión de todos los elementos necesarios para el presente diseño.

El cerebro del sistema se compone de un modulo Xbee. Este modulo ha sido tomado como base del hardware para comunicación de datos debido a la facilidad de programación y simpleza de instalación. Además, por ser un modulo compacto que no necesita otros elementos para su funcionamiento.

Los elementos principales que se interconectan al microcontrolador son:

1. Un teclado matricial 4x4
2. Un LCD 2x16
3. Tres leds indicadores de actividad
4. Un modulo Xbee
5. Una computadora

### 2.5.1.1 Construcción del cerebro del sistema

Se ha tomado como base para el hardware de procesamiento de datos al microcontrolador PIC 16F877A. Este microcontrolador comanda 5 módulos que complementan el cerebro del sistema, estos módulos son:

1. Interfaz de usuario
2. Leds indicadores de actividad
3. Sirena
4. Puerto de comunicación con la PC
5. Dispositivo Xbee

La interfaz de usuario está compuesta de un teclado 4x3 con el cual el usuario controla las claves de habilitación y deshabilitación del sistema y un LCD 2x16 por medio del cual el sistema guía al usuario. La interfaz de usuario se comunica con el microcontrolador por medio de un cable de datos multipar y conectores DB15 hembras en las placas y machos en el cable.

Los leds indicadores de actividad se conectan directamente al microcontrolador y de acuerdo a sus colores indican: sistema habilitado con color verde, sistema deshabilitado con color amarillo y sistema activado con color rojo.

La sirena se conecta directamente al microcontrolador por medio de un relé y su activación actúa en paralelo con la activación del sistema.

La PC, la cual tiene instalado el software de monitoreo<sup>2.2</sup> se conecta al microcontrolador por medio de su puerto de comunicaciones serial RS232.

El dispositivo Xbee se conecta directamente al microcontrolador y comunica a este con los periféricos del sistema.

En la Figura 2.13 se puede observar el esquema del diseño del cerebro del sistema.

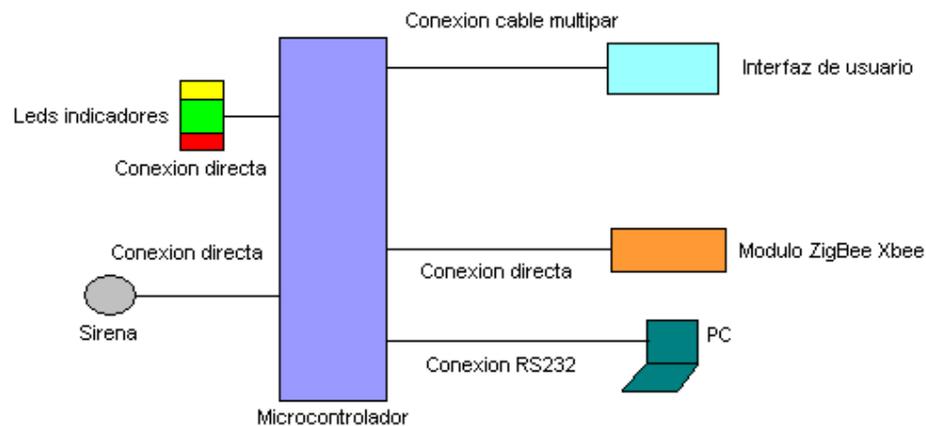


Figura 2.13 Esquema de diseño del cerebro del sistema

Los elementos utilizados en la construcción del cerebro del sistema son:

1. 1 microcontrolador 16F877A
2. 1 pulsador
3. 2 capacitores de 22pF
4. 1 cristal de 4 MHz
5. 3 resistencias de 330Ω
6. 3 leds
7. 2 borneras
8. 2 capacitores de 1Uf
9. 1 regulador 7805
- 10.1 resistencia de 100Ω
- 11.1 resistencia de 10 kΩ
- 12.1 transistor 2N3904
- 13.1 relé de 5V
- 14.1 diodo 1N4007
- 15.1 LM317
- 16.6 capacitores de 10uF
- 17.2 resistencias de 100 kΩ

- 18.1 MAX232
- 19.1 conector db9 hembra para placa
- 20.1 conector db15 hembra para placa
- 21.1 dispositivo Xbee
- 22.1 resistencia 1 k $\Omega$

En la Figura 2.14 se puede observar el esquema del circuito del cerebro del sistema

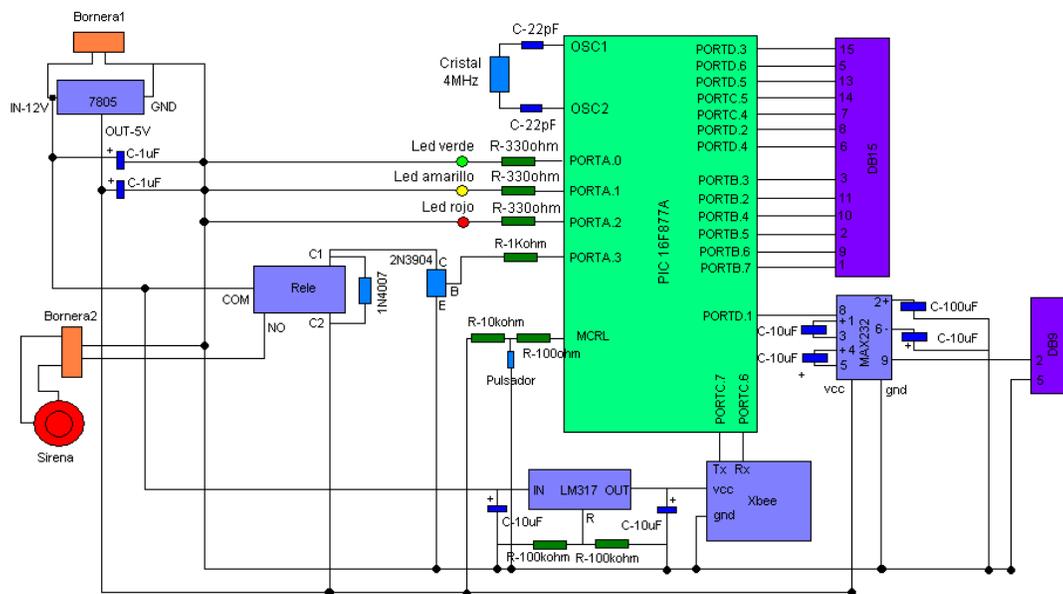


Figura 2.14 Esquema del circuito del cerebro del sistema

#### 2.5.1.1.1 PIC 16F877A

El PIC 16F877A comanda los módulos del cerebro del sistema por medio de sus puertos de entrada y salida:

### ***Puertos I/O para comandar el teclado***

El teclado consta de 4 filas y 3 columnas con 7 conectores, uno por cada fila y cada columna. El microcontrolador utiliza los siguientes 7 puertos para la conexión:

Fila 1	PORTD.3 (Pin 22)
Fila 2	PORTD.6 (Pin 29)
Fila 3	PORTD.5 (Pin 28)
Fila 4	PORTC.5 (Pin 24)
Columna 1	PORTC.4 (Pin 23)
Columna 2	PORTD.2 (Pin 21)
Columna 3	PORTD.4 (Pin 27)

### ***Puertos I/O para comandar el LCD***

El LCD consta de 16 conectores, 6 de los cuales se interconectan con el microcontrolador el cual utiliza los siguientes puertos para la conexión:

R/S	PORTB.3 (Pin 36)
E	PORTB.2 (Pin 35)
D4	PORTB.4 (Pin 37)
D5	PORTB.5 (Pin 38)
D6	PORTB.6 (Pin 39)
D7	PORTB.7 (Pin 40)

Se ha realizado la conexión de R/W directamente a tierra puesto que el LCD se utiliza solo para escritura.

Se ha usado 4 de los 8 conectores de datos para el envío de caracteres hacia el LCD puesto que el sistema de programación utilizado permite el envío de los 4 bits más altos primero y luego los 4 bits más bajos. Esto no ocasiona problemas debido a que el LCD trabaja en microsegundos.

### ***Puertos I/O para comandar los leds indicadores de actividad y Sirena***

LED Verde	PORTA.0 (Pin 2)
LED Amarillo	PORTA.1 (Pin 3)
LED Rojo	PORTA.2 (Pin 4)
Sirena	PORTA.3 (Pin 5)

### ***Puertos I/O para comandar el dispositivo Xbee***

El dispositivo Xbee es el elemento de comunicación de datos por aire. Para la interconexión del microcontrolador y el dispositivo Xbee se necesitan 2 puertos:

TX Xbee	PORTC.7 (Pin 26)
RX Xbee	PORTC.6 (Pin 25)

### ***Puertos I/O para comandar el sistema de monitoreo***

El sistema de monitoreo es un software grafico que indica que dispositivo dentro del sistema se ha activado. Este sistema identifica el dispositivo activado de acuerdo a la información enviada por el cerebro del sistema. Para el envío de esta información se ha utilizado un puerto del microcontrolador:

RX serial PC	PORTD.1 (Pin 20)
--------------	------------------

### ***Puertos generales***

El puerto 1 del microcontrolador corresponde al  $\overline{MCRL}$ , a este puerto se conecta un circuito típico de reset. Este circuito se muestra en la Figura 2.15

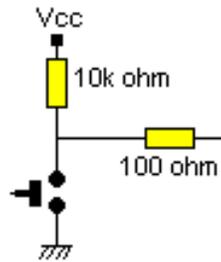


Figura 2.15 Circuito básico de reset para el microcontrolador PIC16F877A

#### 2.5.1.1.2 Dispositivo Xbee

Los dispositivos Xbee se conectan directamente al microcontrolador por medio del uso de dos de sus pines, el de transmisión y el de recepción UART como se observa en la Figura 2.16

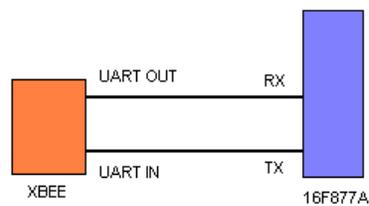


Figura 2.16 Esquema de conexión Xbee-PIC16F877A

El dispositivo Xbee fue configurado de la siguiente forma:

Parámetro	Configuración
Numero serial high	0013A200
Numero serial low	40534C37
Identificador de nodo (NI)	CEREBRO
Canal (CH)	15
Pan ID (ID)	1A5C
Dirección de destino high (DH)	FFFFFFFF
Dirección de destino low (DL)	FFFFFFFF
Dirección de origen de 16 bits (MY)	FFFF
Random delay slot (RN)	1
Coordinador habilitado (CE)	1 (coordinador)
Habilitación de encriptación AES (EE)	1(habilitada)
Velocidad de interfaz de datos (BD)	0(1200 bps)
Configuración DIO7 (D7)	0(deshabilitado CTS control de flujo)
Configuración DIO5 (D5)	0(deshabilitado indicador de asociación)
Habilitación I/O output (IU)	1(habilitado)

Tabla 2.5 Programación del dispositivo Xbee del cerebro del sistema

Todos los demás parámetros de programación que no se han descrito están configurados por default. En el Anexo 2<sup>2.3</sup> se puede observar los parámetros de programación.

### 2.5.1.2 Ruteo del cerebro del sistema

Luego de haber diseñado el cerebro del sistema y haber detallado las conexiones que se utilizaron, se realizó el ruteo del mismo (Figura 2.17) para proceder con la construcción física de la baquelita:

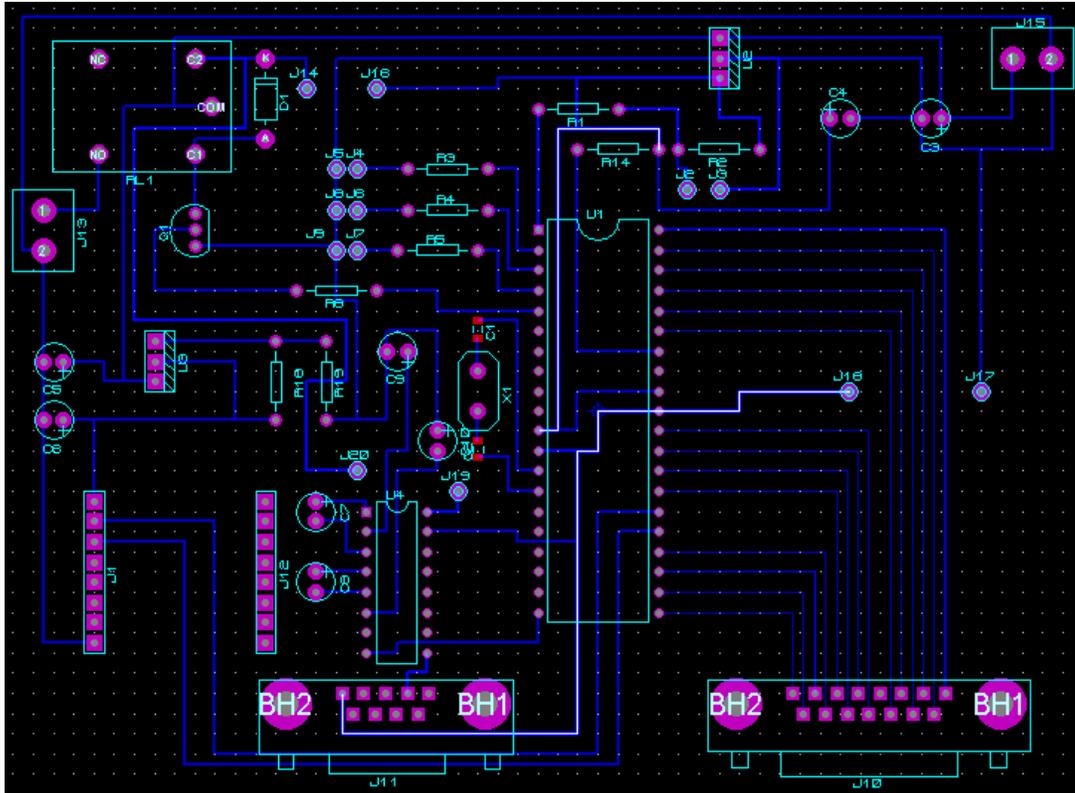


Figura 2.17 Ruteo del cerebro del sistema

### 2.5.1.3 Construcción de la interfaz de usuario

La interfaz de usuario está compuesta por un teclado de 4 filas y 3 columnas, y un display LCD 2 x 16. Para controlar el contraste del LCD se ha utilizado un divisor de tensión con 2 resistencias de  $1\text{k}\Omega$  y  $10\text{k}\Omega$ , y para controlar la intensidad del backlite del LCD se ha utilizado una resistencia de  $100\Omega$ , como se puede observar en la Figura 2.18

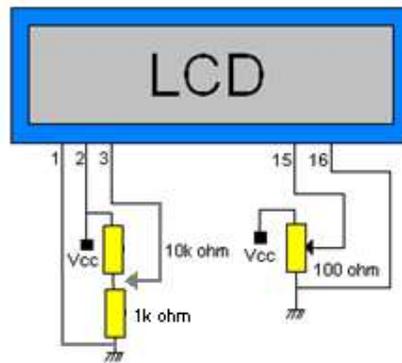


Figura 2.18 Esquema de diseño para controlar contraste y baklite del LCD

Para la conexión entre la interfaz de usuario y el cerebro se ha utilizado un cable multipar con 14 conexiones en modo directo (Figura 2.19). Las 14 conexiones se describen a continuación:

- |              |                   |
|--------------|-------------------|
| 1. PORTB.7-  | D7 LCD            |
| 2. PORTB.5-  | D5 LCD            |
| 3. PORTB.3-  | R/S LCD           |
| 4. N/A       |                   |
| 5. PORTD.6-  | FILA2 TECLADO     |
| 6. PORTD.4-  | COLUMNA 3 TECLADO |
| 7. PORTC.4-  | COLUMNA 1 TECLADO |
| 8. PORTD.2-  | COLUMNA 2 TECLADO |
| 9. PORTB.6-  | D6 LCD            |
| 10. PORTB.4- | D4 LCD            |
| 11. PORTB.2- | E LCD             |
| 12. N/A      |                   |
| 13. PORTD.5- | FILA3 TECLADO     |
| 14. PORTC.5- | FILA 4 TECLADO    |
| 15. PORTD.3- | FILA 1 TECLADO    |

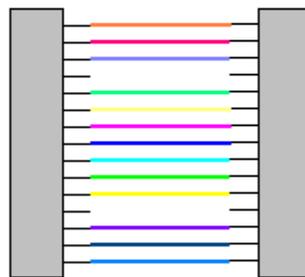


Figura 2.19 Conexión en modo directo de cable multipar

Los elementos utilizados en la construcción de la interfaz de usuario son:

- 1 regulador 7805
- 1 bornera
- 1 conector db15 hembra para placa
- 1 teclado 4x3
- 1 LCD 2x16
- 3 resistencias de 4,7 k $\Omega$
- 1 resistencia de 1k $\Omega$
- 1 resistencia de 10k $\Omega$
- 1 resistencia de 100 $\Omega$

En la Figura 2.20 se puede observar el esquema del circuito de la interfaz de usuario

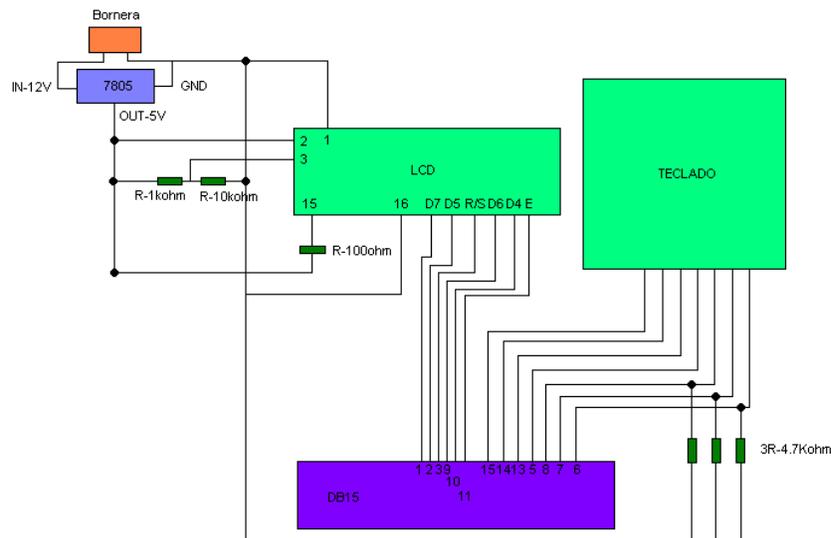


Figura 2.20 Esquema del circuito de la interfaz de usuario

#### 2.5.1.4 Ruteo de la interfaz de usuario

Luego de haber diseñado la interfaz de usuario y haber detallado las conexiones que se utilizaron, se realizó el ruteo del mismo (Figura 2.21) para proceder con la construcción física de la baquelita:

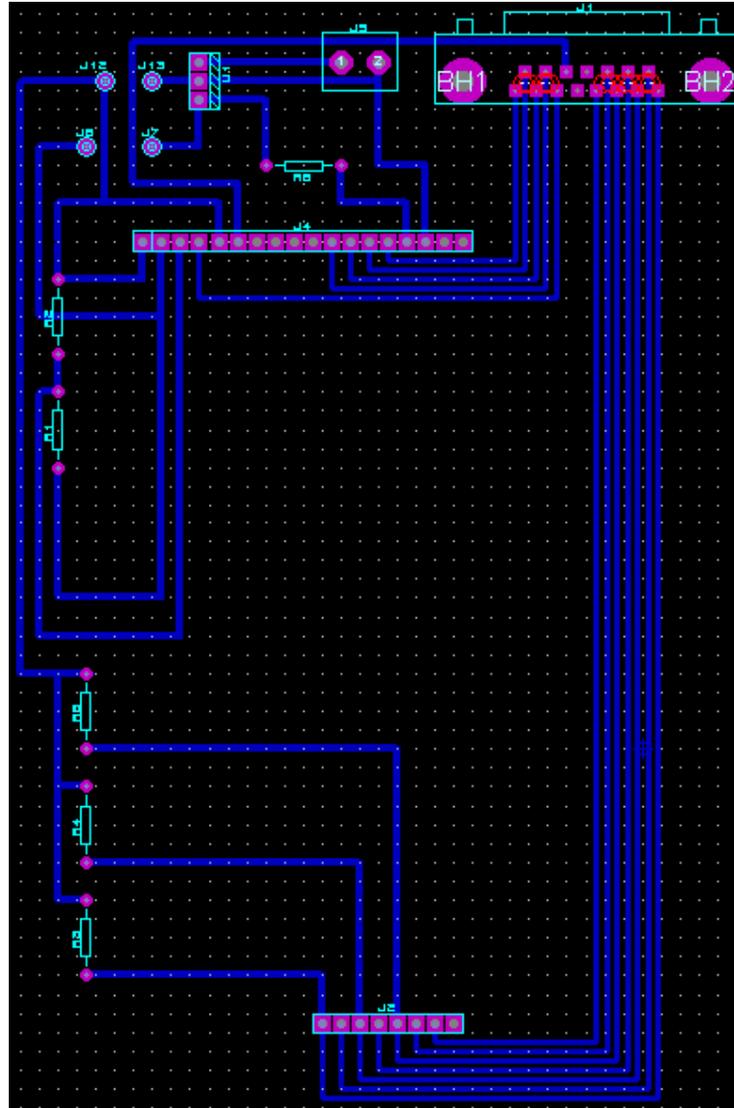


Figura 2.21 Ruteo de la interfaz de usuario

## 2.5.2 PERIFERICOS DEL SISTEMA

Los periféricos son los módulos que están conectados directamente con los sensores. En el diseño se consideró que los periféricos realicen diversas actividades de control, dentro de las cuales las más importantes son:

1. Detección directa de activación de sensores
2. Aviso de activación de sensores al cerebro del sistema

Cuando un sensor se activa, el periférico del sistema envía la señal de activación al cerebro del sistema para su procesamiento.

Los periféricos del sistema se componen de módulos Xbee. Estos módulos han sido tomados como base del hardware para comunicación de datos debido a la facilidad de programación y simpleza de instalación; además, por ser módulos compactos que no necesitan otros elementos para su funcionamiento.

Los elementos principales que se interconectan a los dispositivos Xbee son:

1. Un sensor magnético o de movimiento

Se han diseñado 5 periféricos: 2 para la interconexión con sensor de movimiento y 3 para la interconexión con sensores magnéticos.

### 2.5.2.1 Construcción de los periféricos del sistema

Los periféricos del sistema solo tienen el nivel de comunicación de datos por medio de dispositivos Xbee los cuales se interconecta con el respectivo sensor.

En la Figura 2.22 se puede observar el esquema del diseño de los periféricos del sistema

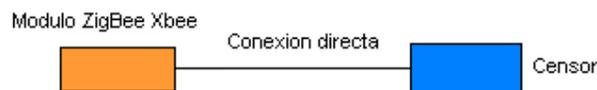


Figura 2.22 Esquema de diseño de los periféricos del sistema

Los elementos utilizados en la construcción de los periféricos son:

1. 1 LM317
2. 2 borneras

3. 2 capacitores de 10uF
4. 1 resistencia de 1k $\Omega$
5. 1 resistencia de 1.2k $\Omega$
6. 1 resistencia de 4.7k $\Omega$

En la Figura 2.23 se puede observar el esquema del circuito de los periféricos del sistema

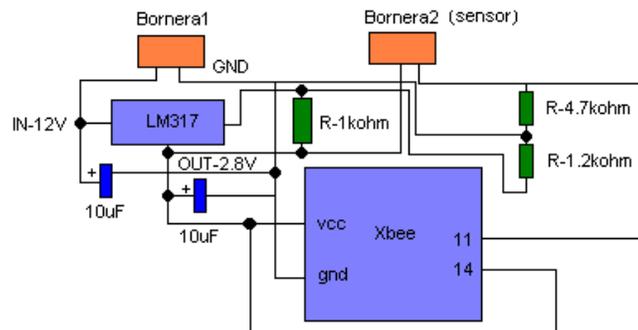


Figura 2.23 Esquema del circuito de los periféricos del sistema

#### 2.5.2.1.1 Dispositivo Xbee

Los dispositivos Xbee se conectan directamente con los sensores, por medio del uso de la conversión analógica-digital.

Los dispositivos Xbee tienen 6 pines que permiten hacer uso de esta conversión. Para que esta conversión funcione se necesita que el voltaje de referencia se encuentre entre 0 y VCC.

Cuando un pin o pines A/D son habilitados, se debe escoger un apropiado muestreo. La velocidad máxima para el muestreo es de 1 muestreo por cada ms.

Los dispositivos Xbee permiten al usuario configurar el número de muestreos antes de que los datos se transmitan. El máximo número de muestreos antes de la transmisión es de 46. La configuración del número de muestreos antes de transmitir los datos se ha mantenido en cero debido a que se ha utilizado la

opción de sleep, la cual permite realizar un muestreo cada vez que el dispositivo despierta.

En el receptor Xbee del cerebro del sistema se debe habilitar la recepción de paquetes por aire para que estos datos puedan ser enviados por la interfaz UART.

Cuando los datos son enviados por la interfaz UART estos están en formato API y tienen la siguiente estructura:

7E	delimitador de inicio
XXXX	longitud de bytes
82	identificador API de direcciones de 64 bits (83 para direcciones de 16 bits)
XXXX	
XXXX	
XXXX	
XXXX	bytes de dirección
XX	bytes de valores RSSI
XX	byte opcional
XX	byte de cantidad de muestreos
XXXX	indicador de canal
XXXX	muestreo de datos (min = 0000; máx.=03FF)
XX	checksum

En el cerebro del sistema se ha programado el PIC 16F877A de tal forma que pueda identificar el mensaje de activación de un sensor y la dirección de origen del mismo por medio de la cadena de caracteres antes descritos.

La identificación de un mensaje de activación se la realiza por medio del análisis de los bytes 18 y 19. Para el presente diseño el valor del voltaje de referencia es igual a VCC por lo que un valor de VCC corresponde a 03FF y un valor de GND corresponde a 0000.

Cuando un sensor está desactivado, es decir, en circuito cerrado, el valor de los bytes 18 y 19 corresponde a 03FF y cuando un sensor esta activado el valor de los bytes 18 y 19 corresponde a 0000.

La identificación de la dirección de origen de un sensor se la realiza por medio del análisis de los bytes 5 al 12 los cuales corresponden a los 64 bits de identificación del dispositivo Xbee.

Los 5 dispositivos Xbee mantienen una programación en común, con excepción de las direcciones de origen e identificación de nodo.

### ***Programación en común***

<b>Parámetro</b>	<b>Configuración</b>
Canal (CH)	15
Pan ID (ID)	1A5C
Dirección de destino high (DH)	13A200
Dirección de destino low (DL)	40534C37
Dirección de origen de 16 bits (MY)	FFFF
Coordinador habilitado (CE)	0 (dispositivo final)
Habilitación de encriptación AES (EE)	1(habilitada)
Modo sleep (SM)	4(sleep cíclico)
Tiempo antes de pasar a modo sleep (ST)	1(1 ms)
Periodo cíclico de sleep (SP)	64(1s)
Velocidad de interfaz de datos (BD)	0(1200 bps)
Configuración DIO7 (D7)	0(deshabilitado CTS control de flujo)
Configuración DIO5 (D5)	0(deshabilitado indicador de asociación)
Configuración DIO4 (D4)	2(ADC)
Habilitación I/O output (IU)	1(habilitado)
Muestreos antes de la transmisión (IU)	1(muestreo)

Tabla 2.6 Programación en común para los dispositivos Xbee de los periféricos

**Sensor de movimiento1**

Parámetro	Configuración
Numero serial high	0013A200
Numero serial low	40310AF6
Identificador de nodo (NI)	MOVIMIENTO1

Tabla 2.7 Programación Xbee para el sensor de movimiento 1

**Sensor de movimiento2**

Parámetro	Configuración
Numero serial high	0013A200
Numero serial low	4053A7C7
Identificador de nodo (NI)	MOVIMIENTO2

Tabla 2.8 Programación Xbee para el sensor de movimiento 2

**Sensor magnético1**

Parámetro	Configuración
Numero serial high	0013A200
Numero serial low	4053A7C6
Identificador de nodo (NI)	MAGNETICO1

Tabla 2.9 Programación Xbee para el sensor magnético 1

### **Sensor magnético2**

<b>Parámetro</b>	<b>Configuración</b>
Numero serial high	0013A200
Numero serial low	4053A7C4
Identificador de nodo (NI)	MAGNETICO2

Tabla 2.10 Programación Xbee para el sensor magnético 2

### **Sensor magnetico3**

<b>Parámetro</b>	<b>Configuración</b>
Numero serial high	0013A200
Numero serial low	40534C2F
Identificador de nodo (NI)	MAGNETICO3

Tabla 2.11 Programación Xbee para el sensor magnético 3

Todos los demás parámetros de programación que no se han descrito están configurados por default. En el Anexo 1<sup>2.3</sup> se puede observar los parámetros de programación.

#### **2.5.2.2 Ruteo de los periféricos del sistema**

Luego de haber diseñado los periféricos del sistema y haber detallado las conexiones que se utilizó, se realizó el ruteo del mismo (Figura 2.24) para proceder con la construcción física de la baquelita.

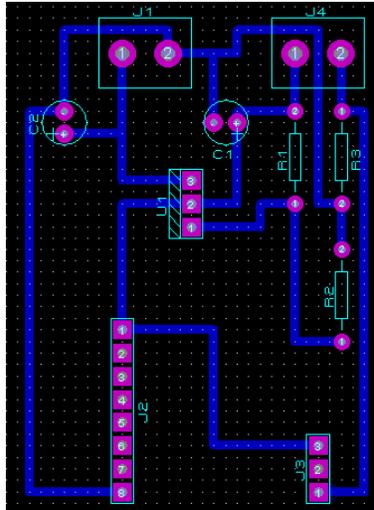


Figura 2.24 Ruteo de los periféricos del sistema

## 2.6 FUENTE DE ENERGIA

La fuente de energía que se ha utilizado para polarizar a los dispositivos es una fuente de 12V, 1A máx. Además de esta fuente se ha utilizado una batería de 12V en caso de falla en el suministro de energía eléctrica. Esta batería provee de energía al sistema por algunas horas hasta que el suministro de energía se normalice. El análisis del consumo de corriente del sistema se describe en el Capítulo 4.

La fuente de energía se ha diseñado con el esquema de 4 pasos: Transformación, rectificación, filtrado y regulación.

Los elementos utilizados en la construcción de la fuente de energía son:

1. 1 transformador MIYAKO LP-573 117 VAC/12-0-12 VDC
2. 1 rectificador de onda completa puente de diodos W10
3. 1 Capacitor de 1000  $\mu$ F

4. 1 Regulador 7812A
5. 1 led indicador de actividad
6. 1 resistencia 1,2 k $\Omega$
7. 2 borneras

En la Figura 2.25 se puede observar el esquema del circuito de la fuente de energía

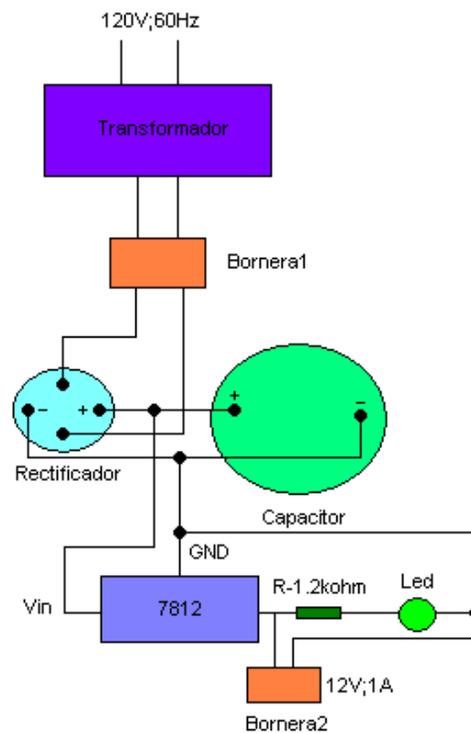


Figura 2.25 Esquema del circuito de la fuente de energía

Luego de haber diseñado la fuente de energía se realizó el ruteo de la misma (Figura 2.26) para proceder con la construcción física de la baquelita.

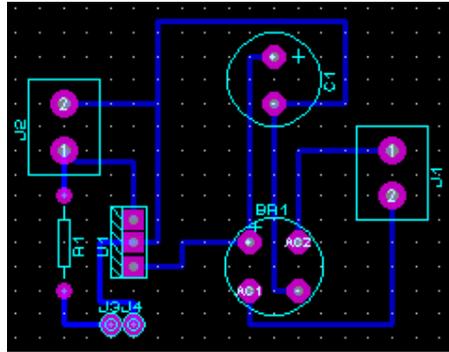


Figura 2.26 Ruteo de la fuente de energía

## 2.7 IMPLEMENTACION DEL HARDWARE

Luego de haber realizado la construcción física de las baquelitas descritas anteriormente se realizó la construcción de las cajas portadoras de las mismas. Estas cajas se construyeron con aluminio de 0.5 mm con el diseño mostrado en la Figura 2.27

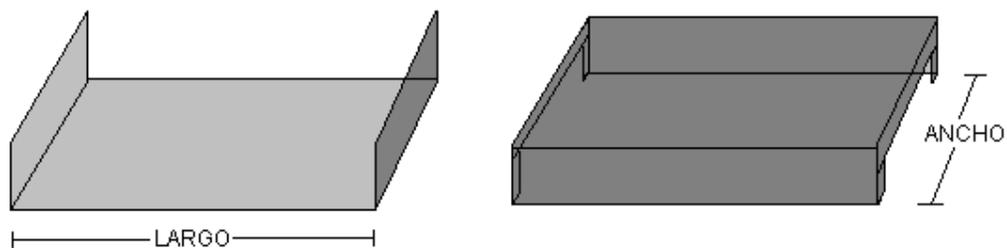


Figura 2.27 Cajas metálicas portadoras de los circuitos

Se ha construido las cajas de las baquelitas con las siguientes medidas (Tabla 2.12):

Modulo	Medidas de baquelita	Medidas de caja
Cerebro	Largo: 10.1 cm Ancho:14.1 cm	Largo: 10.5 cm Ancho:14.5 cm
Interfaz de usuario	Largo:14.6 cm Ancho:10.1 cm	Largo: 15 cm Ancho:10.5 cm
Periféricos	Largo: 6 cm Ancho:4.7 cm	Largo:6.4 cm Ancho:5.1 cm

Tabla 2.12 Medias de las cajas portadoras de los circuitos

***Cerebro del sistema (Figura 2.28)***

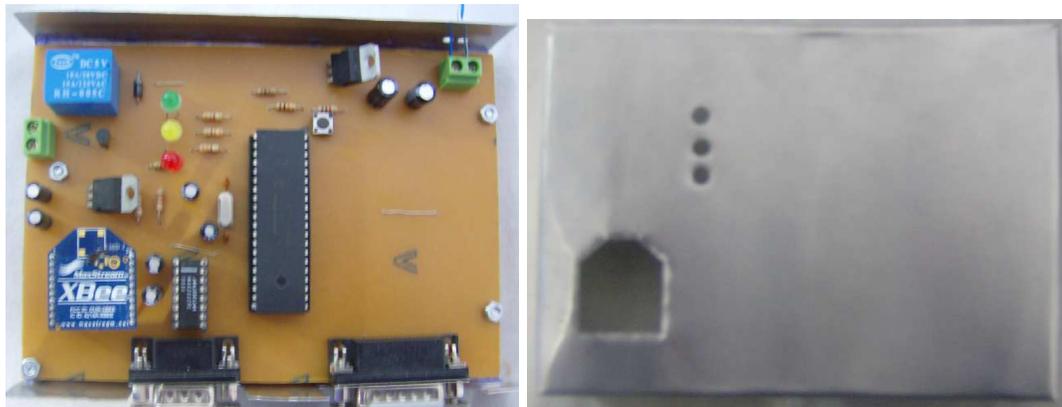


Figura 2.28 Circuito y caja del cerebro del sistema

***Interfaz de usuario (Figura 2.29)***

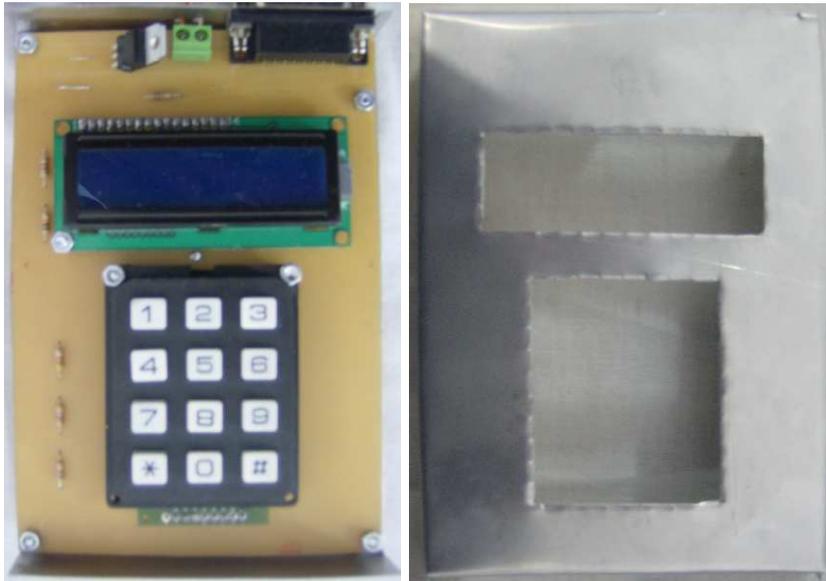


Figura 2.29 Circuito y caja del interfaz de usuario

***Periféricos del sistema (Figura 2.30)***

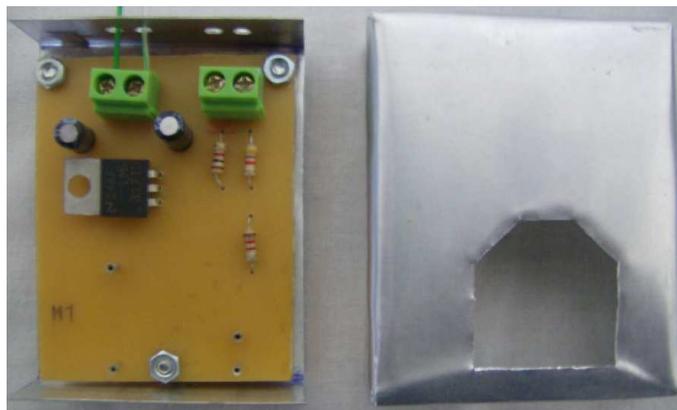


Figura 2.30 Circuito y caja de los periféricos del sistema

La instalación de los equipos en el laboratorio, se realizó de acuerdo a lo descrito en la Figura 2.2.

En el presente capítulo se describió la topología utilizada en el diseño del sistema, así como también el lugar específico de la instalación de los equipos. También se describió la construcción de los módulos del sistema. En el siguiente capítulo se describirá el desarrollo del software de monitoreo para el sistema de alarma contra intrusos.

## **CAPITULO 3**

### **DESARROLLO DEL SOFTWARE DE SOPORTE**

En el presente capítulo se describirá el desarrollo del software necesario para el funcionamiento y control del sistema de seguridad diseñado. Se hablará sobre el desarrollo del software para la central de control, el desarrollo del software para el microcontrolador y también el desarrollo de la interfaz de operación del sistema.

El software de monitoreo ha sido diseñado para alertar oportunamente a quien se encuentre encargado de la seguridad del laboratorio. Como se verá más adelante, este programa es muy útil en medios en los que exista un gran espacio físico que se desee amparar con este sistema de seguridad.

### **3.1 DISEÑO DEL SOFTWARE DEL CEREBRO DEL SISTEMA**

#### **3.1.1 MICROCONTROLADOR PIC 16F877A**

Para la programación de los microcontroladores PIC se seleccionó el lenguaje BASIC en lugar del ENSAMBLADOR debido a las ventajas que presenta este lenguaje, sobre todo en cuanto a su facilidad para el desarrollo de programas. Sus principales características son las siguientes:

- Programación estructurada.
- Economía en las expresiones.
- Abundancia en operadores y tipos de datos.
- Codificación en alto y bajo nivel simultáneamente.
- Reemplaza ventajosamente a la programación en ensamblador.
- Utilización natural de las funciones primitivas del sistema.
- No está orientado a ningún área en especial.
- Producción de código objeto altamente optimizado.
- Facilidad en su aprendizaje.

Estas características hacen al lenguaje BASIC, que es un lenguaje de alto nivel, óptimo para los PICs de la familia 16F.

El software utilizado para la programación del PIC 16F877A es el Win PIC800, el editor de texto es el Microcode Studio. Una vez creados los archivos con el código fuente para el proyecto, estos deben ser compilados y enlazados para crear el respectivo código de máquina y ser cargado al microcontrolador PIC utilizando el compilador PIC Basic Pro. El Microcode Studio se ha escogido ya que es un programa editor de texto diseñado para facilitar la programación de los microcontroladores PIC, además es un software gratuito disponible en internet.

El programa Microcode Studio es un compilador que se encarga de generar el archivo hexadecimal .HEX, necesario para poder grabar las líneas de programación en un microcontrolador PIC. Este no es un software gratuito pero se puede utilizar la versión demo que se puede descargar de internet.

La programación en BASIC del microcontrolador PIC se la ha realizado en base al diagrama de flujo mostrado en la Figura 3.1, cuyo algoritmo de programación explica la secuencia de tareas que se describen a continuación:

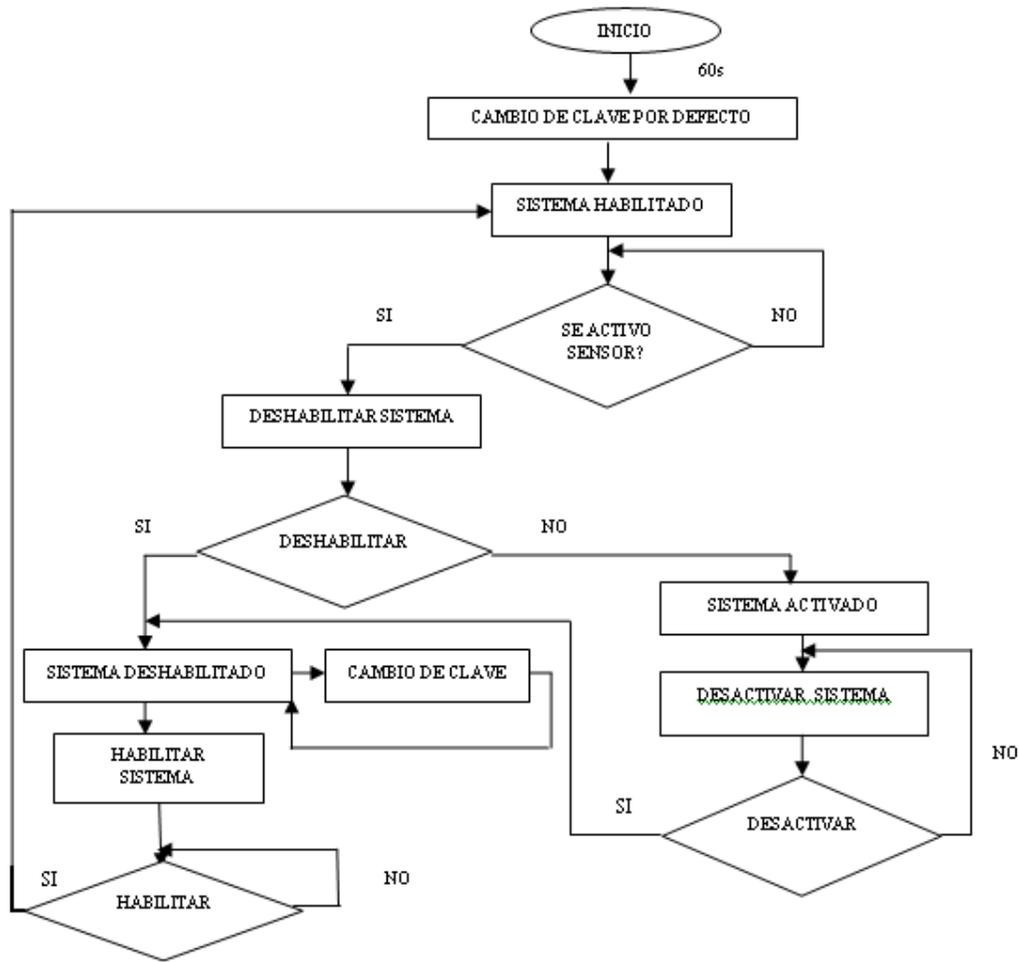


Figura 3.1 Diagrama del funcionamiento del Microcontrolador

#### Cambio de Clave por Defecto.

Introducir clave por defecto

Si es correcta

Introducir nueva clave

Esperar que usuario ingrese dígito 1, 2, 3 y 4

Si ingresa clave nueva

Almacenar clave ingresada

De otro modo

Conservar la clave por defecto

Caso contrario

Volver a pedir clave por defecto

**Fin de Tarea**

**Sistema Habilitado.**

Esperar datos de sensores  
 Verificar dato y validar sensor alarmado  
 Si se activa sensor  
     Pasar a opción deshabilitar sistema  
 Caso contrario  
     Continuar habilitado

**Fin de Tarea****Deshabilitar Sistema**

Esperar que en el lapso de 30s. el usuario introduzca código de desactivación  
 Si se introduce código de desactivación correcto  
     Sistema deshabilitado  
 Caso Contrario  
     Continuar sistema activado

**Fin de Tarea****Sistema deshabilitado**

Esperar a que usuario habilite el sistema o que cambie la clave

**Fin de Tarea****Habilitar sistema**

Esperar que usuario introduzca clave de activación  
 Si se introduce  
     Sistema Habilitado  
 Mientras no  
     Sistema deshabilitado

**Fin de Tarea****Cambio de Clave**

Introducir clave actual  
 Introducir nueva clave

**Fin de Tarea****Sistema Activado**

Encender Sirena  
 Alarmar sistema de Monitoreo

**Fin de Tarea**

**Desactivar Sistema**

Esperar que usuario ingrese código de desactivación

Si se ingresa el código

Deshabilitar sistema

Mientras no

Continuar sistema activado

**Fin de Tarea****3.1.2 PERIFERICOS****3.1.2.1 LCD**

Para construir la interfaz de usuario se ha utilizado un LCD y para su programación se tuvo en cuenta los comandos más utilizados para el manejo del mismo que se muestran en la Tabla 3.1.

COMANDO	OPERACIÓN
\$FE,1	Limpiar el visor LCD
\$FE,2	Volver al inicio
\$FE,\$0C	Apagar el cursor
\$FE,\$0E	Subrayar el cursor activo
\$FE,\$0F	Parpadear el cursor activo
\$FE,\$10	Mover el cursor una posición a la izquierda
\$FE,\$14	Mover el cursor una posición a la derecha
\$FE,\$80	Mover el cursor al comienzo de la primera línea
\$FE,\$C0	Mover el cursor al comienzo de la segunda línea
\$FE,\$94	Mover el cursor al comienzo de la tercera línea
\$FE,\$D4	Mover el cursor al comienzo de la cuarta línea

Tabla 3.1 Tabla de comandos más utilizados para manejar un LCD

## 3.2 DISEÑO DEL SOFTWARE DE LA CENTRAL DE CONTROL “SECURITY SOFT”

### 3.2.1 DESCRIPCIÓN

El fin de este software de aplicación es el uso del mismo en el computador que servirá de central de monitoreo y donde se encontrará el dispositivo ZigBee Coordinador comunicado con el PC mediante un Microcontrolador.

El programa tiene la función de dar aviso oportuno a quien se encuentra monitoreando el computador, utilizado como central de control, de la presencia de intrusos dentro de las instalaciones del laboratorio y ubicarlo en forma muy general en que lugar se encuentra. Para ello, la aplicación se compone de tres formas o ventanas. Una principal para Iniciar el programa, la segunda utilizada para autenticar al usuario, y la última para exhibir el entorno virtual del laboratorio protegido con este sistema de seguridad.

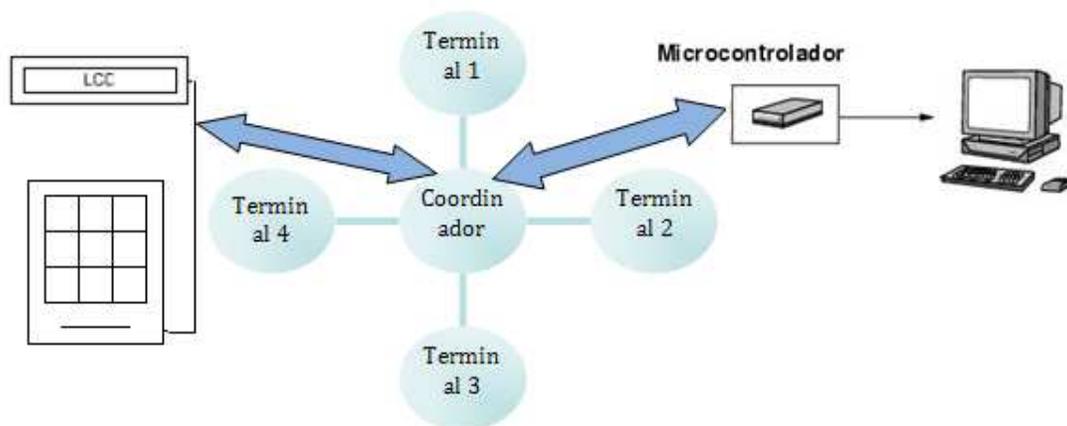


Figura 3.2 Esquema general del proyecto

### 3.2.2 LENGUAJE DE PROGRAMACIÓN

El software de monitoreo ha sido diseñado en el lenguaje de programación Visual BASIC 6.0. El lenguaje se ha escogido debido a que es una herramienta de

diseño de aplicaciones para Windows, en la que estas se desarrollan en gran parte a partir del diseño de una interface gráfica. En una aplicación de Visual Basic, el programa está formado por una parte de código puro, y otras partes asociadas a los objetos que forman la interfaz gráfica.

Es por tanto un término medio entre la programación tradicional, formada por una sucesión lineal de código estructurado, y la programación orientada a objetos. Combina ambas tendencias. Por ello se dice que esta es una PROGRAMACION VISUAL y con este se ha podido desarrollar el programa que se acopla a las necesidades específicas de monitoreo.

### 3.2.3 COMUNICACIÓN SERIAL

MSComm está presente en Visual Basic 6.0 y permite la comunicación de una aplicación VB con el puerto serie. Mediante este control se consigue crear aplicaciones que envíen y reciban datos a través de comunicación serial por el puerto serial.

Las propiedades más importantes de este control son las siguientes:

- ComPort: Activa y regresa el número del puerto serial (Comm1, Comm2)
- PortOpen: Activa y regresa el acceso al puerto.
- Input: Regresa los caracteres del buffer receptor.
- Output: Escribe una cadena sobre el buffer Transmisor.
- Settings: Activa y regresa la razón de Baudios, paridad, número de bits, bits de paro.

El MSComm de esta aplicación está configurado con los parámetros mostrados en la Tabla 3.2 para conseguir la comunicación serial deseada PIC – PC.

PROPIEDAD	VALOR
Bits por Segundo	9600
Bits de Datos	8
Paridad	Ninguno
Bits de Parada	1
Control de Flujo	Ninguno

Tabla 3.2 Propiedades del Componente Serial

### 3.2.3.1 Conexión del Microcontrolador PIC al Puerto Serie del PC

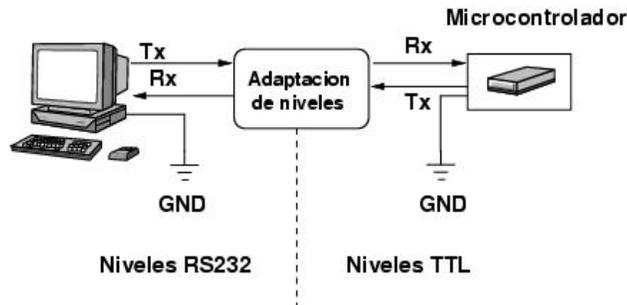


Figura 3.3 Conexión del microcontrolador al PC

Para conectar el PC a un microcontrolador por el puerto serie se utilizan las señales Tx, Rx y GND. El PC utiliza la norma RS232, por lo que los niveles de tensión de los pines están comprendidos entre +15 voltios "1" lógico y -15 voltios el "0" lógico. Los niveles lógicos TTL no son compatibles con los niveles lógicos RS232 del puerto serie del ordenador, razón por la cual se debe introducir en el circuito, una interfaz que traduzca los datos del circuito digital al puerto serie del computador y viceversa. Con el fin de que el microprocesador pueda llevar a cabo comunicaciones seriales hacia el mundo exterior se ha utilizado el transceptor MAX232 que convierte los niveles RS232 (cerca de +15 y -15 V) a voltajes TTL ( 0 a +5 V ) sin requerir nada más que una fuente de +5 V y adicionalmente cuatro capacitores externos.

### 3.2.3.2 El Cableado

El soporte físico de un computador es un conector tipo DB9 macho, de 9 pines, por el que se conectan los dispositivos al puerto serie. Se necesita por tanto un cable con conector DB9 hembra de 9 pines para acceder a él. Por ello se utilizó un cable DB9 hembra a DB9 macho cruzado para la conexión del coordinador hacia la computadora.

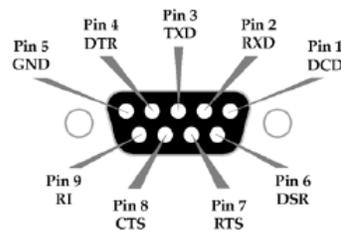


Figura 3.4 Distribución de pines en el conector DB9

La distribución de las señales en cada uno de sus pines es como se muestra en la tabla 3.3

Número de pin	Señal
1	DCD (Data Carrier Detect): Detector de transmisión
2	RX: Recibir datos
3	TX: Transmitir datos
4	DTR (Data Terminal Ready): Terminal de datos lista
5	GND: Señal de tierra
6	DSR (Data Sheet Ready): Ajuste de datos listo
7	RTS (Request To Send): Permiso para transmitir
8	CTS (Clear To Send): listo para enviar
9	RI (Ring Indicator): Indicador de llamada

Tabla 3.3 Disposición de los pines en el ordenador

### 3.2.4 EMPAQUETAMIENTO DEL SOFTWARE

Para crear un instalador del código fuente generado se ha utilizado el creador de software instalador Setup Factory debido a la simplicidad de su manejo, además de las características que ofrece en cuanto a empaquetamiento.

Las características de este software son las siguientes:

1. Instala cualquier archivo en cualquier lugar debido a que trabaja desde Windows 95 hasta Windows Vista.
2. Crea un único archivo ejecutable .exe listo para la distribución ya sea vía web, email, LAN, CD,DVD y diskets.
3. De fácil uso y rápido debido al Asistente de Proyectos que ayuda a crear el instalador sin tener mucha experiencia ni conocimiento.
4. Posee varias opciones de visualización del instalador de un proyecto, se puede configurar según las necesidades y crear un entorno amigable para el usuario.
5. Es capaz de crear instaladores para un proyecto de Visual Basic, lo analiza y automáticamente adiciona archivos y dependencias necesarias para hacerlo correr.
6. Acciones extendidas de librerías, puede ejecutar programas, llamar funciones DLL's, empezar y terminar servicios, enumerar procesos, entre otras cosas.

Principalmente la facilidad de uso del instalador en cualquier ambiente además del entorno visual, es la razón por la que se ha escogido este programa para generar el instalador de este proyecto.

#### **3.2.4.1 Instalación del Software**

En la Figura 3.6 se puede observar el proceso de instalación del Software de monitoreo generado por el empaquetador Setup Factory 7.0.

1. Pantalla de Bienvenida: Indica el software a ser instalado, y da ciertas recomendaciones para hacerlo correctamente.
2. Acuerdo de licencia: Muestra las restricciones a las que se tiene para instalar el software y da la opción de aceptar o no los términos de la licencia.
3. Ingreso de la información del usuario: Se debe ingresar la información del usuario.

4. Elección de la carpeta de instalación: Presenta la opción de cambiar la carpeta por defecto en la que se instalará el software.
5. Listo para instalar: muestra los parámetros que serán utilizados para la instalación. Esta pantalla es la previa a la instalación definitiva del software.
6. Instalación Completada

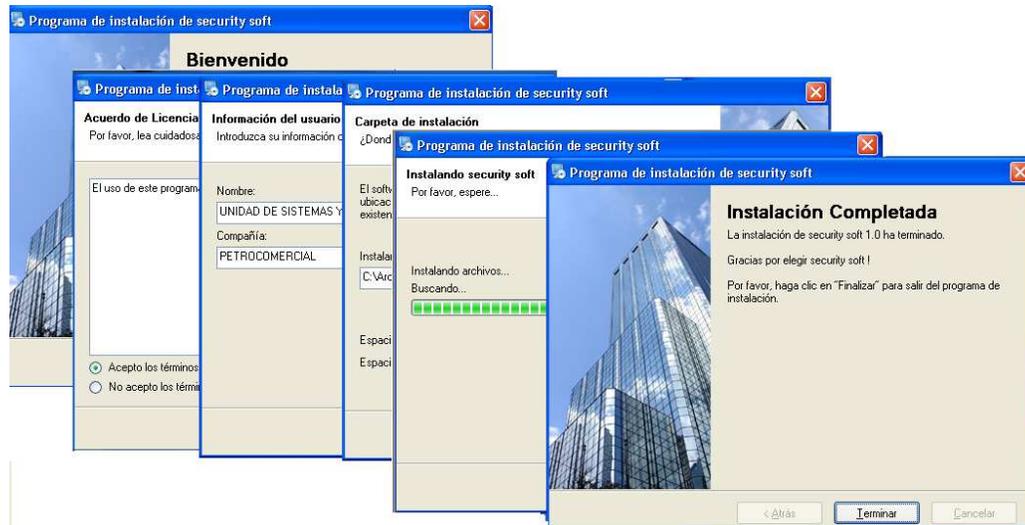


Figura 3.5 Proceso de Instalación del Software en la PC

### 3.2.5 FUNCIONAMIENTO Y CODIGO DEL SOFTWARE DE MONITOREO

A continuación se muestra el funcionamiento básico del programa de monitoreo denominado “Security Soft” y las líneas de código que han sido programadas para que realice las funciones requeridas. En las figuras se observa como es posible ingresar a él y lo sencillo que es ponerlo en funcionamiento. Se describe el diseño del Software desarrollado, el mismo que se lo ha realizado en 3 partes las cuales se detallan a continuación:

1. **Carátula o Pantalla Principal:** que se despliega al darle doble click en el ícono del programa, como se visualiza en la Figura 3.6.



Figura 3.6 Pantalla Principal del Software de Monitoreo

Para obtener esta pantalla se utilizó un formulario Splash que se lo puede encontrar dentro de las opciones de formularios que nos ofrece el Visual Basic 6.0 llamado pantalla principal y se despliega un formulario que se visualiza en la Figura 3.7.



Figura 3.7 Formulario Splash

De esta pantalla se modificó los objetos y principalmente la propiedad **Caption** (cambiar el texto por el que se desea visualizar en cada cuadro dentro del entorno de la pantalla) de cada cuadro **Label**.

Para diseñar la pantalla de presentación del programa, que se observa en la Figura 3.8, se ha utilizado diferentes objetos dentro del formulario splash **caratula** y se ha configurado con las siguientes propiedades:

- StartupPosition: 2 –Center screen *'para centrar la pantalla de presentación*
- BorderStyle: None
- ShowInTaskbar: False

Para cargar la imagen se usó un cuadro de **Imagen** con las siguientes propiedades:

- Picture: se coloca la ruta donde se encuentra la imagen
- Stretch: True

Se adiciona un timer con intervalos de 2000 seg. para que ejecute la carátula, desaparezca y pase a la pantalla de ingreso, para ello se usó la siguiente subrutina:

```

Private Sub Timer1_Timer()
    OLE2.DoVerb 'se acciona el sonido de ingreso al sistema
    Unload Me 'dejar de mostrar la carátula
    ingreso.Show 'pasar a mostrar la pantalla de ingreso
End Sub

```

2. **Pantalla de autenticación o login:** Para el ingreso al programa se despliega la pantalla de autenticación mostrada en la Figura 3.9, luego de cargarse la pantalla principal. Este proceso sirve para autenticar al usuario al ingresar al programa de monitoreo. El nombre de usuario que deberá ser ingresado por defecto es: “admin” y la contraseña es: “public”. Para esta pantalla se ha utilizado el formulario login que está disponible en visual basic.

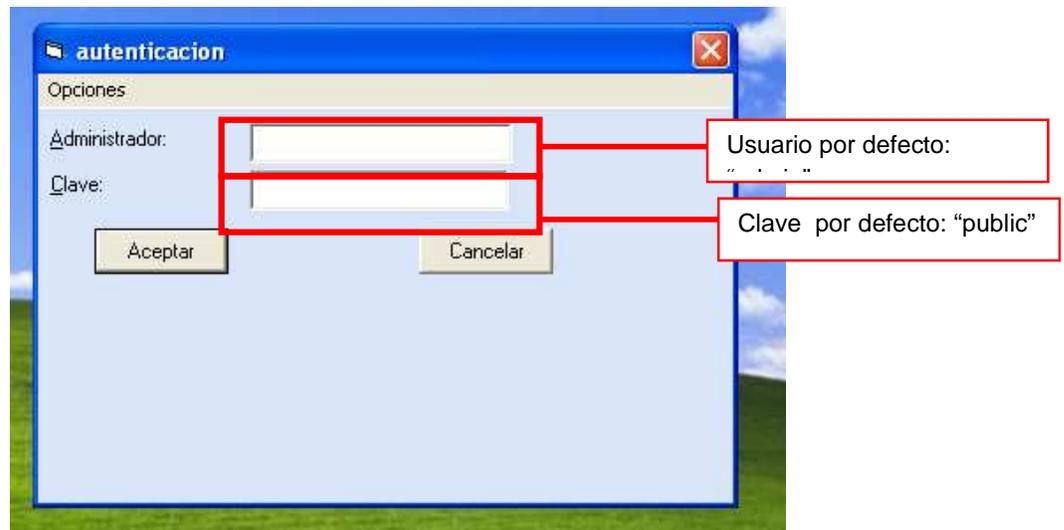


Figura 3.8 Cuadro de Autenticación para inicio de sesión

De no ser ingresado correctamente el nombre de usuario o la contraseña se desplegará un mensaje de error en el inicio de sesión como lo muestra la figura 3.9.

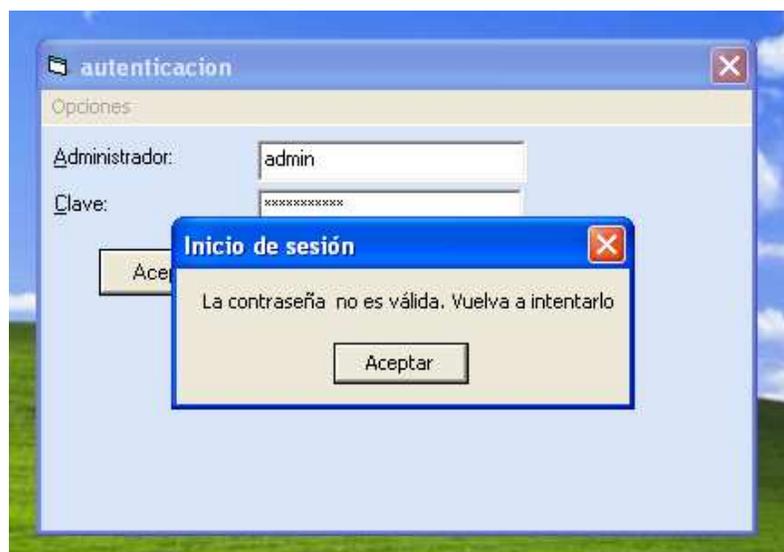


Figura 3.9 Mensaje de error en la autenticación

Si se desea cambiar la contraseña de inicio, se da click en Opciones y nueva clave como se muestra en la Figura 3.10.

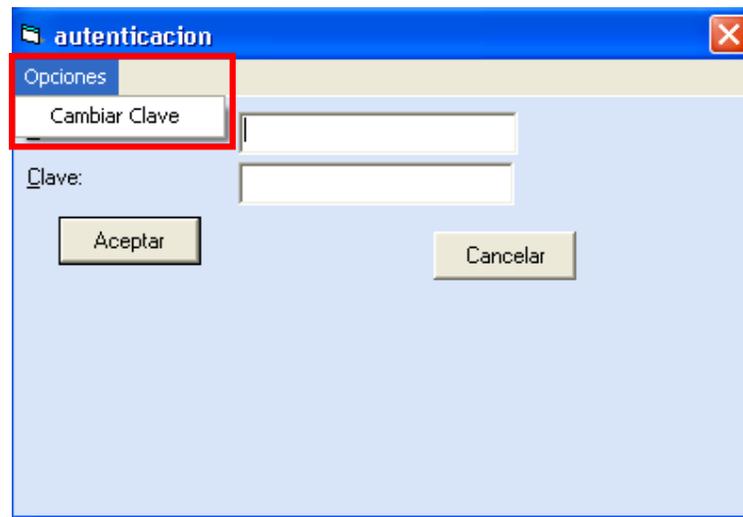


Figura 3.10 Cambio de clave

Luego se desplegará un mensaje de ingreso de la clave anterior, la clave nueva y aplicar.

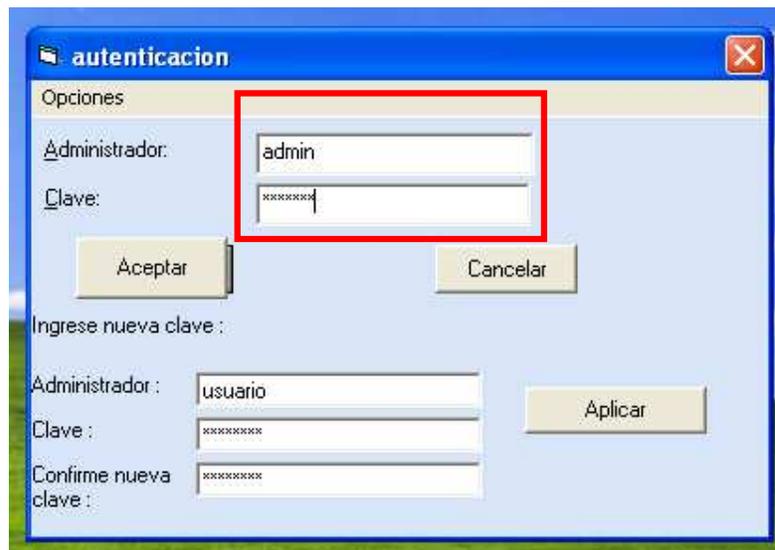


Figura 3.11 Ingreso de la nueva clave

La pantalla de autenticación tiene la estructura mostrada en el diagrama de flujo de la Figura 3.12.

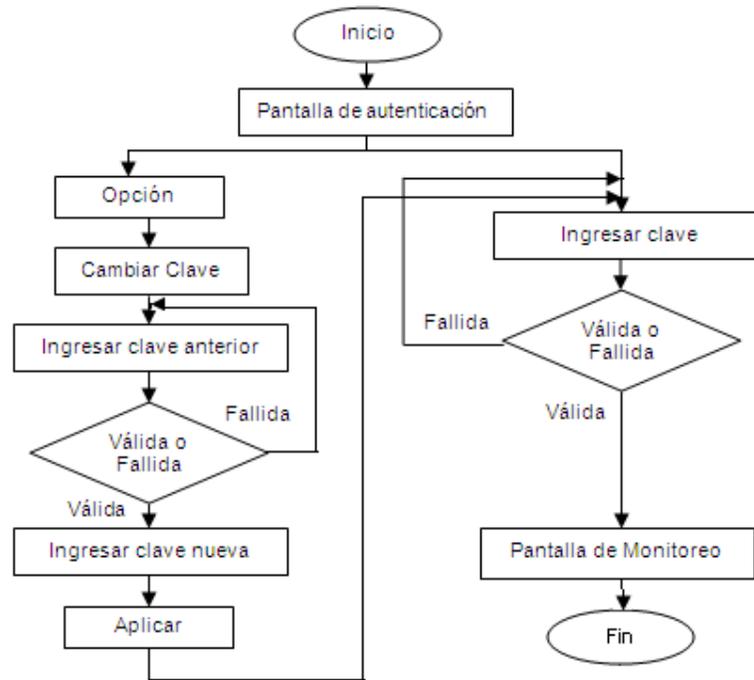


Figura 3.12 Diagrama de la Pantalla de Autenticación

**Opcion**

Mostrar opción de cambio de clave

**Fin de Tarea**

**Cambiar Clave**

Si elige cambiar clave

Se presenta el mensaje: Ingresar clave anterior

De otro modo

Pasa a: Ingresar Clave

**Fin de Tarea**

**Ingresar Clave Anterior**

Si clave Valida

Se presenta mensaje: Ingresar nueva clave

De otro modo

Cambiar clave

**Fin de Tarea**

**Aplicar**

Una vez ingresada clave nueva

Guarda la clave y pasa a:

Ingresar clave

**Fin de Tarea****Ingresar clave**

Si clave Valida

Pasa a pantalla de monitoreo principal

De otro modo

Retorna a: ingresar clave

**Fin de Tarea**

3. **Pantalla del entorno del programa de monitoreo:** la pantalla de monitoreo muestra virtualmente el espacio físico que se está protegiendo, en este caso el laboratorio de informática. Una vez autenticado correctamente el usuario, se ingresa al entorno visual que se muestra en la Figura 3.13.

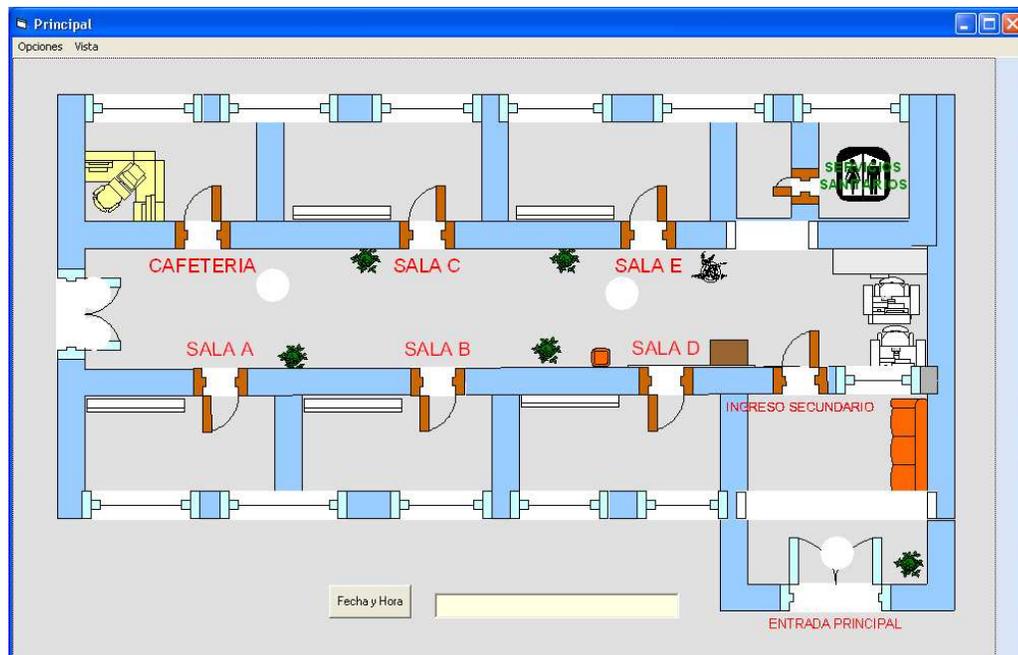


Figura 3.13 Entorno del software “Security Soft”

Se puede observar en el entorno unos círculos en blanco que representan los dispositivos de seguridad que se han ubicado dentro del laboratorio. Una vez que ha sido activado el sistema espera a que alguno de los dispositivos dé aviso al microcontrolador, el mismo que enviará hacia el puerto serial de la PC una señal que provocará que se activen los avisos visuales y los sonidos que alertarán a la persona encargada de que se está produciendo una violación de seguridad dentro del laboratorio. Se puede observar que si se activara el sensor de movimiento, en la pantalla se visualizará lo que se muestra en la Figura 3.14, además se escuchará un sonido de alerta.



Figura 3.14 Sistema de Monitoreo Alarmado

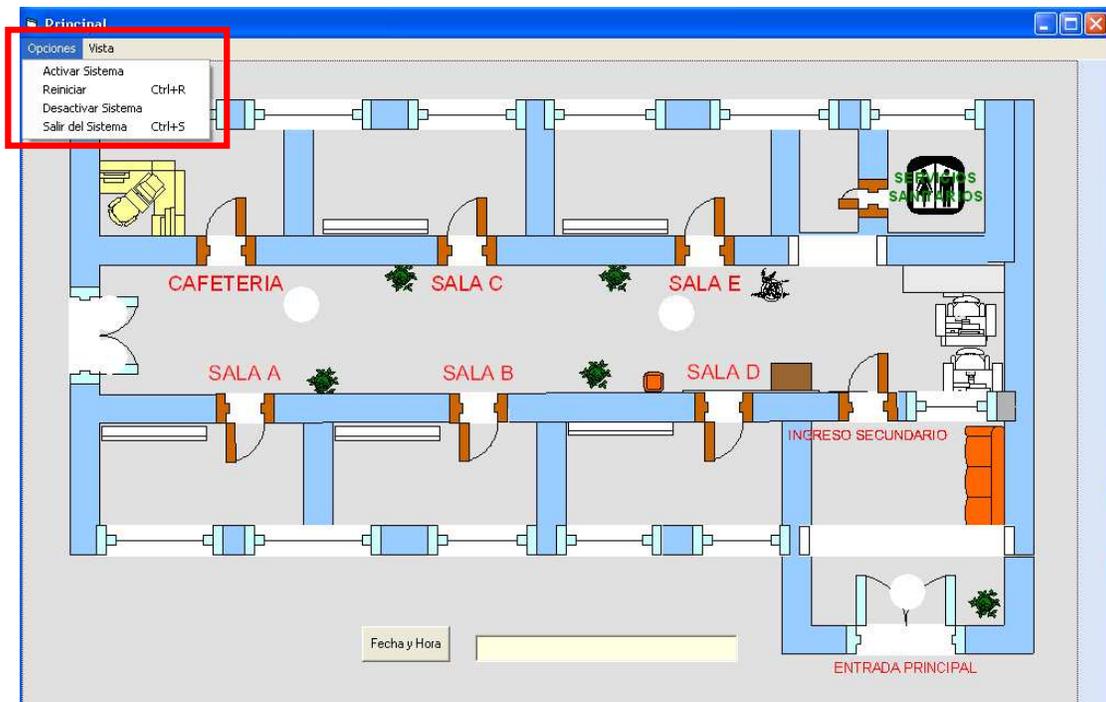


Figura 3.15 Menú Opciones

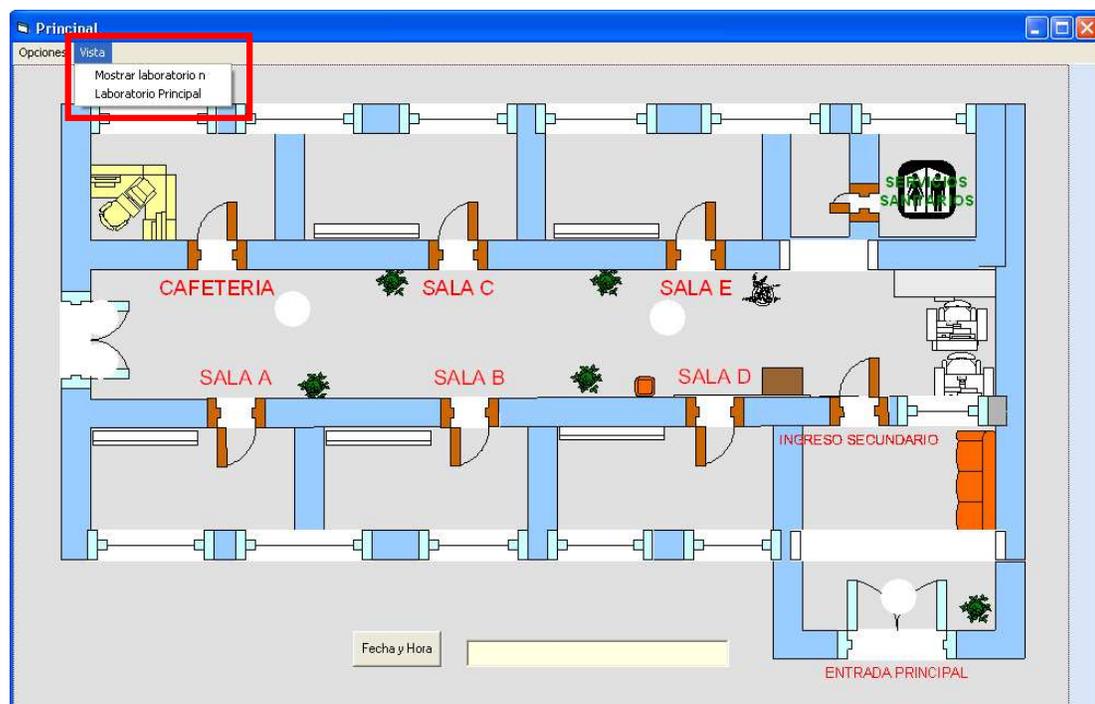


Figura 3.16 Menú Vista

Dentro de este entorno se tiene un menú con Opciones y un menú Vista. En el menú Opciones, como se observa en la Figura 3.15, se despliega un submenú con cuatro posibilidades:

- Activar Sistema: dentro del entorno de monitoreo se debe escoger esta opción para poder abrir el puerto comm que se escogerá para ponerlo a trabajar como se observa en la Figura 3.17

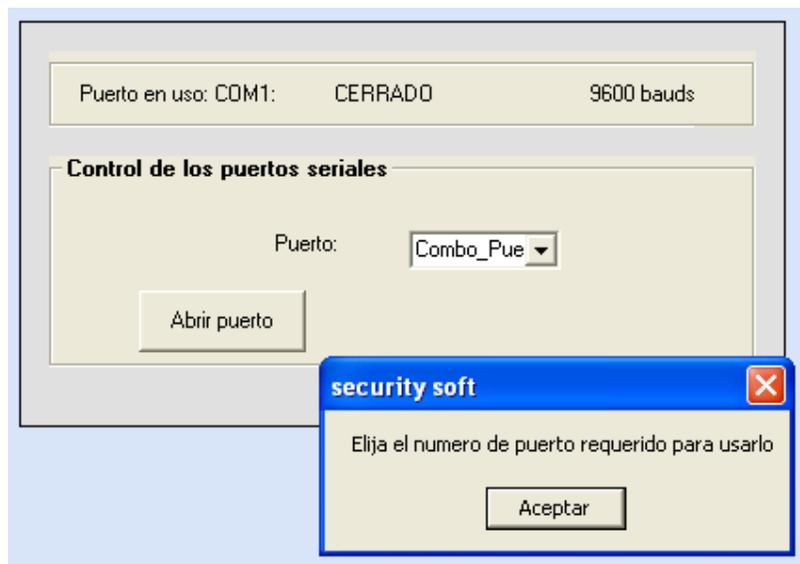


Figura3.17 Opción Activar Sistema

- Reiniciar: se refiere al monitoreo, sirve para desactivar los anuncios y alertas que se encuentra ejecutando el programa para dar aviso oportuno de la presencia de algún intruso, luego de lo cual debe regresar al estado de espera.
- Desactivar Sistema: esta opción únicamente sirve para desactivar el sistema de monitoreo, esto hará que no reciba señales provenientes del cerebro del sistema de alarma. Para lo cual deberá ingresar la clave de desactivación en la pantalla login presentada en la Figura 3.18, la clave para la desactivación es: **nombre de usuario:** admin; **clave:** password.



Figura 3.18 Opción desactivar Sistema de Monitoreo

Al ser autenticado correctamente pasa a la pantalla que da opción de cerrar el puerto comm, mostrado en la Figura 3.19.



Figura 3.19 Cerrar puerto Comm

- Salir del Sistema: para salir del programa de monitoreo.

El menú Vista como se observa en la Figura 3.16, tiene submenús de los diferentes laboratorios que se pueden observar al ser adheridos al sistema de seguridad y monitoreo. Este menú ha sido pensado para una supuesta expansión del sistema a varios laboratorios, de ese modo

se podría monitorear cada uno de los entornos por separado y observarlos dependiendo de las necesidades o de las prioridades que se tenga respecto a ellos.

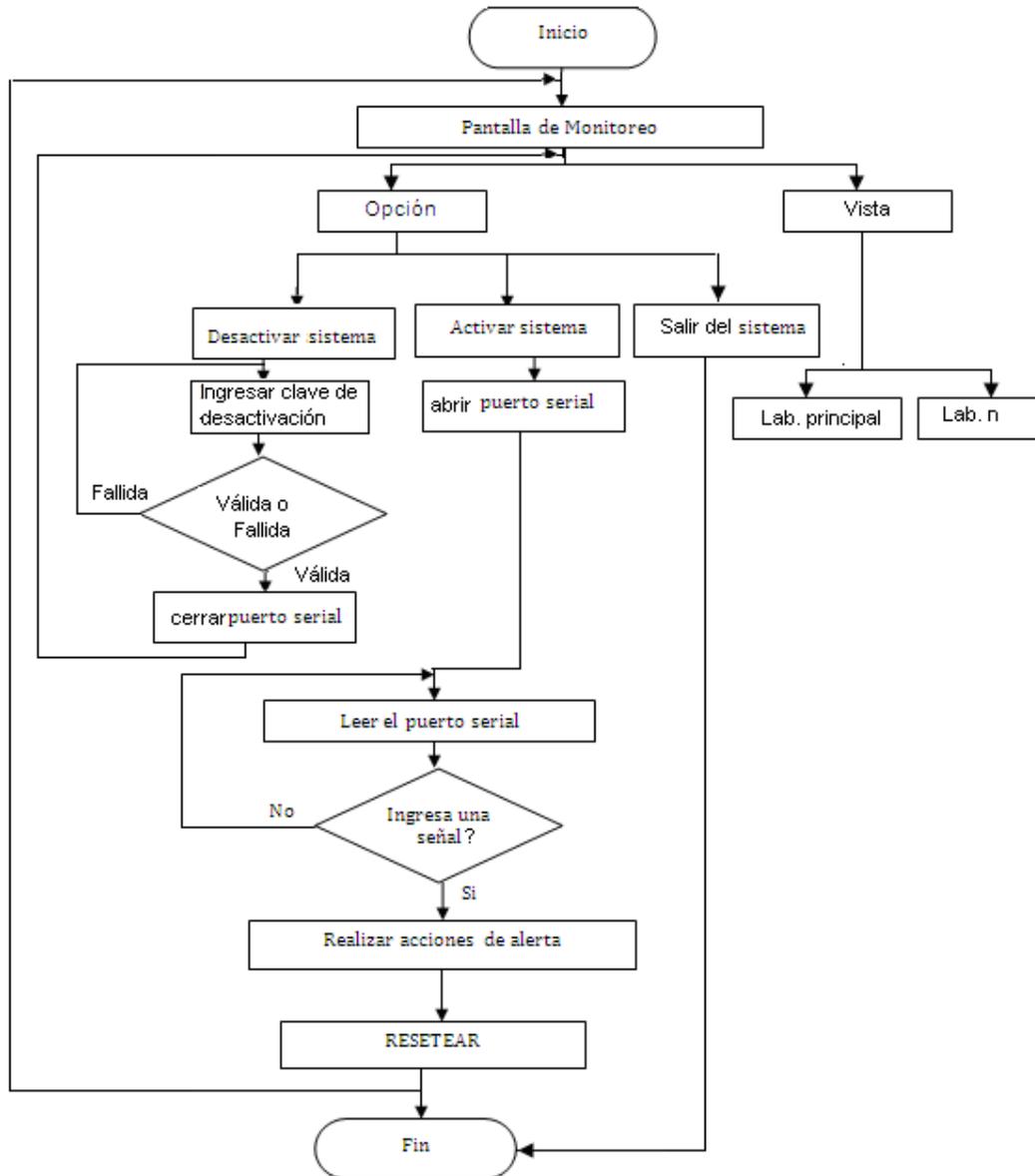


Figura 3.20 Diagrama de la pantalla de monitoreo

#### Opción

Mostrar a usuario varias posibilidades de elección

#### Fin de Tarea

#### Activar Sistema

Presentar cuadro de manejo del puerto Com  
Posibilitar elegir puerto, setear velocidad y abrir el puerto Com  
Esperar a recibir datos por el puerto serial

**Fin de Tarea**

**Desactivar Sistema**

Pasar a pantalla de desactivación

**Fin de Tarea**

**Ingresar clave de desactivación**

Si clave válida

Presentar la pantalla de manejo del puerto Com

Posibilitar elección de cerrar puerto Com

Caso contrario

Volver a pantalla de desactivación

**Fin de Tarea**

**Salir del Sistema**

Finalizar y cerrar todas las pantallas ejecutadas en el programa

**Fin de Tarea**

**Leer el puerto serial**

Esperar a recibir un dato del cerebro

Si recibe dato

Verificar dato y ejecutar subrutina de alerta del sensor alarmado

Caso contrario

Leer puerto serial

**Fin de Tarea**

**Realizar acciones de alerta**

Desplegar mensajes de alerta de intrusos

Encender luz en dispositivo alarmado

Activar el mensaje auditivo de alarma

**Fin de Tarea**

**Resetear**

Borra los mensajes de alerta

Blanquea los dispositivos alarmados dentro del entorno visual

Regresa al estado de espera

**Fin de Tarea**

### 3.2.6 SEGURIDADES

Como se puede observar en la Figura 3.10 y la Figura 3.20, la seguridad que se ha implementado para este software es la restricción del ingreso y de la desactivación del sistema de monitoreo mediante la autenticación de usuario y contraseña.

Para este caso la seguridad del software no es crítica debido a que a través de la central de monitoreo no se tiene acceso al microcontrolador ni a ninguna de las funciones de la alarma de seguridad implementada.

El microcontrolador y las funciones del cerebro están únicamente diseñadas para enviar datos por el puerto serial y no para recibir datos desde el sistema de monitoreo que se encuentra en un computador que puede ser manipulado por alguien diferente del administrador. De ese modo se ha tratado de no hacer que la seguridad del sistema dependa de un factor externo que puede ser fácilmente manipulado por software.

En el presente capítulo se describió el diseño del software del PIC que controla el cerebro central, además del software desarrollado para la central de monitoreo del sistema de seguridad.

En el siguiente capítulo se presentarán las pruebas realizadas con el sistema de seguridad en diferentes ambientes y situaciones para mediante resultados validar el funcionamiento del sistema de seguridad. Se mostrará el detalle de los costos en los que se incurrirá para la implementación de este sistema.

## CAPITULO 4

### PRUEBAS Y RESULTADOS

En este capítulo se describirá las pruebas realizadas para comprobar el funcionamiento del sistema implementado y se analizarán estos resultados. También se detallarán los costos en los cuales incurrió la implementación del proyecto.

#### 4.1 PRUEBAS DE COMUNICACIÓN DE DATOS

Se realizaron pruebas de comunicación de datos con los módulos Xbee utilizando el software X-CTU y las placas de desarrollo USB (Figura 4.1) y RS-232 (Figura 4.2)



Figura 4.1 Placa de desarrollo USB



Figura 4.2 Placa de desarrollo RS-232

#### 4.1.1 PRUEBA BÁSICA DE COMUNICACIÓN PC-XBEE

Se realizó la prueba básica de comunicación entre una PC y el dispositivo Xbee. Para esta comunicación se configuró el módulo de PC del software X-CTU a 9600, 8, N, 1 (Figura 4.3) y se realizó el proceso de Test/Query (Figura 4.4) con los 6 dispositivos. El firmware con el cual se trabajó en los dispositivos Xbee es el 10A5.

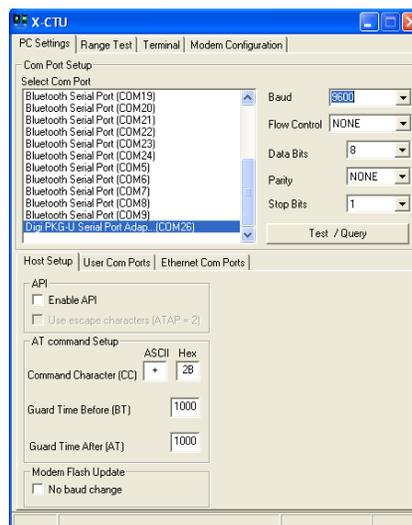


Figura 4.3 Configuración módulo de PC del software X-CTU



Figura 4.4 Proceso Test/Query

#### **Resultado:**

La prueba de comunicación básica entre una PC y los dispositivos Xbee fue exitosa y demuestra que los dispositivos Xbee funcionan con normalidad y están listos para ser configurados.

## 4.1.2 PRUEBA DE COMUNICACIÓN XBEE-XBEE

Se realizó la prueba de comunicación entre el dispositivo Xbee que trabaja como coordinador y el dispositivo Xbee que trabajan como periférico. Para esta prueba se configuró los dispositivos Xbee de acuerdo a la descripción mostrada en el Capítulo 2.

### 4.1.2.1 Prueba con línea de vista (Outdoor)

Se realizó la prueba con línea de vista (Outdoor) (Figura 4.5) separando los dispositivos Xbee para verificar a qué distancia se pierde la comunicación.

Se tomó medidas de recepción de paquetes y RSSI<sup>4.1</sup> a 30 m (Figura 4.6), a 60 m (Figura 4.7) y a 200 m de distancia (Figura 4.8).

Para la prueba se utilizó dos dispositivos Xbee, dos laptops y dos placas de desarrollo: USB y RS-232, respectivamente conectados. En el software X-CTU se utilizó el modulo Range-test con su configuración por default. Esta configuración consiste en el envío de 32 bytes de datos de un dispositivo a otro el cual devuelve la trama de datos hacia el origen.

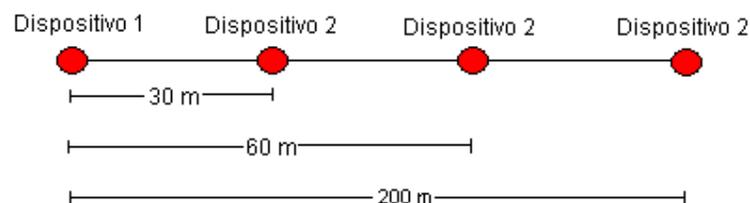


Figura 4.5 Diagrama para prueba con línea de vista

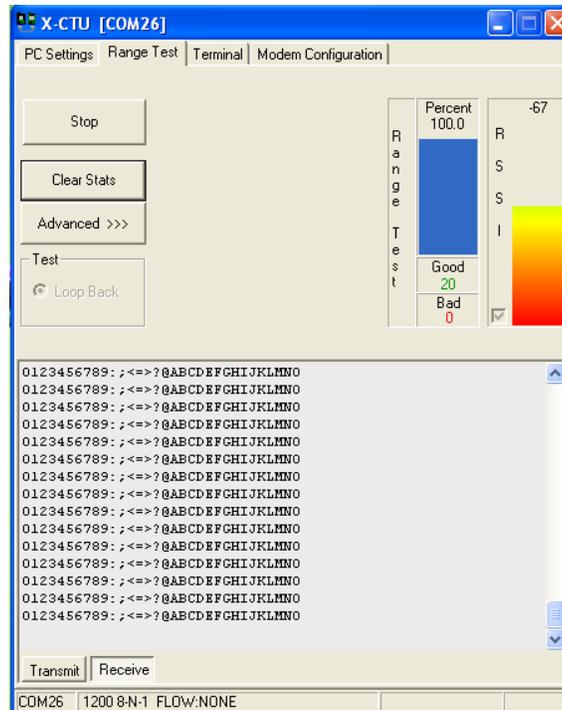


Figura 4.6 Medida de recepción de paquetes y RSSI a 30 m

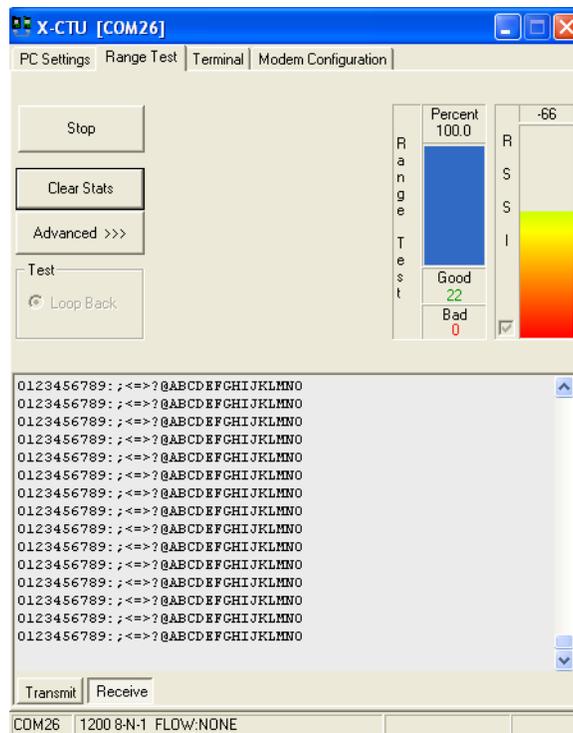


Figura 4.7 Medida de recepción de paquetes y RSSI a 60 m

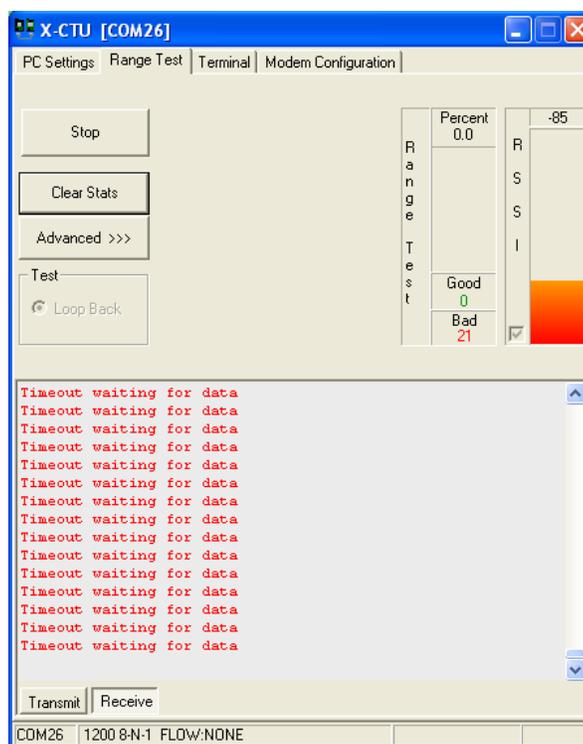


Figura 4.8 Medida de recepción de paquetes y RSSI a 200 m

### **Resultado:**

La prueba con línea de vista demuestra que a la distancia de 30 m se mantiene un 100% de recepción de paquetes con un nivel de recepción de  $-67\text{dBm}$  y a la distancia de 60 m se mantiene un 100% de recepción de paquetes con un nivel de recepción de  $-66\text{dBm}$ .

Hasta los 100 m de distancia la recepción de paquetes es normal y con un buen nivel de RSSI mayor a  $-75\text{dBm}$ . Pasado esta distancia, la comunicación se mantiene sin pérdida de paquetes únicamente si la línea de vista está completamente libre. En el caso de colocarse un obstáculo obstruyendo la línea de vista por más pequeño que sea, la recepción se presenta con pérdida de varios paquetes.

A una distancia de 180 m la comunicación se mantiene sin pérdida de paquetes únicamente si la línea de vista está completamente libre. En el caso de colocarse

un obstáculo obstruyendo la línea de vista por más pequeño que sea, la recepción se presenta con una pérdida total de paquetes.

A la distancia de 200m se pierde la comunicación completamente entre los dispositivos Xbee.

#### 4.1.2.2 Prueba sin línea de vista (Indoor)

Se realizó la prueba sin línea de vista (Indoor) en un ambiente casero común que dispone de paredes de 10cm construidas con bloque y loza de concreto de 20 cm.

Para la prueba se utilizó dos dispositivos Xbee, dos laptops y dos placas de desarrollo: USB y RS-232 respectivamente conectados. En el software X-CTU se utilizó el módulo Range-test con su configuración por default. Esta configuración consiste en el envío de 32 bytes de datos de un dispositivo a otro el cual devuelve la trama de datos hacia el origen.

#### ***Prueba 1:***

La Figura 4.9 muestra el lugar y distancia de instalación de los equipos, la Figura 4.10 muestra la prueba de rango y el RSSI (-dBm) medidas en el dispositivo 2.

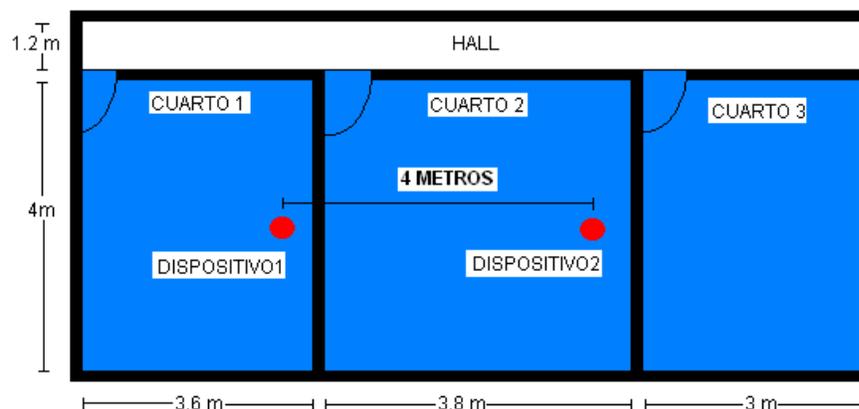


Figura 4.9 Lugar de instalación de los equipos para Prueba 1

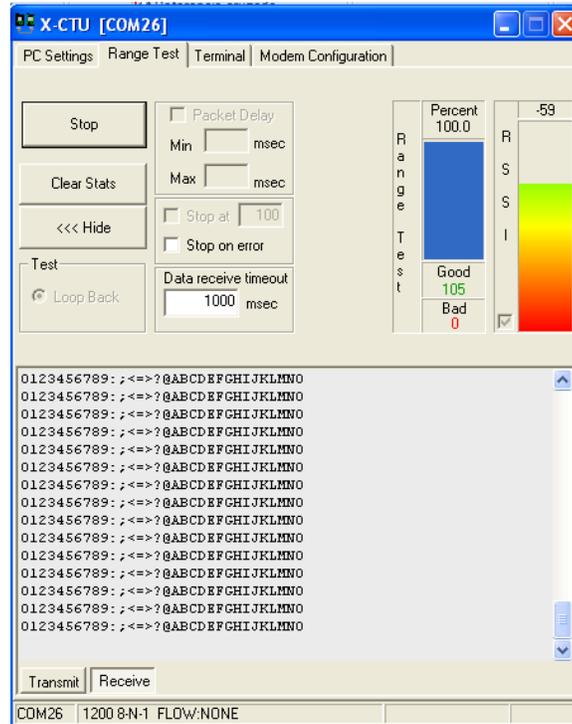


Figura 4.10 Medida de recepción de paquetes y RSSI para Prueba 1

### **Resultado:**

La Prueba 1 de comunicación entre los dos dispositivos Xbee fue exitosa y demuestra que en las condiciones descritas y la distancia especificada se mantiene un 100% de recepción de paquetes sin pérdida de los mismos en una transmisión de 105 tramas con un nivel de recepción de -59 dBm.

### **Prueba 2:**

La Figura 4.11 muestra el lugar y distancia de instalación de los equipos, la Figura 4.12 muestra la prueba de rango y el RSSI (-dBm) medidas en el dispositivo 2.

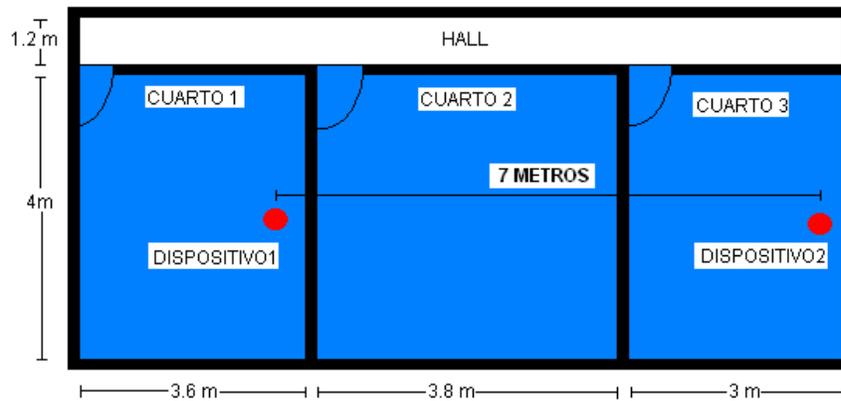


Figura 4.11 Lugar de instalación de los equipos para Prueba 2

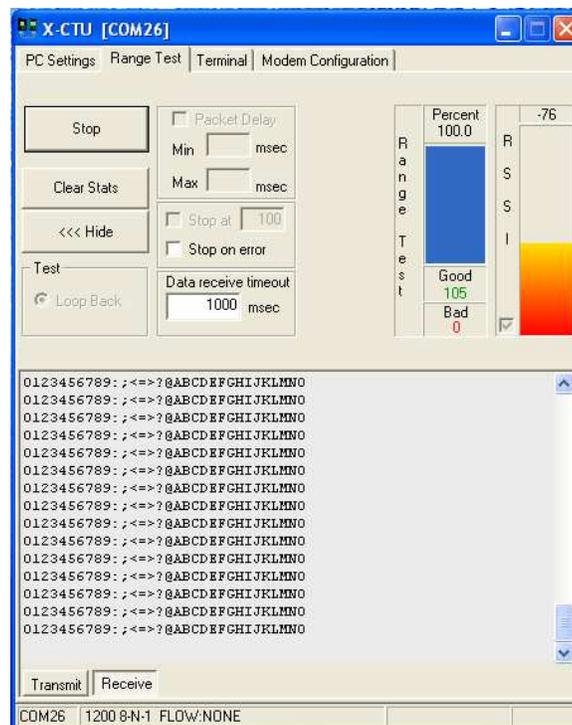


Figura 4.12 Medida de recepción de paquetes y RSSI para Prueba 2

### **Resultado:**

La Prueba 2 de comunicación entre los dos dispositivos Xbee fue exitosa y demuestra que en las condiciones descritas y la distancia especificada se mantiene un 100% de recepción de paquetes sin pérdida de los mismos en una transmisión de 105 tramas con un nivel de recepción de -76 dBm.

### Prueba 3:

La Figura 4.13 muestra el lugar y distancia de instalación de los equipos, la Figura 4.14 muestra la prueba de rango y el RSSI (-dBm) medidas en el dispositivo 2.

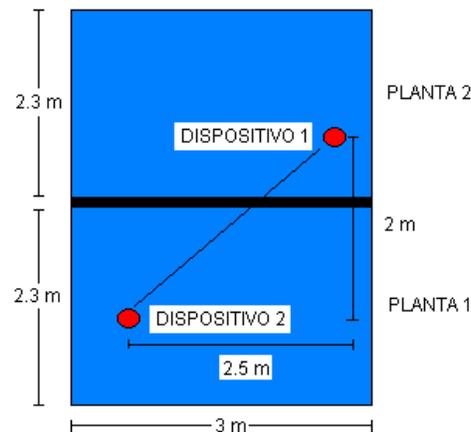


Figura 4.13 Lugar de instalación de los equipos para Prueba 3

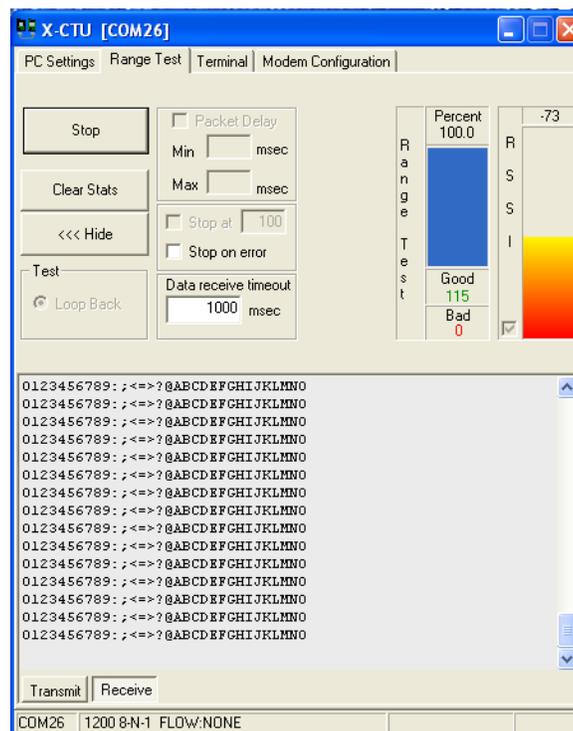


Figura 4.14 Medida de recepción de paquetes y RSSI para Prueba 3

**Resultado:**

La Prueba 3 de comunicación entre los dos dispositivos Xbee fue exitosa y demuestra que en las condiciones descritas y la distancia especificada se mantiene un 100% de recepción de paquetes sin pérdida de los mismos en una transmisión de 115 tramas con un nivel de recepción de -73 dBm.

**Prueba 4:**

La Figura 4.15 muestra el lugar y distancia de instalación de los equipos, la Figura 4.16 muestra la prueba de rango y el RSSI (-dBm) medidas en el dispositivo 2.

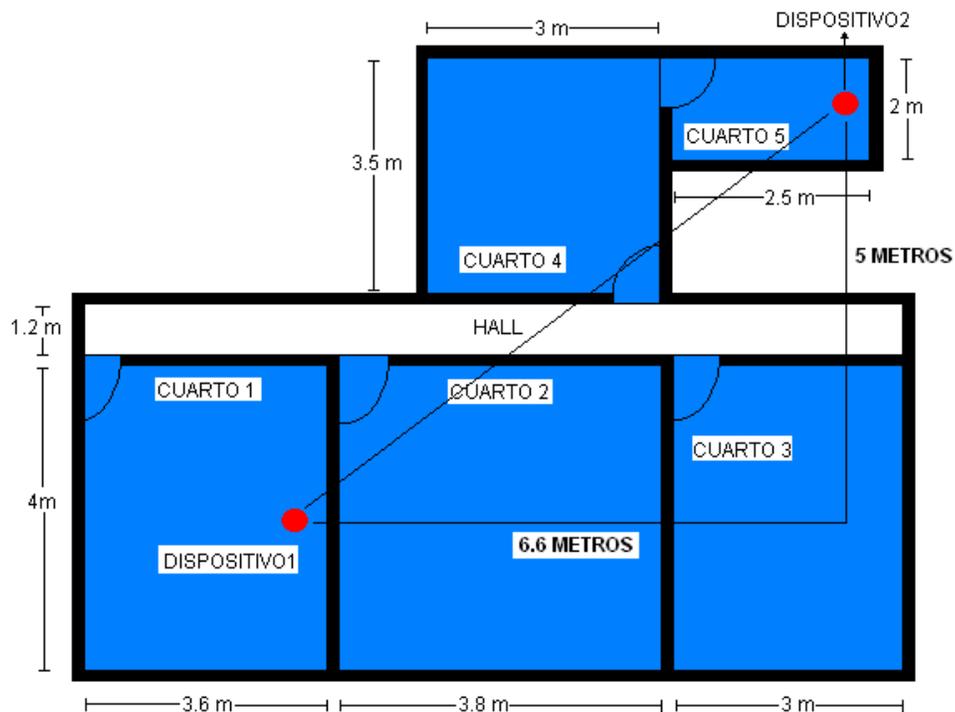


Figura 4.15 Lugar de instalación de los equipos para Prueba 4

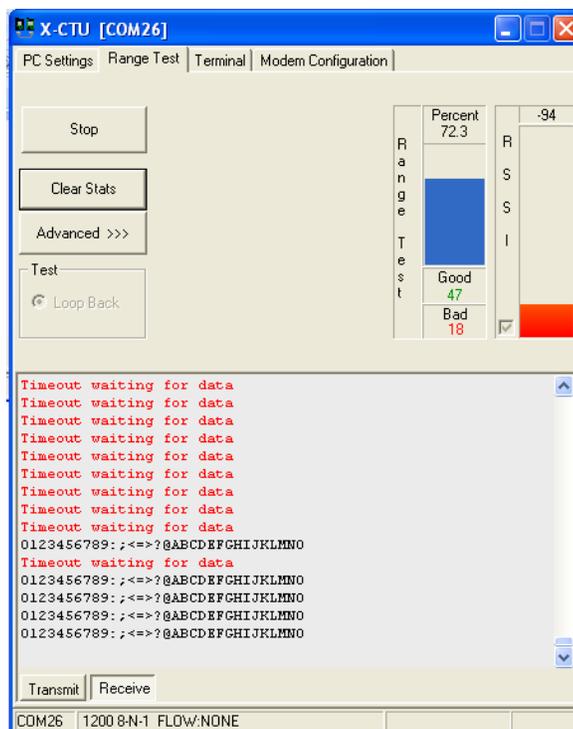


Figura 4.16 Medida de recepción de paquetes y RSSI para Prueba 4

### **Resultado:**

La Prueba 4 de comunicación entre los dos dispositivos Xbee no fue exitosa y demuestra que en las condiciones descritas y la distancia especificada se mantiene un aproximado del 70% de recepción de paquetes con una pérdida significativa de los mismos, con un nivel de recepción de -94 dBm.

### **Prueba 5:**

La Figura 4.17 muestra el lugar y distancia de instalación de los equipos, en donde se ha introducido una fuente intencional de interferencia microondas de 2.4 GHz. La Figura 4.18 muestra la prueba de rango y el RSSI (-dBm) medidas en el dispositivo 2

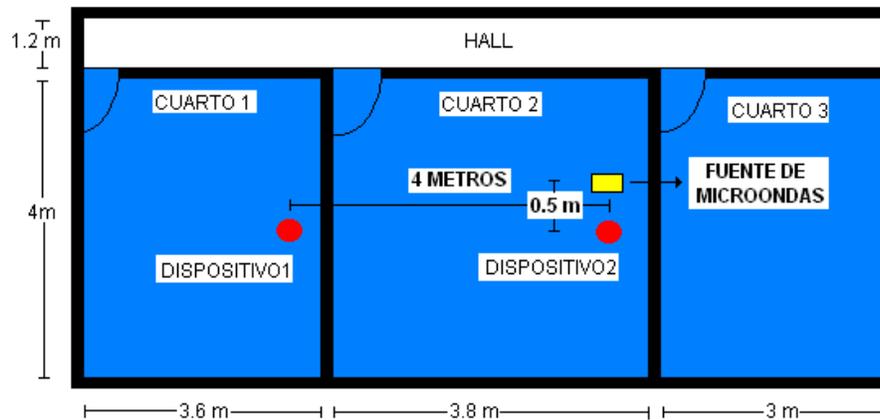


Figura 4.17 Lugar de instalación de los equipos para Prueba 5



Figura 4.18 Medida de recepción de paquetes y RSSI para Prueba 5

### **Resultado:**

La Prueba 5 de comunicación entre los dos dispositivos Xbee fue exitosa y demuestra que en las condiciones descritas y la distancia especificada, considerando un ambiente en el cual se encuentra una interferencia microondas de 2.4 GHz se mantiene un 100% de recepción de paquetes con un nivel de recepción de -55 dBm.

**Resultado Final:**

De acuerdo a las pruebas realizadas con línea de vista el alcance práctico máximo que proporcionan los dispositivos Xbee para mantener un 0% de probabilidad de pérdida de paquetes es de 120 m.

De acuerdo a las pruebas realizadas sin línea de vista el alcance máximo que proporcionan los dispositivos Xbee depende del nivel RSSI. Al separar los dispositivos Xbee entre si el nivel RSSI disminuye hasta llegar a un mínimo de -88 dBm con el cual se mantiene un 100% de recepción de paquetes. Bajo este nivel los paquetes se empiezan a perder y la comunicación no es efectiva.

Al introducir una fuente microondas cerca de unos de los dispositivos Xbee se observa que esta no ocasiona interferencia que provoque la mala recepción o envío de paquetes de datos.

En el Capitulo 2 se describió el lugar de instalación de los dispositivos. De acuerdo a esta descripción la comunicación entre los periféricos del sistema y el cerebro se realiza con línea de vista. Considerando la distancia que existe entre los dispositivos la comunicación se realiza con un 100% de recepción de paquetes en el cerebro del sistema.

**4.2 PRUEBAS DE PROCESAMIENTO DE DATOS**

Se realizó pruebas de procesamiento de datos con el cerebro del sistema y sus periféricos. Para que estas pruebas fueran realizadas fue necesario que el nivel de comunicación de datos entre el cerebro y los periféricos estuviera trabajando correctamente y que de igual forma los periféricos estuvieran enviando las señales correctas.

#### 4.2.1 PRUEBA DE FUNCIONAMIENTO DE PERIFERICOS

Se realizó la prueba de funcionamiento de los periféricos con el uso de un sensor y un dispositivo Xbee en un extremo y una PC conectada a la placa de desarrollo USB en el otro extremo.

Los dispositivos Xbee tanto en el periférico como en la placa de desarrollo han sido configurados de acuerdo a la descripción del Capítulo 2.

En la PC y con el uso del software X-CTU y su módulo de Terminal se observó la cadena de caracteres que el periférico envió (Figura 4.19).

```

X-CTU [COM26]
PC Settings | Range Test | Terminal | Modem Configuration
Line Status: CTS | CD | DSR
Assert: DTR | RTS | Break
Close Com Port | Assemble Packet | Clear Screen | Hide Hex

~. . . . . 7E 00 10 82 00 13 A2 00 40 53 A7 C6
@S..8.. 38 00 01 20 00 00 00 6F 7E 00 10 82
..o~. . . . . 00 13 A2 00 40 53 A7 C6 36 00 01 20
@S..6.. 00 00 00 71 7E 00 10 82 00 13 A2 00
..q~. . . . . 40 53 A7 C6 39 00 01 20 00 00 00 6E
@S..9.. 7E 00 10 82 00 13 A2 00 40 53 A7 C6
..n~. . . . . 36 00 01 20 00 00 00 71 7E 00 10 82
@S..6.. 00 13 A2 00 40 53 A7 C6 36 00 01 20
..q~. . . . . 00 00 00 71 7E 00 10 82 00 13 A2 00
@S..6.. 40 53 A7 C6 32 00 01 20 00 00 00 75
..q~. . . . . 7E 00 10 82 00 13 A2 00 40 53 A7 C6
@S..2.. 32 00 01 20 00 00 00 75 7E 00 10 82
..u~. . . . . 00 13 A2 00 40 53 A7 C6 36 00 01 20
@S..2.. 00 00 00 71 7E 00 10 82 00 13 A2 00
..u~. . . . . 40 53 A7 C6 3F 00 01 20 00 00 00 68
@S..6.. 7E 00 10 82 00 13 A2 00 40 53 A7 C6
..q~. . . . . 3F 00 01 20 00 00 00 68 7E 00 10 82
@S..?.. 00 13 A2 00 40 53 A7 C6 35 00 01 20
..h~. . . . . 00 00 00 72 7E 00 10 82 00 13 A2 00
@S..?.. 40 53 A7 C6 30 00 01 20 00 00 00 77
..h~. . . . . 7E 00 10 82 00 13 A2 00 40 53 A7 C6
@S..5.. 35 00 01 20 00 00 00 72
..r~. . . . .
@S..0..
..w~. . . . .
@S..5.. . . . .r]

COM26 | 1200 8-N-1 FLOW:NONE | Rx: 260 bytes

```

Figura 4.19 Cadena de caracteres enviados por un periférico

#### **Resultados:**

El módulo Terminal del software X-CTU nos muestra los caracteres enviados por el módulo Xbee que actúa como periférico. En esta prueba se observa que el dispositivo Xbee 13A2004053A7C6 envía su cadena de caracteres informando que el sensor está activado. Debido a que todos los dispositivos Xbee que se

encuentran en los periféricos tienen la misma configuración, con esta prueba se demuestra que los periféricos trabajan correctamente y que el microcontrolador va a recibir los datos correctos para su procesamiento

#### **4.2.2 PRUEBA DE FUNCIONAMIENTO DEL CEREBRO DEL SISTEMA**

Se realizó la prueba de funcionamiento del cerebro del sistema considerando que los periféricos funcionan y envían los datos correctos. Para probar el procesamiento de datos por parte del cerebro del sistema hay que inicializarlo.

##### ***Prueba 1:***

Inicialización del sistema

Se energizó el sistema de alarma con 12V

El microcontrolador se inicializó (led amarillo encendido) y envió un mensaje al LCD:

BIENVENIDO - CAMBIO DE CLAVE  
INGRESE CLAVE PROVISIONAL

El microcontrolador realizó el cambio de clave provisional (0,0,0,0), para ello esperó que se ingrese los cuatro dígitos de la nueva clave:

El microcontrolador envió al LCD el siguiente mensaje:

INGRESE DIGITO 1	el usuario ingresara digito 0
INGRESE DIGITO 2	el usuario ingresara digito 0
INGRESE DIGITO 3	el usuario ingresara digito 0
INGRESE DIGITO 4	el usuario ingresara digito 0

Luego de que el microcotrolador aceptó la clave provisional, solicitó la nueva clave:

INGRESE NUEVO DIGITO 1	el usuario ingresara el nuevo digito 1
INGRESE NUEVO DIGITO 2	el usuario ingresara el nuevo digito 2
INGRESE NUEVO DIGITO 3	el usuario ingresara el nuevo digito 3
INGRESE NUEVO DIGITO 4	el usuario ingresara el nuevo digito 4

Luego de haber cambiado la clave provisional el sistema mostró el texto:

CLAVE CAMBIADA  
EL SISTEMA SE ACTIVARA EN 60s

Al transcurrir 60s el sistema mostró el texto:

SISTEMA ACTIVADO

El sistema fue activado (led verde encendido) y estuvo listo para recibir datos del dispositivo Xbee para su respectivo procesamiento.

### ***Resultado:***

La Prueba 1 de inicialización del sistema fue probada con el cambio de varios passwords obteniendo un resultado exitoso que demuestra la estabilidad del sistema.

### ***Prueba 2:***

Procesamiento de datos

Los dispositivos Xbee fueron configurados para enviar una trama de datos cada segundo, por tanto, el cerebro del sistema debió estar listo para recibir esta información. Si bien los dispositivos Xbee envían tramas cada segundo es

incontrolable la diferencia de tiempo entre el envío de las tramas de los 5 dispositivos Xbee.

Al enviar 20 bytes de datos por cada trama a 1200 bps, el tiempo que toma esta transmisión es de 133.33 ms.

En el peor de los casos una trama ingresa al microcontrolador seguida inmediatamente por otra y el tiempo que toma el microcontrolador para procesar los datos e identificar si el mensaje indica activación de un sensor, debe ser menor al tiempo de ingreso del primer bit de la siguiente trama.

A 1200 bps el tiempo de ingreso de un bit es de 0.83 ms, comparado con el tiempo de varios micro segundos que toma el microcontrolador en analizar los datos no existe probabilidad de pérdida de ninguna trama.

Con el sistema inicializado y los periférico funcionales, se activó los sensores intencionalmente. Con esta activación el cerebro del sistema cambia su estado:

El microcontrolador envió al LCD el texto:

**INTRUSO - EL SISTEMA SE ACTIVARA EN 30s**

Luego de 30s el microcontrolador mostró el texto:

**INTRUSO**

El microcontrolador activó la sirena y el sistema de monitoreo mostró el dispositivo activado (Figura 4.20).



Figura 4.20 Sistema de monitoreo activado

**Resultado:**

La Prueba 2 de procesamiento de datos demuestra que al ser activados varios sensores al mismo tiempo los datos son enviados al cerebro del sistema, estos son debidamente procesados y activan la sirena. El periférico que envía primero la trama de datos es mostrado como sensor activado en el sistema de monitoreo con lo cual demuestra el éxito del procesamiento de datos.

**Resultado Final:**

Las pruebas realizadas demuestran que tanto los periféricos del sistema como el cerebro y su procesamiento de datos trabajan correctamente y son estables.

### 4.3 PRUEBAS DE CONSUMO DE CORRIENTE

Se realizaron las pruebas de consumo de corriente considerando que se utilizó una fuente de 12 V-1A, la cual alimenta todo el sistema. Para medir el consumo de corriente total del sistema se realizó una medición parcial al cerebro del sistema, al interfaz de usuario y a los periféricos del sistema. Esta medición fue realizada con el uso de un amperímetro.

#### **4.3.1 CONSUMO DE CORRIENTE DEL CEREBRO DEL SISTEMA**

Los elementos que consumen corriente en el cerebro del sistema son: el microcontrolador, el MAX232, la sirena, los leds indicadores de actividad y el dispositivo Xbee.

De acuerdo a la medición el consumo de corriente del cerebro del sistema, esta fue de 70 mA y se mantiene constante cuando el sistema está habilitado y también cuando esta deshabilitado.

Se activó un sensor intencionalmente y el cerebro cambió su estado hacia activado, la sirena se encendió y el consumo de corriente aumentó a 470 mA.

#### **4.3.2 CONSUMO DE CORRIENTE DEL INTERFAZ DE USUARIO**

El elemento que consume corriente en el interfaz de usuario es el LCD, el cual al estar utilizando el backlite, mantuvo un consumo constante de corriente de 13 mA.

#### **4.3.3 CONSUMO DE CORRIENTE DE LOS PERIFERICOS DEL SISTEMA**

Los elementos que consumen corriente en los periféricos del sistema son los dispositivos Xbee y los sensores de movimiento.

Los dispositivos Xbee mantuvieron un consumo de corriente de 55 mA y los sensores de movimiento mantuvieron un consumo promedio de 16 mA.

El sistema dispone de 5 periféricos y 2 sensores de movimiento, por tanto el consumo total de corriente en los periféricos fue de 307 mA.

**Resultado:**

Se midió parcialmente el consumo de corriente de los elementos del sistema. El consumo total de corriente del sistema cuando no está activado es de 390 mA. Este consumo representa el 39% de la corriente máxima disponible de la fuente de energía.

Cuando el sistema está activado y la sirena encendida el consumo de corriente es de 790 mA. Este consumo representa el 79% de la corriente máxima disponible de la fuente de energía.

Con estos resultados se demuestra que la fuente de energía de 12V-1A es suficiente para alimentar el sistema sin problemas.

Debido a que la fuente que alimenta el sistema toma la energía de la red eléctrica del edificio es necesario disponer de una batería de respaldo que mantenga al sistema funcional en caso de ausencia de esta energía.

La capacidad de la batería depende del número de horas que el sistema debe funcionar con ausencia de la energía del edificio. Se escogió una batería de 12V-7Ah con la cual el tiempo aproximado de energía para el sistema cuando no está activado es de 17,9 horas. El tiempo aproximado de energía para el sistema cuando está activado y la sirena encendida es de 8,8 horas.

#### **4.4 DETALLE DE COSTOS QUE INCURRIERON EN LA IMPLEMENTACIÓN DEL PROYECTO**

Para realizar la implementación del proyecto se realizó el análisis de ingeniería correspondiente. Este análisis incurrió en un costo de \$400

#### 4.4.1 COSTO DE CONSTRUCCION DEL CEREBRO DEL SISTEMA (Tabla 4.1):

Elemento	Costo (\$)
Dispositivo Xbee	33,00
Microcontrolador PIC16F877A	6,75
Sirena	5,10
Elementos electrónicos varios	14,50
Caja portadora del circuito	4,00
<b>TOTAL</b>	<b>63,35</b>

Tabla 4.1 Costo de construcción del cerebro del sistema

#### 4.4.2 COSTO DE CONSTRUCCION DEL INTERFAZ DE USUARIO (Tabla 4.2):

Elemento	Costo (\$)
Display LCD	6,90
Teclado	7,50
Elementos electrónicos varios	5,60
Caja portadora del circuito	4,00
<b>TOTAL</b>	<b>24,00</b>

Tabla 4.2 Costo de construcción del interfaz de usuario

#### 4.4.3 COSTO DE CONSTRUCCION DE LOS PERIFERICOS DEL SISTEMA (Tabla 4.3):

Elemento	Costo (\$)
Dispositivo Xbee	33,00
Elementos electrónicos varios	1,50
Caja portadora del circuito	2,00
<b>SUBTOTAL</b>	<b>36,50</b>
<b>TOTAL</b>	<b>182,5</b>

Tabla 4.3 Costo de construcción de los periféricos del sistema

#### 4.4.4 COSTO DE CONSTRUCCION DE LA FUENTE DE ENERGIA (Tabla 4.4):

Elemento	Costo (\$)
Transformador	5,85
Elementos electrónicos varios	2,50
Caja portadora del circuito	2,50
Batería	31,00
<b>TOTAL</b>	<b>41,85</b>

Tabla 4.4 Costo de construcción de la fuente de energía

#### 4.4.5 COSTOS VARIOS (Tabla 4.5):

Elemento	Costo (\$)
Kit de desarrollo Xbee	164,00
Cable de datos	10,00
Cable de energía	10,00
<b>TOTAL</b>	<b>184,00</b>

Tabla 4.5 Costos varios

El costo total en el cual incurrió la implementación del proyecto fue de: \$895,70

Los dispositivos Xbee y el kit de desarrollo Xbee son elementos que no están disponibles en Ecuador, por tanto, fueron importados de Estados Unidos de Norteamérica.

En el presente capítulo se describió las pruebas realizadas que validan el funcionamiento del sistema de alarma y demuestran la estabilidad del mismo. También se describió el costo en el cual incurrió la implementación del proyecto. En el siguiente capítulo se describirá la posibilidad de ampliación de este sistema de alarma hacia diversos sitios de relevancia que no disponen de seguridad anti intrusos.

## **CAPITULO 5**

### **POSIBILIDADES DE AMPLIACIÓN A OTROS AMBIENTES CERCANOS**

En el presente capítulo se realiza un pequeño análisis de las posibilidades de expansión que se puede tener con este sistema de seguridad, para ello se toma en cuenta algunos laboratorios carentes de protección, cercanos al laboratorio en el que se implementa el sistema de seguridad.

El propósito principal es dar una visión del funcionamiento, mostrar cuales deberían ser los cambios claves en el diseño base para soportar el aumento del área de cobertura que desea protegerse, así como el aumento de los dispositivos (sensores) que requiera el usuario.

Dentro de este proyecto se ha visto la necesidad de incluir este capítulo debido a que la mayoría de los ambientes que, en la actualidad, se desea proteger no están limitados por la distancia y son en su mayoría susceptibles a cambios de estructura, de distribución, entre otros factores, que harían que un sistema estático sea bastante obsoleto frente a esas necesidades. Por ello se da una solución breve para ese tipo de ambientes; mostrando cuáles serían los cambios estratégicos que conseguirán crear una red dinámica que responda a los requerimientos de expansibilidad.

#### **5.1 DESCRIPCIÓN**

Los laboratorios que se han considerado para la ampliación del sistema son de forma específica los existentes en el edificio Eléctrica-Química:

- Laboratorio de transmisión ubicado en el 8º piso
- Laboratorio de instrumentación ubicado en el 6º piso

Se han escogido estos laboratorios debido a la cercanía de los mismos al sitio protegido por el sistema diseñado.

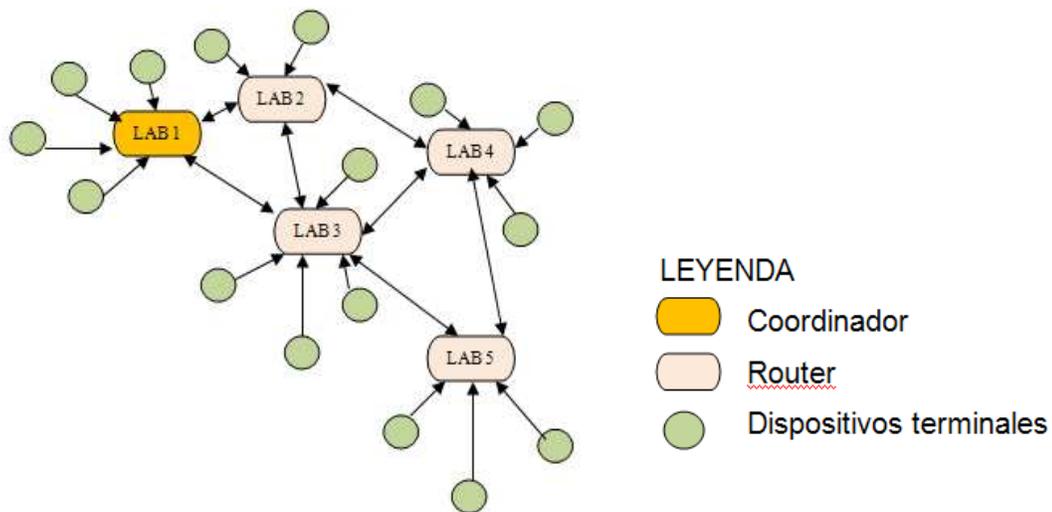


Figura 5.1 Diagrama General del Sistema de Seguridad Extendido

El sistema expandido a los demás laboratorios tendría la siguiente estructura como se muestra en la Figura 5.1:

1. Se tendrá un cerebro por cada laboratorio además del interfaz de usuario para controlar el lugar de forma local.
2. Existirá en cada laboratorio el número de dispositivos terminales necesarios para cubrir con las necesidades de seguridad (en puertas, ventanas, pasillos, etc.).
3. Se colocará obligatoriamente un dispositivo router en cada laboratorio de modo que este realice las funciones de coordinador local, el mismo que se comunicará con el coordinador central para dar alerta de producirse alguna irrupción a cualquiera de sus dispositivos terminales ahí colocados.
4. Se necesitará centralizar el sistema de monitoreo y en general el sistema de seguridad, esto dará la opción de contar con una persona de seguridad que se encargue de dar aviso oportuno y tomar las medidas necesarias para detener el posible robo de los lugares protegidos.

## **5.2 TOPOLOGIA FISICA DEL SISTEMA**

La topología del sistema será en estrella ya que cada red estará inalámbricamente conectada por medio de los routers al coordinador del cerebro central.

## **5.3 TOPOLOGIA LOGICA DEL SISTEMA**

La topología lógica del sistema es en malla debido a que todos los dispositivos routers se pueden comunicar entre sí, con el coordinador y con los dispositivos terminales.

## **5.4 REQUERIMIENTOS DE HARDWARE**

El hardware descrito en el Capítulo 2 sirve para la ampliación de la red, de este modo se tendría un sistema como el implementado en el laboratorio escogido. Para cada laboratorio que se desee adjuntar al sistema de seguridad, el único cambio en hardware que se debe considerar es en cuanto a los dispositivos Zigbee, los routers de cada red local y el coordinador central deben tener la capacidad de comunicarse en una red malla; además, deben tener una mayor cobertura para poder alcanzar grandes distancias.

### **5.4.1 DISPOSITIVOS ZIGBEE**

#### **5.4.1.1 Dispositivos Router**

Los dispositivos que se seleccionará para la ampliación del sistema son los que pueden formar mallas y que tienen un mayor alcance dentro de sus características. El protocolo ZigBee de estos módulos está diseñado para trazar automáticamente una ruta entre varios nodos sin la necesidad de la intervención del usuario. La principal ventaja que se visualiza es la capacidad de auto-renovar

las rutas hacia el destino dependiendo de los cambios que pueda sufrir la red durante la transmisión de la información.

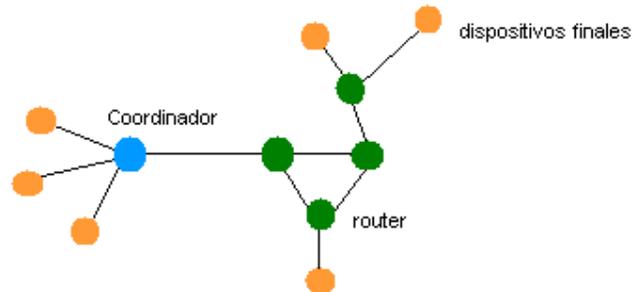


Figura 5.2 Red Malla que forman los dispositivos

Los dispositivos seleccionados son los XBee-PRO ZB, las características principales se detallan a continuación:

#### 5.4.1.1.1 Especificaciones

Especificaciones generales	XBee-PRO ZB
Firmware	802.15.4
Topologías de red	Malla; Punto-punto; Punto-Multipunto
Rango urbano indoor	90 m
Rango con línea de vista outdoor	1,6 km

Tabla 5.1 Especificaciones generales de los dispositivos ZigBee

#### Características Generales

- Interfaz serial de datos  
3.3V CMOS UART
- Método de Configuración  
comandos API o AT, localmente o por aire
- Banda de frecuencia de Operación  
ISM 2.4 GHz (2.4000 - 2.4835 GHz)

- Inmunidad a la interferencia  
canales con DSSS (Direct Sequence Spread Spectrum)  
4 entradas ADC de 10-bit  
10 I/O Digitales
- Velocidad de transmisión  
1200Kbps – 1 Mbps

### **Performance**

- Potencia de Transmisión  
63 mW (+18 dBm) EIRP(10 Mw (+10 dBm))
- Sensibilidad del receptor (1% PER)  
-102 dBm

### **Networking y Seguridad**

- Encriptación  
AES 128-bit
- Confiabilidad del envío de paquetes  
Retransmisión y acuses de recibo (Acknowledgments)
- Direccionamiento de 64 bits IEEE MAC
- Canales  
13

### **Requerimientos de Energía**

- Fuente de Voltaje: 3.0- 3.4 VDC
- Corriente de Transmisión (a 3.3 V): 295mA
- Corriente de recepción (a 3.3 V): 45mA
- Power-down current: 10  $\mu$ a (a 25  $^{\circ}$ C)

### **Antena**

- Wire Whip Antena

## Dimensiones

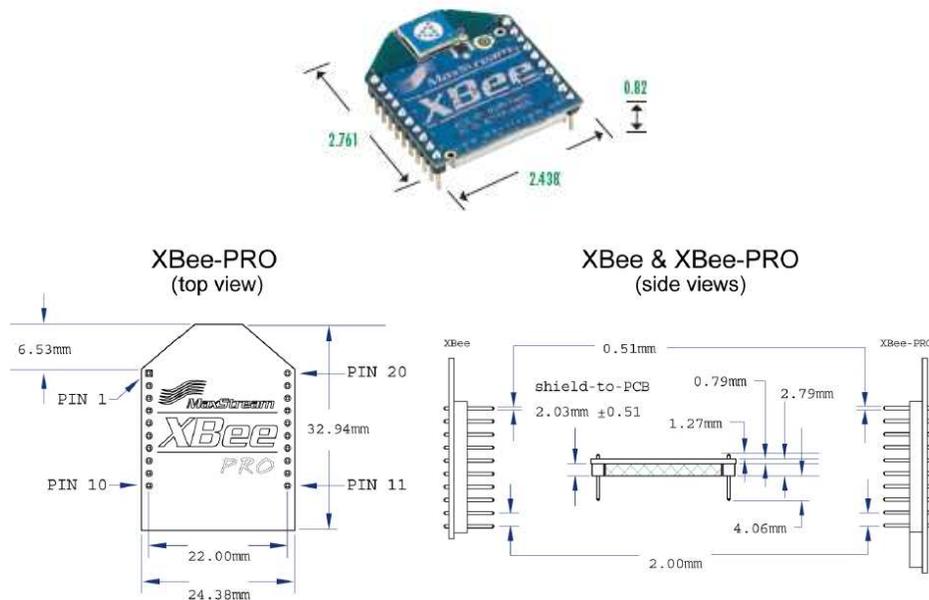


Figura 5.3 Dimensiones de los dispositivos Xbee-PRO

### 5.4.1.2 Dispositivos Terminales

Los dispositivos terminales que se usará son los mismos que se han señalado en el Capítulo 2 en el punto 2.5.1. Son los módulos ZigBee marca XBee Series 1, las especificaciones se visualizan en la Tabla 2.1.

## 5.5 ANALISIS DE LOS SITIOS

Una visión general de los laboratorios a los que se extenderá el sistema de seguridad diseñado se muestran a continuación:

### 5.5.1 CENTRO DE MONITOREO (GARITA DE LOS GUARDIAS)

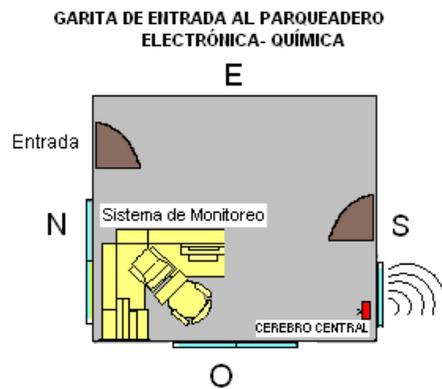


Figura 5.4 Centro de monitoreo (garita entrada Eléctrica-Química)

#### 5.5.1.1 Lugar de instalación de los equipos

La garita de los guardias se ha escogido por la seguridad y por las medidas inmediatas que podrán tomarse al ocurrir una violación de seguridad en las instalaciones de los laboratorios mencionados. El sistema dentro de este ambiente consta únicamente de un modulo cerebro al que se comunicarán todos los dispositivos routers de los tres laboratorios. El cerebro central físicamente se ubicará como se observa en la Figura 5.4.

## 5.5.2 LABORATORIO DE INSTRUMENTACION

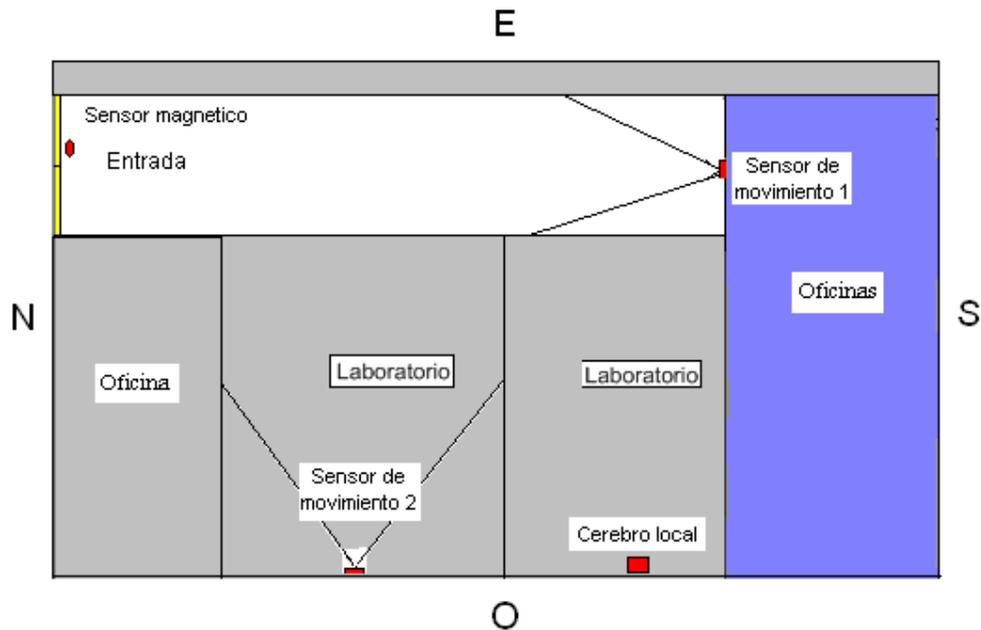


Figura 5.5 Diagrama del Laboratorio de Instrumentación

### 5.5.2.1 Topología Física

La topología física que se utilizaría es la topología en estrella. Cada uno de los dispositivos finales estarán conectados de forma inalámbrica únicamente con el coordinador, para cada una de las redes implementadas en los laboratorios.

### 5.5.2.2 Topología Lógica

La topología lógica que se utilizaría es la topología en estrella la cual permite solo las comunicaciones dispositivo final-coordinador.

### 5.5.2.3 Lugar de instalación de los equipos

El sistema dentro de este laboratorio consta de un modulo cerebro y tres módulos finales. Se tienen dos sensores de movimiento, un sensor magnético y el cerebro local.

Los dispositivos físicamente se han ubicado como se observa en la Figura 5.5.

### 5.5.3 LABORATORIO DE TRANSMISIÓN Y SISTEMAS RADIANTES

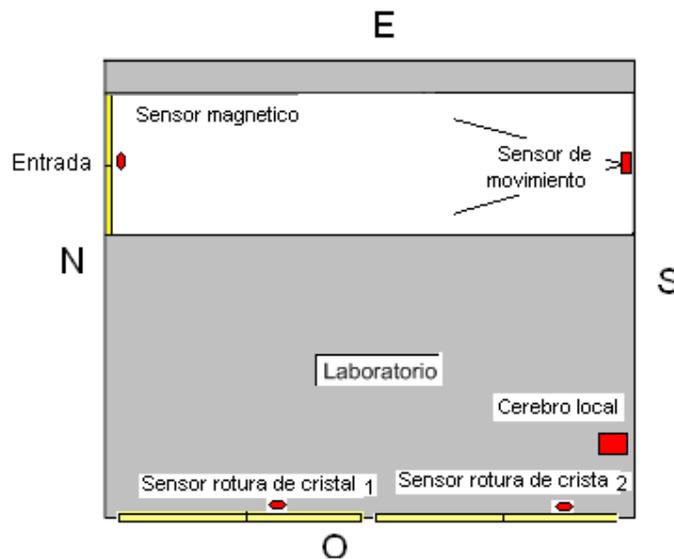


Figura 5.6 Diagrama del Laboratorio de Transmisión

#### 5.5.3.1 Topología Física

La topología física que se utilizará es la topología en estrella. Cada uno de los dispositivos finales estarían conectados de forma inalámbrica únicamente con el coordinador, para cada una de las redes implementadas en los laboratorios.

#### 5.5.3.2 Topología Lógica

La topología lógica que se utilizará es la topología en estrella la cual permite solo las comunicaciones dispositivo final-coordinador.

### **5.5.3.3 Lugar de instalación de los equipos**

Laboratorio de transmisión ubicado en el 8º piso consta de un modulo cerebro y cuatro módulos terminales: un sensor de movimiento, un sensor magnético y un sensor de rotura de vidrios.

Los dispositivos físicamente se encuentran ubicados como se observa en la Figura 5.6.

## **5.6 CAMBIOS EN EL SISTEMA DE MONITOREO**

Las modificaciones a realizarse en el software original serían las que se describen a continuación:

### **5.6.1 REQUERIMIENTOS DE SOFTWARE**

El sistema ampliado el monitoreo estaría centralizado en la garita de entrada donde el encargado tendrá la posibilidad de monitorear todos los laboratorios desde ese lugar.

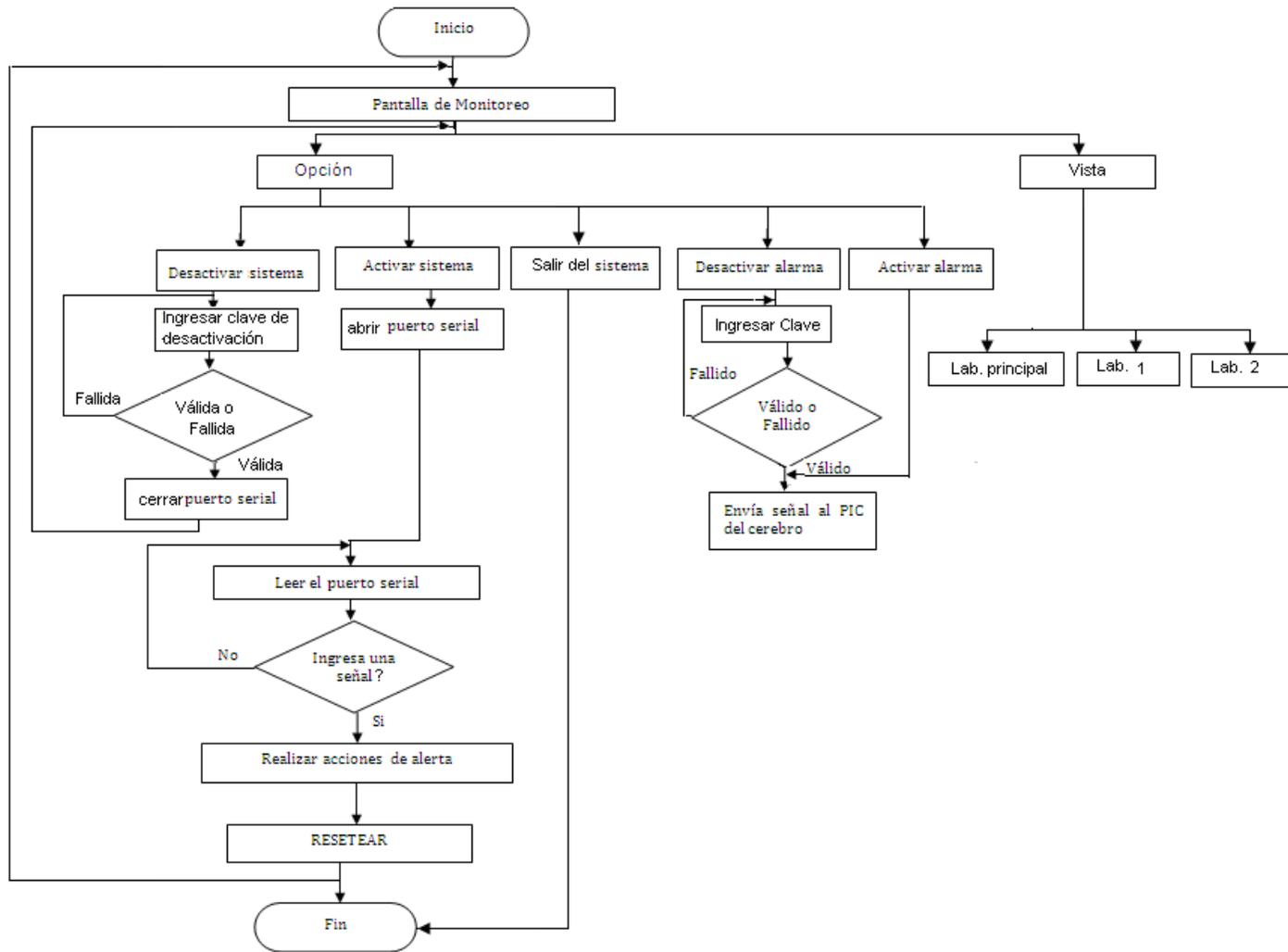


Figura 5.7 Diagrama de flujo del funcionamiento del programa "Security Soft"

Las opciones generales que posee el Software actual, revisadas en el Capítulo 3, serán las mismas. Para la programación del sistema de monitoreo ampliado se ha realizado algunos cambios en el diagrama de flujo como se puede visualizar en la Figura 5.6. Los cambios en la estructura de programación son pocos y se describen a continuación:

En lo que se refiere a menú Opciones:

**Activar alarma**

Enviar una señal por el puerto serial al cerebro central del sistema de seguridad.

**Fin de Tarea**

**Desactivar alarma**

Passar a pantalla de desactivación

**Fin de Tarea**

**Ingresar Clave**

Si clave Válida

Enviar una señal por el puerto serial al cerebro central del sistema de seguridad.

El PIC activa o desactiva la alarma

Caso contrario

Regresar a petición de clave

**Fin de Tarea**

En lo que se refiere a menú Vistas:

Se tiene la posibilidad de visualizar tres pantallas diferentes que representan a cada laboratorio dotado del sistema de seguridad diseñado.

Para cumplir con las necesidades expuestas del sistema, el requerimiento básico en cuanto a software se basa principalmente en:

- Dentro del entorno visual, el aumento de las diferentes plantas de los laboratorios mencionados de modo que se pueda visualizar mediante una barra de menú, ubicado en la parte superior, los distintos laboratorios y los dispositivos allí colocados. Para ello se deberá únicamente realizar el esquema general del área y distribución de cada laboratorio mencionado. Como se puede observar en la Figura 5.8.
- Dentro de la programación de los objetos que se añadirían en nuestro entorno, se realizará un llamado de las subrutinas que se programó para el

software del laboratorio implementado inicialmente, esto facilita la adecuación del software para las necesidades del expansión.

- Otra implementación que se haría en cuanto al Software sería crear una Subrutina que sea capaz de permitir al usuario del programa Activar y Desactiva de forma remota la Alarma de Seguridad; es decir, permitir una comunicación serial PC-PIC. Esta opción facilitaría al administrador de sistema de seguridad el manejo del mismo.

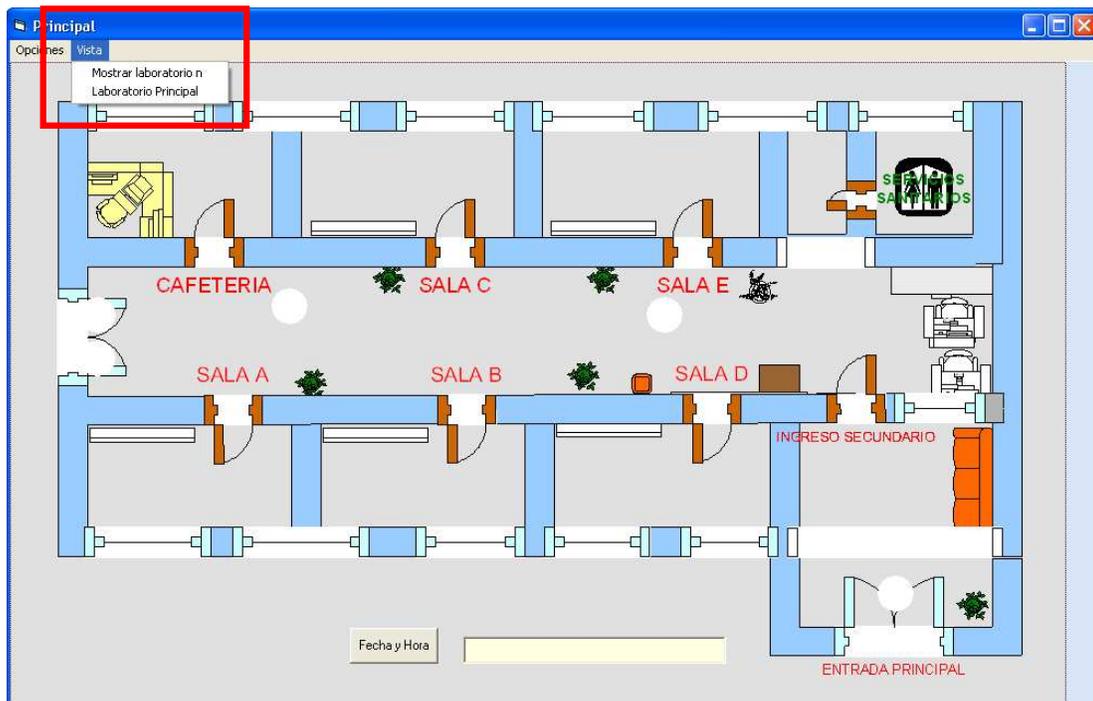


Figura 5.8 Vista de los diferentes laboratorios

## 5.7 COSTO DE LA AMPLIACION DEL SISTEMA DE SEGURIDAD

Debido a que se tiene el sistema implementado en uno de los laboratorios los costos en los cuales se tiene que incurrir son de forma general para los demás laboratorios a excepción del dispositivo Xbee que actúa como coordinador en el laboratorio actualmente protegido, el cual debe ser actualizado:

### 5.7.1 COSTO DE CONSTRUCCION DEL CEREBRO DEL SISTEMA

Para cada laboratorio se instalará un cerebro, además del que se encuentra en la garita donde se centralizará el sistema de monitoreo, así se tiene tres con el siguiente desglose de costos.

Elemento	Costo (\$)
Dispositivo Xbee-PRO	46,00
Microcontrolador PIC16F877A	6,75
Elementos electrónicos varios	14,50
Caja portadora del circuito	4,00
<b>SUBTOTAL</b>	71,25
Dispositivo Xbee-PRO actualizado	46,00
<b>TOTAL</b>	259,75

Tabla 5.2 Costo de construcción del cerebro del sistema

### 5.7.2 COSTO DE CONSTRUCCION DEL INTERFAZ DE USUARIO

Al igual que el cerebro se usarán 3 interfaces de usuario que pertenecerán a cada red:

Elemento	Costo (\$)
Display LCD	6,90
Teclado	7,50
Elementos electrónicos varios	5,60
Caja portadora del circuito	4,00
<b>SUBTOTAL</b>	24,00
<b>TOTAL</b>	72,00

Tabla 5.3 Costo de construcción del interfaz de usuario

### 5.7.3 COSTO DE CONSTRUCCION DE LOS PERIFERICOS DEL SISTEMA

- Circuito para las puertas, se necesitan 2

Elemento	Costo (\$)
Dispositivo Xbee	33,00
Elementos electrónicos varios	1,50
Sensor magnético	2,00
Caja portadora del circuito	2,00
<b>SUBTOTAL</b>	<b>38,50</b>
<b>TOTAL</b>	<b>77,00</b>

Tabla 5.4 Costo de construcción de circuito para puerta

- Circuito para los pasillos, se necesitan 3

Elemento	Costo (\$)
Dispositivo Xbee	33,00
Elementos electrónicos varios	1,50
Sensor de movimiento	20,00
Caja portadora del circuito	2,00
<b>SUBTOTAL</b>	<b>56,50</b>
<b>TOTAL</b>	<b>169,50</b>

Tabla 5.5 Costo de construcción circuito para pasillo

- Circuito para las ventanas, se necesitan 2

Elemento	Costo (\$)
Dispositivo Xbee	33,00
Elementos electrónicos varios	1,50
Sensor de rotura de vidrios	25,00
Caja portadora del circuito	2,00
<b>SUBTOTAL</b>	61,50
<b>TOTAL</b>	123,00

Tabla 5.6 Costo de construcción circuito para ventana

#### 5.7.4 COSTO DE CONSTRUCCION DE LA FUENTE DE ENERGIA

Al igual que el cerebro se usarán 3 fuentes de energía que pertenecerán a cada laboratorio:

Elemento	Costo (\$)
Transformador	5,85
Elementos electrónicos varios	2,50
Caja portadora del circuito	2,50
Batería	31,00
<b>SUBTOTAL</b>	41,85
<b>TOTAL</b>	125,55

Tabla 5.7 Costo de construcción de la fuente de energía

### 5.7.5 COSTOS VARIOS

Elemento	Costo (\$)
Cable de datos	30,00
Cable de energía	30,00
<b>TOTAL</b>	<b>60,00</b>

Tabla 5.8 Costos varios

El costo en el cual se incurrirá para la ampliación del sistema de seguridad a los dos laboratorios adicionales será de: \$886,80

El costo de Ingeniería será de: \$300,00

El costo total será por lo tanto de: **\$1186,80**

En el presente capítulo se describió los sitios cercanos al laboratorio, relevantes en importancia y carentes de protección. Se diseñó un sistema de alarma para estos sitios.

En el siguiente capítulo se describirán las conclusiones y recomendaciones.

## CAPITULO 6

### CONCLUSIONES Y RECOMENDACIONES

#### 6.1 CONCLUSIONES

Las características de los dispositivos Xbee Series 1 y su facilidad de configuración e instalación los dotan de una excelente robustez. Esta robustez nos permite concluir que estos dispositivos junto a sensores apropiados, son adecuados para ser utilizados en nuestro sistema de alarma anti intrusos, con lo cual cualquier el sistema es dotado de una efectividad al momento de mantener una comunicación inalámbrica.

El microcontrolador PIC16F877A es un elemento resistente y de fácil programación. Estas características nos permiten concluir que al momento de utilizarlo como elemento de procesamiento de datos provee a nuestro sistema anti intrusos la robustez necesaria para cumplir con las tareas encomendadas.

El sistema anti intrusos fue diseñado para que la comunicación entre el cerebro y los periféricos del mismo sea efectuada con línea de vista. Esta opción nos permite concluir que la comunicación es completamente efectiva a pesar de presentarse cualquier obstáculo, incluso en un sistema sin línea de vista la comunicación se mantendría efectiva hasta los 30 m indoor.

El software de monitoreo del sistema anti intrusos muestra al responsable de la seguridad de una forma muy sencilla y grafica el lugar protegido. Esta característica nos permite concluir que para cualquier evento que se presente, el sistema está listo para mostrar señales visuales informativas.

La interfaz grafica del software de monitoreo es bastante amigable al usuario al estar desarrollada con Microsoft Visual Basic 6.0 y al estar empaquetada con Security Soft. Estas prestaciones nos permiten concluir que cualquier responsable de la seguridad puede identificar sin problemas al sistema e instalarlo en cualquier maquina con un sistema operativo Windows 98, 2000 y XP.

De acuerdo a las pruebas de funcionamiento del sistema podemos concluir que el diseño e implementación del mismo fue realizado conforme a las necesidades de protección anti intrusos demostrando la estabilidad y eficiencia total del sistema.

Se realizó el diseño para la ampliación del sistema de seguridad para dos laboratorios que se encuentran en el mismo edificio considerando un sistema de monitoreo centralizado en la garita principal. De acuerdo a este diseño podemos concluir que la comunicación de los 3 laboratorios con la garita se puede realizar sin problemas construyendo una red Zigbee en malla y utilizando dispositivos routers de mayor alcance.

El estándar Zigbee es un conjunto de protocolos de comunicación inalámbrica de bajo consumo, basado en el estándar 802.15.4 de redes WPANs. Este estándar fue diseñado para ser utilizado en aplicaciones que requieren una comunicación segura con una baja tasa de envío de datos, por lo cual se puede concluir que sus características lo hacen ideal para utilizarlo como nivel de comunicaciones de nuestro sistema anti intrusos.

## **6.2 RECOMENDACIONES**

Se recomienda que en el caso de realizar una ampliación al presente sistema se realice un análisis de los dispositivos Xbee disponibles en el mercado, esto debido al desarrollo constante en las características de los mismos.

Se recomienda ubicar los dispositivos Xbee de tal forma que puedan mantener línea de vista y de esta forma garantizar que las comunicaciones sean eficientes.

Se recomienda utilizar la tecnología Zigbee en sistemas de alarma debido a su gran eficiencia en la comunicación de datos inalámbricos.

## REFERENCIAS BIBLIOGRAFICAS

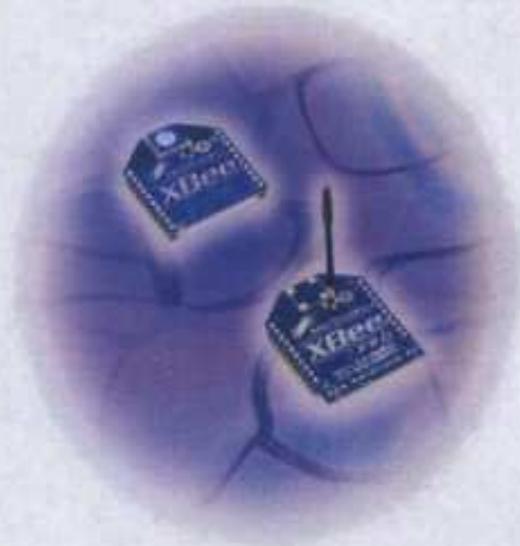
1. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), IEEE 802.15.4-2006. (PDF)
2. "ZigBee Competitive Technology Analysis", ZigBee Alliance (PDF)
3. ZigBee: "Wireless Control That Simply Works", William C. Craig (PDF)
4. "Vision for the Home", ZigBee Alliance (PDF)
5. ZigBee Enables Smart Buildings of the Future Today, ZigBee Alliance (PDF)
6. ZigBee: The Choice for Energy Management and Efficiency, ZigBee Alliance (PDF)
7. Microcontroladores PIC Programación en Basic, Carlos A. Reyes, 2 Edición, Págs. 1-15, 17-23, 33-41, 79-84, 98-114, 127-142179-186.
8. Electrónica Práctica con Microcontroladores PIC, Santiago Corrales, Págs. 9-24, 95-119.
9. Datasheet Digi, XBee™ ZigBee®/802.15.4 Modules (PDF)
10. Manual XBee \XBee-Pro OEM RF Modules, DIGI (PDF)
11. <http://www.ieee802.org/15/pub/TG4.html>
12. <http://www.eetimes.com/showArticle.jhtml?articleID=173600329>
13. <http://www.scribd.com/doc/101172/pic16f877-en-espanol1>
14. <http://es.wikipedia.org/wiki/ZigBee>
15. <http://www.digi.com/>
16. <http://www.monografias.com/trabajos17/manual-visual/manual-visual.shtml>
17. <http://www.programatium.com/vb.htm>

## **ANEXOS**

## **ANEXO 1: Digi, XBee™ ZigBee®/802.15.4 Modules**

# XBee™ ZigBee® /802.15.4 Modules

2.4 GHz OEM RF Modules



Part of Digi's Drop-in Networking product family, XBee OEM RF modules provide reliable, wireless data communication over ZigBee/802.15.4 networks. Available in Series 1 or Series 2 models for point-to-multipoint or mesh topologies, they enable OEMs with excellent wireless performance in a cost-effective, small form factor solution.



## Features/Benefits

- ZigBee/802.15.4 compatible RF modules
- 2.4 GHz ISM band for use worldwide
- Fully interoperable with other Digi Drop-in Networking products, including gateways, device adapters and extenders
- Available in Series 1 or Series 2 models for point-to-multipoint or mesh topologies
- Pin-swappable regular and long-range-PRO versions
- Low cost
- Common footprint for a variety of Digi RF modules
- Low-power sleep modes
- Multiple antenna options
- Industrial temperature (-40° C to 85° C)

## Overview

The XBee family of ZigBee/802.15.4 RF modules is the premiere choice for OEMs looking for excellent wireless performance in a cost-effective, small form factor solution. Each XBee module comes in either a regular or long-range \*-PRO\* version\*. All XBee modules are pin-for-pin compatible with the exception of a few varying I/O features, which provides a standard footprint for OEMs with multiple applications.

XBee Series 1 is based on ZigBee/802.15.4 silicon from Freescale\*. Its 802.15.4 firmware feature set makes it ideal for point-to-point, peer-to-peer, and point-to-multipoint (star) topologies. The XBee Series 1 gives the user maximum control over network nodes and minimum latency.

XBee Series 2 is based on ZigBee/802.15.4 silicon from Ember\*\*. It features ZigBee firmware for creating ad-hoc mesh networks. The XBee Series 2 performs automatic route discoveries to create a self-healing network of full-function routers and low-power end devices. XBee Series 1 and Series 2 modules do not communicate with one another.

Known for ease of use, the XBee modules are ready to operate out of the box and offer simple AT commands or an API for advanced, user-settable configurations. XBee modules are recognized worldwide for reliable wireless data communication in the license free 2.4 GHz ISM band. Visit our website for a complete listing of countries that have approved the XBee as a certified, license-free RF module with no need for further testing.

XBee modules are a part of Digi's full line of Drop-in Networking products. ConnectPort X gateways and XBee device adapters, modules and extenders provide end-to-end wireless connectivity to commercial-grade electronic devices in locations where wired infrastructure does not exist or satisfy customer needs. To learn more about Drop-in Networking, visit [www.digi.com/products/wirelessdropinetworking](http://www.digi.com/products/wirelessdropinetworking).



## Features/Specifications

Product Selection Guide	Series 1		Series 2	
Style	Hexacore		DigiCore	
Frequency	802.15.4		ZigBee	
Network Topologies	Point-to-point, peer-to-peer, point-to-multipoint (star)		Mesh	
	XBee™ Series 1	XBee-PRO™ Series 1	XBee™ Series 2	XBee-PRO™ Series 2*
Indoor/Urban range	100 ft (30 m)	300 ft (90 m)	120 ft (40 m)	n/a
Outdoor/RF Line-of-Sight Range	300 ft (90 m)	1 mi (1.6 km)	400 ft (120 m)	n/a
	 802.15.4 - Star		 ZigBee - Mesh	

\* XBee-PRO Series 2 zoning only.

### PERFORMANCE

- General**
- RF data rate: 250 Kbps
  - Operating temperature: -40° C to 85° C (-40° F to 185° F)
- Series 1 (XBee / XBee-PRO)**
- Indoor/Urban range: 100 ft (30 m) / 300 ft (90 m)
  - Outdoor/RF line-of-sight range: 300 ft (90 m) / 1 mi (1.6 km)
  - Transmit power output: 1 mW (0 dBm) / 40 mW (+18 dBm) -  
Note: In Europe XBee-PRO modules must be set to 10 mW (10 dBm), in Japan XBP modules are calibrated to 10 mW (10 dBm).
  - Receiver sensitivity (1% FER): -82 dBm / -100 dBm
- Series 2 (XBee)**
- Indoor/Urban range: 120 ft (40 m)
  - Outdoor/RF line-of-sight range: 400 ft (120 m)
  - Transmit power output: 1.25 mW (+1 dBm) (2 mW (+3 dBm) best mode)
  - Receiver sensitivity (1% FER): -87 dBm (-98 dBm best mode)

### FEATURES

- General**
- Serial data interface: 3.3V CMOS UART
  - Configuration method: API or AT commands, local or over-the-air
  - Frequency band: 2.4 GHz
  - Interference immunity: DSSS (Direct Sequence Spread Spectrum) channels
- Series 1**
- Serial data rate: 1200 - 250000 bps
  - 0/10-bit ADC inputs, (0) Digital I/O
- Series 2**
- Serial data rate: 1200 - 1 Mbps
  - 0/10-bit ADC inputs, (0) Digital I/O

### NETWORKING AND SECURITY

- Encryption: AES 128-bit
- Reliable packet delivery: Retries/Acknowledgments
- PAN ID, 64-bit IEEE MAC address, 16 channels (12 channels - XBee-PRO Series 1)

### POWER REQUIREMENTS

- Series 1 (XBee / XBee-PRO)**
- Supply voltage: 2.8 - 3.4 VDC / 2.8 - 3.4 VDC
  - Transmit current (0 1.3 V): 45 mA / 215 mA
  - Receive current (0 1.3 V): 50 mA / 55 mA
  - Power-down current: <10 uA / <10 uA
- Series 2 (XBee)**
- Supply voltage: 2.1 - 3.6 VDC
  - Transmit current (0 3.3 V): 35 mA (40 mA best mode)
  - Receive current (0 3.3 V): 38 mA (40 mA best mode)
  - Power-down current: <1 uA @ 25 °C

### ANTENNA OPTIONS

- Wire whip antenna
- Chip antenna
- U.F.L connector
- SMA female RF connector

### REGULATORY APPROVALS

- Series 1 (XBee / XBee-PRO)**
- US (FCC Part 15.247): OUI-XBEE / OUI-XBEE-PRO
  - Canada (IC): 4214A-XBEE / 4214A-XBEE-PRO
  - Europe (CE): ETS / ETS (max. tx power output: 10 mW)
  - Australia
  - Japan
- Series 2 (XBee)**
- US (FCC Part 15.247): OUI-XBEE2
  - Canada (IC): 4214A-XBEE2
  - Europe (CE): ETS
  - Japan



Please visit [www.digi.com](http://www.digi.com) for part numbers.

**DIGI SERVICE AND SUPPORT** - You can purchase with confidence knowing that Digi is here to support you with expert technical support and a one-year warranty. [www.digi.com/support](http://www.digi.com/support)

WHEN  
**RELIABILITY**  
MATTERS™

**Digi International**  
71001 Ross Road S.  
Waukegan, IL 60087  
USA  
Ph: 815-812-3444  
815-812-3444  
Tel: 815-812-4552  
email: [info@digi.com](mailto:info@digi.com)

**Digi International**  
France  
31 rue des Pommiers  
92150 Nanterre sur Seine  
Ph: +33-1-55-61-98-98  
Fax: +33-1-55-61-98-99  
[www.digi.fr](http://www.digi.fr)

**Digi International**  
UK  
1815 Building South St  
22-14 Salsburghs-Str.  
Wickham Ave  
Tokyo 170-0001, Japan  
Ph: +81-3-5478-0381  
Fax: +81-3-5478-0382  
[www.digi.co.jp](http://www.digi.co.jp)

**Digi International**  
(HK) Limited  
Suite 1103-01, 17/F,  
8 West Centre  
187 Joo Road  
North Point, Hong Kong  
Ph: +852-2573-1888  
Fax: +852-2573-9889  
[www.digi.cn](http://www.digi.cn)

**Digi International**, the leader in device networking for business, develops reliable products and technologies to connect and securely manage local or remote wireless devices over the network or via the web. With over 20 million units shipped worldwide since 1982, Digi offers the highest levels of performance, flexibility and quality.

[www.digi.com](http://www.digi.com)

© 2006-2007 Digi International Inc.

All rights reserved. Digi, Digi International, the Digi logo, the When Reliability Matters logo, ConnectPort, XBee, XBee-PRO and XBee2 are either trademarks or registered trademarks of Digi International Inc. in the United States and other countries worldwide. All other trademarks are the property of their respective holders.

91001413  
A1/1007



**ANEXO 2: XBee \XBee-Pro OEM RF Modules, Págs. 33-51**

### 3.3. Command Descriptions

Command descriptions in this section are listed alphabetically. Command categories are designated within "< >" symbols that follow each command title. Xbee/Xbee-PRO RF Modules expect parameter values in hexadecimal (designated by the "0x" prefix).

All modules operating within the same network should contain the same firmware version.

#### A1 (End Device Association) Command

<Networking (Association)> The A1 command is used to set and read association options for an End Device.

Use the table below to determine End Device behavior in relation to the A1 parameter.

AT Command: AT+A1

Parameter Range: 0 - 0x0F (bitfield)

Default Parameter Value: 0

Related Commands: ID (PAN ID), NI (Node Identifier), CH (Channel), CE (Coordinator Enable), A2 (Coordinator Association)

Minimum Firmware Version Required: v1.x80

Bit number	End Device Association Option
1 - ReservePanID	0 - Will only associate with Coordinator operating on PAN ID that matches node identifier 1 - May associate with Coordinator operating on any PAN ID
1 - ReserveChannel	0 - Will only associate with Coordinator operating on Channel that matches CH setting 1 - May associate with Coordinator operating on any Channel 0 - Device will not attempt Association
2 - ActAssociate	1 - Device attempts Association until success Note: This bit is used only for non-Beacon systems. End Device in a Beaconing system must always associate to a Coordinator
3 - PriCoordCapable	0 - Pri Wake will not poll the Coordinator for pending (direct) Data 1 - Pri Wake will send Pri Request to Coordinator to extract any pending data
4-7	(reserved)

#### A2 (Coordinator Association) Command

<Networking (Association)> The A2 command is used to set and read association options of the Coordinator.

Use the table below to determine Coordinator behavior in relation to the A2 parameter.

AT Command: AT+A2

Parameter Range: 0 - 7 (bitfield)

Default Parameter Value: 0

Related Commands: ID (PAN ID), NI (Node Identifier), CH (Channel), CE (Coordinator Enable), A1 (End Device Association), A5 (Active Scan), ED (Energy Scan)

Minimum Firmware Version Required: v1.x80

Bit number	End Device Association Option
0 - ReservePanID	0 - Coordinator will not perform Active Scan to locate available PAN ID. It will operate on ID (PAN ID) 1 - Coordinator will perform Active Scan to determine an available ID (PAN ID). If a PAN ID conflict is found, the ID parameter will change.
1 - ReserveChannel	0 - Coordinator will not perform Energy Scan to determine free channel. It will operate on the channel determined by the CH parameter 1 - Coordinator will perform Energy Scan to find a free channel. Then operate on that channel
2 - AllowAssociate	0 - Coordinator will not allow any devices to associate to it. 1 - Coordinator will allow devices to associate to it.
3-7	(reserved)

The binary equivalent of the default value (hex) is 0000110 - '111 0' is the last digit of the sequence.

### AC (Apply Changes) Command

<AT Command Mode Options> The AC command is used to explicitly apply changes to module parameter values. 'Applying changes' means that the module is re-initialized based on changes made to its parameter values. Once changes are applied, the module immediately operates according to the new parameter values.

AT Command: ATAC

Minimum Firmware Version Required: v1.4A0

This behavior is in contrast to issuing the WR (Write) command. The WR command saves parameter values to non-volatile memory, but the module still operates according to previously saved values until the module is re-booted or the CH (Exit AT Command Mode) command is issued.

Refer to the "AT Command - Queue Parameter Value" API type for more information.

### AI (Association Indication) Command

<networking (Association)> The AI command is used to indicate occurrences of errors during the last association request.

AT Command: ATAI

Parameter Range: 0 - 0x13 (read-only)

Use the table below to determine meaning of the returned values.

Related Commands: AS (Active Scan), ID (PAN ID), CH (Channel), ED (Energy Scan), A1 (End Device Association), A2 (Coordinator Association), CE (Coordinator Enable)

Minimum Firmware Version Required: v1.4B0

Returned Value (Hex)	Association Indication
0x00	Successful Completion - Coordinator successfully started or End Device association complete
0x01	Active Scan Timeout
0x02	Active Scan found no PANs
0x03	Active Scan found PAN, but the Coordinator Allow Association bit is not set
0x04	Active Scan found PAN, but Coordinator and End Device are not configured to support beacons
0x05	Active Scan found PAN, but Coordinator ID (PAN ID) value does not match the ID of the End Device
0x06	Active Scan found PAN, but Coordinator CH (Channel) value does not match the CH of the End Device
0x07	Energy Scan Timeout
0x08	Coordinator start request failed
0x09	Coordinator could not start due to Invalid Parameter
0x0A	Coordinator Reassignment in progress
0x0B	Association Request not sent
0x0C	Association Request timed out - no reply was received
0x0D	Association Request Not an Invalid Parameter
0x0E	Association Request Channel Access Failure - Request was not transmitted - CCA failure
0x0F	Remote Coordinator did not send an ACK after Association Request was sent
0x10	Remote Coordinator did not reply to the Association Request, but an ACK was received after sending the request
0x11	Reserved
0x12	Synch-Loss - Lost synchronization with a Discovering Coordinator
0x13	Disassociated - No longer associated to Coordinator

**AP (API Enable) Command**

<Serial Interfacing> The AP command is used to enable the RF module to operate using a frame-based API instead of using the default Transparent (UART) mode.

AT Command: ATAP

Parameter Range: 0 - 2

Parameter	Configuration
0	Disabled (Transparent operation)
1	API enabled
2	API enabled (with escaped characters)

Default Parameter Value: 0

Minimum Firmware Version Required: v1.x80

Refer to the API Operation section when API operation is enabled (AP = 1 or 2).

**AS (Active Scan) Command**

<AT Command Mode Options> The AS command is used to send a Beacon Request to a Broadcast Address (0xFFFF) and Broadcast PAN (0xFFFF) on every channel. The parameter determines the amount of time the RF module will listen for Beacons on each channel. A PanDescriptor is created and returned for every Beacon received from the scan. Each PanDescriptor contains the following information:

AT Command: ATAS

Parameter Range: 0 - 6

Related Command: SD (Scan Duration), DL (Destination Low Address), DH (Destination High Address), ID (PAN ID), CH (Channel)

Minimum Firmware Version Required: v1.x80

CoordAddress (5H + S; parameters) <CR>

CoordPanID (3D parameter) <CR>

CoordAddrMode <CR>

0x02 = 16-bit Short Address

0x03 = 64-bit Long Address

Channel (CH parameter) <CR>

SecurityUse <CR>

ACLEntry <CR>

SecurityFailure <CR>

SuperFrameSpec <CR> (2 bytes)

bit 15 - Association Permitted (HSB)

bit 14 - PAN Coordinator

bit 13 - Reserved

bit 12 - Battery Life Extension

bits 8-11 - Final CAP Slot

bits 4-7 - Superframe Order

bits 0-3 - Beacon Order

IsPerme <CR>

RSSI <CR> ( ; RSSI is returned as -dBm)

TimeStamp <CR> (3 bytes)

<CR> (A carriage return <CR> is sent at the end of the AS command)

The Active Scan is capable of returning up to 5 PanDescriptors in a scan. The actual scan time on each channel is measured as  $\text{Time} = [(2 \wedge (\text{SD Parameter})) * 15.36] \text{ms}$ . Total scan time is this time multiplied by the number of channels to be scanned (16 for the XBee, 12 for the XBee-PRO).

NOTE: Refer the scan table in the SD description to determine scan times. If using API Mode, no <CR>'s are returned in the response. Refer to the API Mode Operation section.

**AV (ADC Voltage Reference) Command**

<Serial Interfacing> The AV command is used to set/read the ADC reference voltage switch. The Xbee-PRO has an ADC voltage reference switch which allows the module to select between an on-board voltage reference or to use the VREF pin on the connector.

This command only applies to Xbee-PRO RF Modules and will return error on an Xbee RF Module.

AT Command: ATAV

Parameter Range: 0 - 1

Parameter	Configuration
0	VREF Pin
1	Internal on-board reference - VCC

Default Parameter Value: 0

Minimum Firmware Version Required: v1.x80

**BD (Interface Data Rate) Command**

<Serial Interfacing> The BD command is used to set and read the serial interface data rate used between the RF module and host. This parameter determines the rate at which serial data is sent to the module from the host. Modified interface data rates do not take effect until the CN (Exit AT Command Mode) command is issued and the system returns the 'OK' response.

When parameters 0-7 are sent to the module, the respective interface data rates are used (as shown in the table on the right).

The RF data rate is not affected by the BD parameter. If the interface data rate is set higher than the RF data rate, a flow control configuration may need to be implemented.

AT Command: ATBD

Parameter Range: 0 - 7 (standard rates)  
0x50-0x1C200 (non-standard rates)

Parameter	Configuration (bps)
0	1200
1	2400
2	4800
3	9600
4	19200
5	38400
6	57600
7	115200

Default Parameter Value: 3

**Non-standard Interface Data Rates:**

Any value above 0x07 will be interpreted as an actual baud rate. When a value above 0x07 is sent, the closest interface data rate represented by the number is stored in the BD register. For example, a rate of 19200 bps can be set by sending the following command line "ATBD4800". NOTE: When using MaxStream's X-CTU Software, non-standard interface data rates can only be set and read using the X-CTU 'Terminal' tab. Non-standard rates are not accessible through the 'Modem Configuration' tab.

When the BD command is sent with a non-standard interface data rate, the UART will adjust to accommodate the requested interface rate. In most cases, the clock resolution will cause the stored BD parameter to vary from the parameter that was sent (refer to the table below). Reading the BD command (send "ATBD" command without an associated parameter value) will return the value actually stored in the module's BD register.

Parameters Sent Versus Parameters Stored

BD Parameter Sent (HEX)	Interface Data Rate (bps)	BD Parameter Stored (HEX)
0	1200	0
4	19,200	4
7	115,200	7
0C	300	0B
1C200	115,200	18007

**CA (CCA Threshold) Command**

<RF Interfacing> CA command is used to set and read CCA (Clear Channel Assessment) thresholds. Prior to transmitting a packet, a CCA is performed to detect energy on the transmit channel. If the detected energy is above the CCA Threshold, the RF module will not transmit the packet.

AT Command: ATCA

Parameter Range: 0 - 0x50 (-dBm)

Default Parameter Value: 0x2C (-44 decimal dBm)

Minimum Firmware Version Required: v1.x80

**CC (Command Sequence Character) Command**

<AT Command Mode Options> The CC command is used to set and read the ASCII character used between guard times of the AT Command Mode Sequence (GT + CC + GT). This sequence enters the RF module into AT Command Mode so that data entering the module from the host is recognized as commands instead of payload.

The AT Command Sequence is explained further in the AT Command Mode section.

AT Command: ATCC  
 Parameter Range: 0 - 0xFF  
 Default Parameter Value: 0x2B (ASCII '+' )  
 Related Command: GT (Guard Times)

**CE (Coordinator Enable) Command**

<Serial Interfacing> The CE command is used to set and read the behavior (End Device vs. Coordinator) of the RF module.

AT Command: ATCE  
 Parameter Range: 0 - 1

Parameter	Configuration
0	End Device
1	Coordinator

Default Parameter Value: 0  
 Minimum Firmware Version Required: v1.x80

**CH (Channel) Command**

<Networking (Addressing) > The CH command is used to set/read the operating channel on which RF connections are made between RF modules. The channel is one of three addressing options available to the module. The other options are the PAN ID (ID command) and destination addresses (DL & DH commands).

In order for modules to communicate with each other, the modules must share the same channel number. Different channels can be used to prevent modules in one network from listening to transmissions of another. Adjacent channel rejection is 23 dB.

The module uses channel numbers of the 802.15.4 standard.  
 Center Frequency = 2.405 + (CH - 110) \* 5 MHz (d = decimal)

AT Command: ATCH  
 Parameter Range: 0x0B - 0x1A (XBee)  
 0x0C - 0x17 (XBee-PRO)  
 Default Parameter Value: 0x0C (12 decimal)  
 Related Commands: ID (PAN ID), DL (Destination Address Low, DH (Destination Address High)

Refer to the XBee/XBee-PRO Addressing section for more information.

**CM (Exit Command Mode) Command**

<AT Command Mode Options> The CM command is used to explicitly exit the RF module from AT Command Mode.

AT Command: ATCM

**CT (Command Mode Timeout) Command**

<AT Command Mode Options> The CT command is used to set and read the amount of inactive time that elapses before the RF module automatically exits from AT Command Mode and returns to Idle Mode.

Use the CM (Exit Command Mode) command to exit AT Command Mode manually.

AT Command: ATCT  
 Parameter Range: 2 - 0xFFFF  
 [x 100 milliseconds]  
 Default Parameter Value: 0x64 (100 decimal (which equals 10 decimal seconds))  
 Number of bytes returned: 2  
 Related Command: CM (Exit Command Mode)

**D0 - D4 (DIO<sub>n</sub> Configuration) Commands**

<I/O Settings> The D0, D1, D2, D3 and D4 commands are used to select/read the behavior of their respective AD/DIO lines (pin 20, 19, 18, 17 and 11 respectively).

Options include:

- Analog-to-digital converter
- Digital input
- Digital output

AT Commands:

ATD0, ATD1, ATD2, ATD3, ATD4

Parameter Range: 0 - 5

Parameter	Configuration
0	Disabled
1	n/a
2	ADC
3	DI
4	DO low
5	DO high

Default Parameter Value: 0

Maximum Firmware Version Required: 1.x.A0

**D5 (DIO5 Configuration) Command**

<I/O Settings> The D5 command is used to select/read the behavior of the DIO5 line (pin 15).

Options include:

- Associated Indicator (LED blinks when the module is associated)
- Analog-to-digital converter
- Digital input
- Digital output

AT Command: ATD5

Parameter Range: 0 - 5

Parameter	Configuration
0	Disabled
1	Associated Indicator
2	ADC
3	DI
4	DO low
5	DO high

Default Parameter Value: 1

Parameters 2-5 supported as of firmware version 1.x.A0

**D6 (DIO6 Configuration) Command**

<I/O Settings> The D6 command is used to select/read the behavior of the DIO6 line (pin 16).

Options include:

- RTS flow control
- Analog-to-digital converter
- Digital input
- Digital output

AT Command: ATD6

Parameter Range: 0 - 5

Parameter	Configuration
0	Disabled
1	RTS Flow Control
2	n/a
3	DI
4	DO low
5	DO high

Default Parameter Value: 0

Parameters 3-5 supported as of firmware version 1.x.A0

**D7 (DIO7 Configuration) Command**

<I/O Settings> The D7 command is used to select/read the behavior of the DIO7 line (pin 12). Options include:

- CTS flow control
- Analog-to-digital converter
- Digital input
- Digital output

AT Command: ATD7

Parameter Range: 0 - 5

Parameter	Configuration
0	Disabled
1	CTS Flow Control
2	n/a
3	DI
4	DO low
5	DO high

Default Parameter Value: 1

Parameters 3-5 supported as of firmware version 1.4A0

**D8 (DIO8 Configuration) Command**

<I/O Settings> The D8 command is used to select/read the behavior of the DIO8 line (pin 9). This command enables configuring the pin to function as a digital input. This line is also used with Pin Sleep.

AT Command: ATD8

Parameter Range: 0 - 3

(1, 2, 4 & 5 n/a)

Parameter	Configuration
0	Disabled
3	DI

Default Parameter Value: 0

Minimum Firmware Version Required: 1.4A0

**DA (Force Disassociation) Command**

<(Special)> The DA command is used to immediately disassociate an End Device from a Coordinator and reattempt to associate.

AT Command: ATDA

Minimum Firmware Version Required: v1.4B0

**DB (Received Signal Strength) Command**

<Diagnostics> DB parameter is used to read the received signal strength (in dBm) of the last RF packet received. Reported values are accurate between -40 dBm and the RF module's receiver sensitivity.

AT Command: ATDB

Parameter Range: 0 - 0x64 (read-only)

Absolute values are reported. For example: 0x5B = -89 dBm (decimal). If no packets have been received (since last reset, power cycle or sleep event), "0" will be reported.

**DH (Destination Address High) Command**

<Networking (Addressing)> The DH command is used to set and read the upper 32 bits of the RF module's 64-bit destination address. When combined with the DL (Destination Address Low) parameter, it defines the destination address used for transmission.

AT Command: ATDH

Parameter Range: 0 - 0xFFFFFFFF

Default Parameter Value: 0

Related Commands: DL (Destination Address Low), CH (Channel), ID (PAN ID), MY (Source Address)

An module will only communicate with other modules having the same channel (CH parameter), PAN ID (ID parameter) and destination address (DH + DL parameters).

To transmit using a 16-bit address, set the DH parameter to zero and the DL parameter less than 0xFFFF. 0x000000000000FFFF (DL concatenated to DH) is the broadcast address for the PAN.

Refer to the XBee/XBee-PRO Addressing section for more information.

**DL (Destination Address Low) Command**

<Networking (Addressing)> The DL command is used to set and read the lower 32 bits of the RF module's 64-bit destination address. When combined with the DH (Destination Address High) parameter, it defines the destination address used for transmission.

A module will only communicate with other modules having the same channel (CH parameter), PAN ID (ID parameter) and destination address [DH + DL parameters].

To transmit using a 16-bit address, set the DH parameter to zero and the DL parameter less than 0xFFFF. 0x00000000000000FFFF (DL concatenated to DH) is the broadcast address for the PAN.

Refer to the XBee/XBee-PRO Addressing section for more information.

AT Command: ATDL

Parameter Range: 0 - 0xFFFFFFFF

Default Parameter Value: 0

Related Commands: DH (Destination Address High), CH (Channel), ID (PAN ID), MY (Source Address)

**DH (Destination Node) Command**

<Networking (Identification)> The DH command is used to resolve a NI (Node Identifier) string to a physical address. The following events occur upon successful command execution:

1. DL and DH are set to the address of the module with the matching NI (Node Identifier).
2. 'OK' is returned.
3. RF module automatically exits AT Command Mode.

If there is no response from a modem within 300 msec or a parameter is not specified (left blank), the command is terminated and an 'ERROR' message is returned.

AT Command: ATDH

Parameter Range: 20-character ASCII String

Minimum Firmware Version Required: v1.x80

**DP (Disassociation Cyclic Sleep Period) Command**

<Sleep Mode (Low Power)>

**NonBeacon Firmware**

End Device - The DP command is used to set and read the time period of sleep for cyclic sleeping remotes that are configured for Association but are not associated to a Coordinator. (i.e. If a device is configured to associate, configured as a Cyclic Sleep remote, but does not find a Coordinator, it will sleep for DP time before reattempting association.) Maximum sleep period is 358 seconds (0x58B0). DP should be > 0 for NonBeacon systems.

AT Command: ATDP

Parameter Range: 1 - 0x58B0  
(x 10 milliseconds)

Default Parameter Value: 0x3E8  
(1000 decimal)

Related Commands: SM (Sleep Mode), SP (Cyclic Sleep Period), ST (Time before Sleep)

Minimum Firmware Version Required: v1.x80

**EA (ACK Failures) Command**

<Diagnostics> The EA command is used to reset and read the count of ACK (acknowledgement) failures. This parameter value increments when the module expects its transmission retries without receiving an ACK on a packet transmission. This count saturates at its maximum value.

Set the parameter to '0' to reset count.

AT Command: ATEA

Parameter Range: 0 - 0xFFFF

Minimum Firmware Version Required: v1.x80

**EC (CCA Failures) Command**

<Diagnostics> The EC command is used to read and reset the count of CCA (Clear Channel Assessment) failures. This parameter value increments when the RF module does not transmit a packet due to the detection of energy that is above the CCA threshold level (set with CA command). This count saturates at its maximum value. Set the EC parameter to "0" to reset count.

AT Command: ATEC  
 Parameter Range: 0 - 0xFFFF  
 Related Command: CA (CCA Threshold)  
 Minimum Firmware Version Required: v1.x80

**ED (Energy Scan) Command**

<Networking (Association)> The ED command is used to send an "Energy Detect Scan". This parameter determines the length of scan on each channel. The maximal energy on each channel is returned and each value is followed by a carriage return. An additional carriage return is sent at the end of the command.

AT Command: ATED  
 Parameter Range: 0 - 6  
 Related Command: SD (Scan Duration), SC (Scan Channel)  
 Minimum Firmware Version Required: v1.x80

The values returned represent the detected energy level in units of -dBm. The actual scan time on each channel is measured as  $Time = [(2 * ED-PARAM) + 15.36] ms$ .

Note: Total scan time is this time multiplied by the number of channels to be scanned. Also refer to the SD (Scan Duration) table. Use the SC (Scan Channel) command to choose which channels to scan.

**EE (AES Encryption Enable) Command**

<Networking (Security)> The EE command is used to set/read the parameter that disables/enables 128-bit AES encryption.

AT Command: ATEE  
 Parameter Range: 0 - 1

Parameter	Configuration
0	Disabled
1	Enabled

The XBee/XBee-PRO firmware uses the 802.15.4 Default Security protocol and uses AES encryption with a 128-bit key. AES encryption dictates that all modules in the network use the same key and the maximum RF packet size is 95 bytes.

Default Parameter Value: 0  
 Related Commands: KY (Encryption Key), AP (API Enable), MM (MAC Mode)  
 Minimum Firmware Version Required: v1.x80

When encryption is enabled, the module will always use its 64-bit long address as the source address for RF packets. This does not affect how the MY (Source Address), DH (Destination Address High) and DL (Destination Address Low) parameters work.

If MH (MAC Mode) > 0 and AP (API Enable) parameter > 0. With encryption enabled and a 16-bit short address set, receiving modules will only be able to issue RX (Receive) 64-bit indicators. This is not an issue when MH = 0.

If a module with a non-matching key detects RF data, but has an incorrect key. When encryption is enabled, non-encrypted RF packets received will be rejected and will not be sent out the UART.

Transparent Operation --> All RF packets are sent encrypted if the key is set.  
 API Operation --> Receive frames use an option bit to indicate that the packet was encrypted.

**FP (Force Poll) Command**

<Networking (Association)> The FP command is used to request indirect messages being held by a Coordinator.

AT Command: ATFP  
 Minimum Firmware Version Required: v1.x80

**FR (Software Reset) Command**

<Special> The FR command is used to force a software reset on the RF module. The reset simulates powering off and then on again the module.

AT Command: ATFR  
 Minimum Firmware Version Required: v1.x80

**GT (Guard Times) Command**

<AT Command Mode Options> GT Command is used to set the GI (data in from host) time-of-silence that surrounds the AT command sequence character (CC Command) of the AT Command Mode sequence (GT + CC + GT).

AT Command: ATGT  
 Parameter Range: 2 - 0x0CE4  
 (x 1 millisecond)  
 Default Parameter Value: 0x1E8  
 (1000 decimal)

The GI time-of-silence is used to prevent inadvertent entrance into AT Command Mode.

Related Command: CC (Command Sequence Character)

Refer to the Command Mode section for more information regarding the AT Command Mode Sequence.

**HV (Hardware Version) Command**

<Diagnostics> The HV command is used to read the hardware version of the RF module.

AT Command: ATHV  
 Parameter Range: 0 - 0xFFFF (Read-only)  
 Minimum Firmware Version Required: v1.x80

**IA (I/O Input Address) Command**

<I/O Settings (I/O Line Passthrough)> The IA command is used to bind a module output to a specific address. Outputs will only change if received from this address. The IA command can be used to set/read both 16 and 64-bit addresses.

AT Command: ATIA  
 Parameter Range: 0 - 0xFFFFFFFFFFFFFFFF  
 Default Parameter Value: 0xFFFFFFFFFFFFFFFF  
 (will not allow any received I/O packet to change outputs)  
 Minimum Firmware Version Required: v1.xA0

Setting all bytes to 0xFF will not allow the reception of any I/O packet to change outputs. Setting the IA address to 0xFFFF will cause the module to accept all I/O packets.

**IC (DIO Change Detect) Command**

<I/O Settings> The IC command is used to enable the monitoring of the change detect feature on DIO lines 0-7. If a change is detected, data is transmitted with DIO data only. Any samples queued and waiting for transmission are sent first.

AT Command: ATIC  
 Parameter Range: 0 - 0xFF (bitfield)  
 Default Parameter Value: 0 (disabled)  
 Minimum Firmware Version Required: 1.xA0

Refer to the "ADC and Digital I/O Line Support" sections of the "RF Module Operations" chapter for more information.

**ID (Pan ID) Command**

<Networking (Addressing)> The ID command is used to set and read the PAN (Personal Area Network) ID of the RF module. Only modules with matching PAN IDs can communicate with each other. Unique PAN IDs enable control of which RF packets are received by a module.

AT Command: ATID  
 Parameter Range: 0 - 0xFFFF  
 Default Parameter Value: 0x3333  
 (13106 decimal)

Setting the ID parameter to 0xFFFF indicates a global transmission for all PANs. It does not indicate a global receive.

**IO (Digital Output Level) Command**

<I/O Settings> The IO command is used to set digital output levels. This allows DIO lines setup as outputs to be changed through Command Mode.

**AT Command: ATIO**

**Parameter Range:** 8-bit bitmap (where each bit represents the level of an I/O line that is setup as an output.)

**Minimum Firmware Version Required:** v1.xAD

**IR (Sample Rate) Command**

<I/O Settings> The IR command is used to set/read the sample rate. When set, the module will sample all enabled DIO/ADC lines at a specified interval. This command allows periodic reads of the ADC and DIO lines in a non-Sleep Mode setup.

**AT Command: ATIR**

**Parameter Range:** 0 – 0xFFFF (x 1 msec) (cannot guarantee 1 ms timing when T=1)

**Default Parameter Value:** 0

**Related Command:** IT (Samples before TX)

**Minimum Firmware Version Required:** v1.xAD

Example: When IR = 0x0A, the sample rate is 10 ms (or 100 Hz).

**IS (Force Sample) Command**

<I/O Settings> The IS-command is used to force a read of all enabled DIO/ADC lines. The data is returned through the UART.

**AT Command: ATIS**

**Parameter Range:** 1 – 0xFF

**Default Parameter Value:** 1

**Minimum Firmware Version Required:** v1.xAD

When operating in Transparent Mode (AP=0), the data is returned in the following format:

All bytes are converted to ASCII  
 number of samples <CR>  
 channel mask <CR>  
 DIO data <CR> (if DIO lines are enabled <CR>  
 ADC channel Data <cr> <-This will repeat for every enabled ADC channel <CR>  
 <CR> (end of data noted by extra <CR>)

When operating in API mode (AP > 0), the command will immediately return an 'OK' response. The data will follow in the normal API format for DIO data.

**IT (Samples before TX) Command**

<I/O Settings> The IT command is used to set/read the number of DIO and ADC samples to collect before transmitting data.

**AT Command: ATIT**

**Parameter Range:** 1 – 0xFF

**Default Parameter Value:** 1

**Minimum Firmware Version Required:** v1.xAD

One ADC sample is considered complete when all enabled ADC channels have been read. The module can buffer up to 92 bytes of sample data.

Since the module uses a 10-bit A/D converter, each sample uses two Bytes. This leads to a maximum buffer size of 46 samples or IT=0x2E.

When Sleep Modes are enabled and IR (Sample Rate) is set, the module will remain awake until IT samples have been collected.

**IU (I/O Output Enable) Command**

<I/O Settings> The IU command is used to disable/enable I/O UART output. When enabled (IU = 1), received I/O line data packets are sent out the UART. The data is sent using an API frame regardless of the current AP parameter value.

AT Command: ATIU

Parameter Range: 0 - 1

Parameter	Configuration
0	Disabled - Received I/O line data packets will NOT sent out UART.
1	Enabled - Received I/O line data will be sent out UART.

Default Parameter Value: 1

Minimum Firmware Version Required: v1.xA0

**KY (AES Encryption Key) Command**

<Networking (Security)> The KY command is used to set the 128-bit AES (Advanced Encryption Standard) key for encrypting/decrypting data. Once set, the key cannot be read out of the module by any means.

AT Command: ATKY

Parameter Range: 0 - (any 16-Byte value)

Default Parameter Value: 0

Related Command: IE (Encryption Enable)

Minimum Firmware Version Required: v1.xA0

The entire payload of the packet is encrypted using the key and the CRC is computed across the ciphertext. When encryption is enabled, each packet carries an additional 16 Bytes to convey the random CBC Initialization Vector (IV) to the receiver(s). The KY value may be "0" or any 128-bit value. Any other value, including entering ATKY by itself with no parameters, will cause an error. A module with the wrong key (or no key) will receive encrypted data, but the data driven out the serial port will be meaningless. Likewise, a module with a key will receive unencrypted data sent from a module without a key, but the output will be meaningless. Because CBC mode is utilized, repetitive data appears differently in different transmissions due to the randomly-generated IV.

When queried, the system will return an "Ok" message and the value of the key will not be returned.

**M0 (PWM0 Output Level) Command**

<I/O Settings> The M0 command is used to set/read the output level of the PWM0 line (pin 6).

AT Command: ATM0

Parameter Range: 0 - 0x03FF (steps)

Default Parameter Value: 0

Related Commands: PE (PWM0 Enable), AC (Apply Changes), CN (Exit Command Mode)

Minimum Firmware Version Required: v1.xA0

Before setting the line as an output:

1. Enable PWM0 output (PE = 2)
2. Apply settings (use CN or AC)

The PWM period is 64  $\mu$ sec and there are 0x03FF (1023 decimal) steps within this period. When M0 = 0 (0% PWM), 0x01FF (50% PWM), 0x03FF (100% PWM), etc.

**M1 (PWM1 Output Level) Command**

<I/O Settings> The M1 command is used to set/read the output level of the PWM1 line (pin 7).

AT Command: ATM1

Parameter Range: 0 - 0x03FF

Default Parameter Value: 0

Related Commands: PE (PWM1 Enable), AC (Apply Changes), CN (Exit Command Mode)

Minimum Firmware Version Required: v1.xA0

Before setting the line as an output:

1. Enable PWM1 output (PE = 2)
2. Apply settings (use CN or AC)

**MH (MAC Mode) Command**

<Networking (Addressing)> The MH command is used to set and read the MAC Mode value. The MH command disables/enables the use of a MaxStream header contained in the 802.15.4 RF packet. By default (MH = 0), MaxStream Mode is enabled and the module adds an extra header to the data portion of the 802.15.4 packet. This enables the following features:

- ND and DN command support
- Duplicate packet detection when using ACKs.

The MH command allows users to turn off the use of the extra header. Modes 1 and 2 are strict 802.15.4 modes. If the MaxStream header is disabled, ND and DN parameters are also disabled.

Note: When MH > 0, application and CCA failure retries are not supported.

AT Command: ATMM

Parameter Range: 0 - 2

Parameter	Configuration
0	MaxStream Mode (802.15.4 + MaxStream header)
1	802.15.4 (no ACKs)
2	802.15.4 (with ACKs)

Default Parameter Value: 0

Related Commands: ND (Node Discover), DN (Destination Node)

Minimum Firmware Version Required: v1.x80

**MY (16-bit Source Address) Command**

<Networking (Addressing)> The MY command is used to set and read the 16-bit source address of the RF module.

By setting MY to 0xFFFF, the reception of RF packets having a 16-bit address is disabled. The 64-bit address is the module's serial number and is always enabled.

AT Command: ATMY

Parameter Range: 0 - 0xFFFF

Default Parameter Value: 0

Related Commands: DH (Destination Address High), DL (Destination Address Low), CH (Channel), ID (PAN ID)

**ND (Node Discover) Command**

<Networking (Identification)> The ND command is used to discover and report all modules on its current operating channel (CH parameter) and PAN ID (ID parameter). ND also accepts an NI (Node Identifier) value as a parameter. In this case, only a module matching the supplied identifier will respond.

ND uses a 64-bit long address when sending and responding to an ND request. The ND command causes a module to transmit a globally addressed ND command packet. The amount of time allowed for responses is determined by the NT (Node Discover Time) parameter.

In AT Command mode, command completion is designated by a carriage return (0x0D). Since two carriage returns end a command response, the application will receive three carriage returns at the end of the command. If no responses are received, the application should only receive one carriage return. When in API mode, the application should receive a frame (with no data) and status (set to 'OK') at the end of the command. When the ND command packet is received, the remote sets up a random time delay (up to 2.2 sec) before replying as follows:

Node Discover Response (AT command mode format - transparent operation):

- MY (Source Address) value<CR>
- SH (Serial Number High) value<CR>
- SL (Serial Number Low) value<CR>
- DB (Received Signal Strength) value<CR>
- NI (Node Identifier) value<CR>
- <CR> (This is part of the response and not the end of command indicator)

Node Discover Response (API format - data is binary (except for NI)):

- 2 bytes for MY (Source Address) value
- 4 bytes for SH (Serial Number High) value
- 4 bytes for SL (Serial Number Low) value
- 1 byte for DB (Received Signal Strength) value
- NULL-terminated string for NI (Node Identifier) value (max 20 bytes w/out NULL terminator)

**NI (Node Identifier) Command**

<Networking (Identification)> The NI command is used to set and read a string for identifying a particular node.

Rules:

- Register only accepts printable ASCII data.
- A string can not start with a space.
- A carriage return ends command.
- Command will automatically end when maximum bytes for the string have been entered.

This string is returned as part of the ND (Node Discover) command. This identifier is also used with the DN (Destination Node) command.

AT Command: ATNI

Parameter Range: 20-character ASCII string

Related Commands: ND (Node Discover), DN (Destination Node)

Minimum Firmware Version Required: v1.xA0

**NT (Node Discover Time) Command**

<Networking (Identification)> The NT command is used to set the amount of time a base node will wait for responses from other nodes when using the ND (Node Discover) command. The NT value is transmitted with the ND command.

Remote nodes will set up a random hold-off time based on this time. The remotes will adjust this time down by 250 ms to give each node the ability to respond before the base ends the command. response received on the base would be discarded.

AT Command: ATNT

Parameter Range: 0x01 - 0xFC  
(x 100 msec)

Default: 0x19 (2.5 decimal seconds)

Related Commands: ND (Node Discover)

Minimum Firmware Version Required: 1.xA0

Once the ND command has ended, any

**P0 (PWM0 Configuration) Command**

<I/O Setting (I/O Line Passing)> The P0 command is used to select/read the function for PWM0 (Pulse Width Modulation output 0). This command enables the option of translating incoming data to a PWM so that the output can be translated back into analog form.

With the IA (I/O Input Address) parameter correctly set, AD0 values can automatically be passed to PWM0.

AT Command: ATP0

The second character in the command is the number zero ('0'), not the letter 'O'.

Parameter Range: 0 - 2

Parameter	Configuration
0	Disabled
1	RSSI
2	PWM0 Output

Default Parameter Value: 1

**P1 (PWM1 Configuration) Command**

<I/O Setting (I/O Line Passing)> The P1 command is used to select/read the function for PWM1 (Pulse Width Modulation output 1). This command enables the option of translating incoming data to a PWM so that the output can be translated back into analog form.

With the IA (I/O Input Address) parameter correctly set, AD1 values can automatically be passed to PWM1.

AT Command: ATP1

Parameter Range: 0 - 2

Parameter	Configuration
0	Disabled
1	RSSI
2	PWM1 Output

Default Parameter Value: 0

Minimum Firmware Version Required: v1.xA0

**PL (Power Level) Command**

<RF Interfacing> The PL command is used to select and read the power level at which the RF module transmits conducted power.

**WHEN OPERATING IN EUROPE:**

XBee-PRO RF Modules must be configured to operate at a maximum transmit power output level of 10 dBm. The PL parameter must equal "0" (10 dBm).

Additionally, European regulations stipulate an EIRP power maximum of 12.86 dBm (19 mW) for the XBee-PRO and 12.11 dBm for the XBee when integrating high-gain antennas.

**WHEN OPERATING IN JAPAN:**

XBee-PRO RF Modules optimized for use in Japan contain firmware that limits transmit power output to 10 dBm. If PL=4 (default), the maximum power output level is 10 dBm. For a list of module part numbers approved for use in Japan, contact MaxStream (call 1-801-765-9665 or send e-mail to sales@maxstream.net).

AT Command: ATPL

Parameter Range: 0 - 4

Parameter	XBee	XBee-PRO
0	-10 dBm	10 dBm
1	-6 dBm	12 dBm
2	-4 dBm	14 dBm
3	-2 dBm	16 dBm
4	0 dBm	18 dBm

Default Parameter Value: 4

**PR (Pull-up Resistor Enable) Command**

<Serial Interfacing> The PR command is used to set and read the bit field that is used to configure internal the pull-up resistor status for I/O lines. "1" specifies the pull-up resistor is enabled, "0" specifies no pull up.

- bit 0 - AD4/DIO4 (pin 11)
- bit 1 - AD3/DIO3 (pin 17)
- bit 2 - AD2/DIO2 (pin 18)
- bit 3 - AD1/DIO1 (pin 19)
- bit 4 - AD0/DIO0 (pin 20)
- bit 5 - AD6/DIO6 (pin 16)
- bit 6 - DSS (pin 9)
- bit 7 - DIN/CONFIG (pin 3)

For example: Sending the command "ATPR 6F" will turn bits 0, 1, 2, 3, 5 and 6 ON; and bits 4 & 7 will be turned OFF. (The binary equivalent of "0x6F" is "01101111". Note that "bit 0" is the last digit in the hexfield.

AT Command: ATPR

Parameter Range: 0 - 0xFF

Default Parameter Value: 0xFF  
(all pull-up resistors are enabled)

Minimum Firmware Version Required: v1.x80

**PT (PWM Output Timeout) Command**

<I/O Settings (I/O Line Passing)> The PT command is used to set/read the output timeout value for both PWM outputs.

When PWM is set to a non-zero value: Due to I/O line passing, a time is started which when expired will set the PWM output to zero. The timer is reset when a valid I/O packet is received.

AT Command: ATPT

Parameter Range: 0 - 0xFF (x 100 msec)

Default Parameter Value: 0xFF

Minimum Firmware Version Required: 1.x80

**RE (Restore Defaults) Command**

<(Special)> The RE command is used to restore all configurable parameters to their factory default settings. The RE command does not write restored values to non-volatile (persistent) memory. Issue the WR (Write) command subsequent to issuing the RE command to save restored parameter values to non-volatile memory.

AT Command: ATRE

**RN (Random Delay Slots) Command**

<Networking & Security> The RN command is used to set and read the minimum value of the back-off exponent in the CSMA-CA algorithm. The CSMA-CA algorithm was engineered for collision avoidance (random delays are inserted to prevent data loss caused by data collisions).

AT Command: `ATRN`

Parameter Range: 0 - 3 [exponent]

Default Parameter Value: 0

If RN = 0, collision avoidance is disabled during the first iteration of the algorithm (802.15.4 - macMHR).

CSMA-CA stands for "Carrier Sense Multiple Access - Collision Avoidance". Unlike CSMA-CD (reacts to network transmissions after collisions have been detected), CSMA-CA acts to prevent data collisions before they occur. As soon as a module receives a packet that is to be transmitted, it checks if the channel is clear (no other module is transmitting). If the channel is clear, the packet is sent over-the-air. If the channel is not clear, the module waits for a randomly selected period of time, then checks again to see if the channel is clear. After a time, the process ends and the data is lost.

**RO (Packetization Timeout) Command**

<Serial Interfacing> RO command is used to set and read the number of character times of inter-character delay required before transmission.

AT Command: `ATRO`

Parameter Range: 0 - 0xFF  
[x character times]

Default Parameter Value: 1

RF transmission commences when data is detected in the DI (data in from host) buffer and RO character times of silence are detected on the UART receive lines (after receiving at least 1 byte).

RF transmission will also commence after 100 Bytes (maximum packet size) are received in the DI buffer.

Set the RO parameter to '0' to transmit characters as they arrive instead of buffering them into one RF packet.

**RP (RSSI PWM Timer) Command**

<I/O Settings (I/O Line Pasring)> The RP command is used to enable PWM (Pulse Width Modulation) output on the RF module. The output is calibrated to show the level a received RF signal is above the sensitivity level of the module. The PWM pulses vary from 24 to 100%. Zero percent means PWM output is inactive. One to 24% percent means the received RF signal is at or below the published sensitivity level of the module. The following table shows levels above sensitivity and PWM values.

AT Command: `ATRP`

Parameter Range: 0 - 0xFF  
[x 100 msec]

Default Parameter Value: 0x28 (40 decimal)

The total period of the PWM output is 64  $\mu$ s. Because there are 445 steps in the PWM output, the minimum step size is 144 ns.

**PWM Messages**

dB above Sensitivity	PWM percentage (high period / total period)
10	41%
20	33%
30	25%

A non-zero value defines the time that the PWM output will be active with the RSSI value of the last received RF packet. After the set time when no RF packets are received, the PWM output will be set low (0 percent PWM) until another RF packet is received. The PWM output will also be set low at power-up until the first RF packet is received. A parameter value of 0xFF permanently enables the PWM output and it will always reflect the value of the last received RF packet.

**RR (Xbee Retries) Command**

<Networking (Addressing)> The RR command is used set/read the maximum number of retries the module will execute in addition to the 3 retries provided by the 802.15.4 MAC. For each Xbee retry, the 802.15.4 MAC can execute up to 3 retries.

This values does not need to be set on all modules for retries to work. If retries are enabled, the transmitting module will set a bit in the Maxstream RF Packet header which requests the receiving module to send an ACK (acknowledgement). If the transmitting module does not receive an ACK within 200 msec, it will re-send the packet within a random period up to 40 msec. Each Xbee retry can potentially result in the MAC sending the packet 4 times (1 try plus 3 retries). Note that retries are not attempted for packets that are purged when transmitting with a Cyclic Sleep Coordinator.

AT Command: ATRR

Parameter Range: 0 - 9

Default: 0

Minimum Firmware Version Required: 1.x40

**SC (Scan Channels) Command**

<Networking (Association)> The SC command is used to set and read the list of channels to scan for as Active and Energy Scans as a bit field.

This effects scans initiated in command mode (AS (Active Scan) and ED (Energy Scan) commands) and during End Device Association and Coordinator startup.

AT Command: ATSC

Parameter Range: 0 - 0xFFFF (Bitfield)  
(bits 0, 14, 15 are not allowed when using the Xbee-PRO)

Default Parameter Value: 0x1FFE (all Xbee-PRO channels)

Related Commands: ED (Energy Scan), SD (Scan Duration)

Minimum Firmware Version Required: v1.x80

bit 0 - 0x08	bit 4 - 0x0F	bit 8 - 0x13	bit 12 - 0x17
bit 1 - 0x0C	bit 5 - 0x10	bit 9 - 0x14	bit 13 - 0x18
bit 2 - 0x0D	bit 6 - 0x11	bit 10 - 0x15	bit 14 - 0x19
bit 3 - 0x0E	bit 7 - 0x12	bit 11 - 0x16	bit 15 - 0x1A

**SD (Scan Duration) Command**

<Networking (Association)> The SD command is used to set and read the exponent value that determines the duration (in time) of a scan.

**End Device** (Duration of Active Scan during Association) - In a Beacon system, set SD = bit of the Coordinator. SD must be set at least to the highest BE parameter of any Beaconsing Coordinator with which an End Device or Coordinator wish to discover.

**Coordinator** - If the 'ReassignPANID' option is set on the Coordinator (refer to A2 parameter), the SD parameter determines the length of time the Coordinator will scan channels to locate existing PANs. If the 'ReassignChannel' option is set, SD determines how long the Coordinator will perform an Energy Scan to determine which channel it will operate on.

Scan Time is measured as ((# of Channels to Scan) \* (2 - SD) \* 15.36ms). The number of channels to scan is set by the SC command. The Xbee RF Module can scan up to 16 channels (SC = 0xFFFF). The Xbee PRO RF Module can scan up to 12 channels (SC = 0x1FFE).

Examples Values below show results for a 12-channel scan.

SD = 0, time = 0.18 sec	SD = 8, time = 47.19 sec
SD = 1, time = 0.74 sec	SD = 9, time = 3.19 min
SD = 2, time = 2.95 sec	SD = 10, time = 12.58 min
SD = 3, time = 11.80 sec	SD = 11, time = 50.33 min

**SH (Serial Number High) Command**

<Diagnostics> The SH command is used to read the high 32 bits of the RF module's unique IEEE 64-bit address.

The module serial number is set at the factory and is read-only.

AT Command: ATSH

Parameter Range: 0 - 0xFFFFFFFF (read-only)

Related Commands: SL (Serial Number Low), MY (Source Address)

**SL (Serial Number Low) Command**

<Diagnostics> The SL command is used to read the low 32 bits of the RF module's unique IEEE 64-bit address.

The module serial number is set at the factory and is read-only.

AT Command: ATSL

Parameter Range: 0 - 0xFFFFFFFF (read-only)

Related Commands: SH (Serial Number High), MY (Source Address)

**SM (Sleep Mode) Command**

<Sleep Mode (Low Power)> The SM command is used to set and read Sleep Mode settings. By default, Sleep Modes are disabled (SM = 0) and the RF module remains in Idle/Receive Mode. When in this state, the module is constantly ready to respond to either serial or RF activity.

SM command options vary according to the networking system type. By default, the module is configured to operate in a Nonbeacon system.

\* The Sleep Coordinator option (SM=6) only exists for backwards compatibility with firmware version 1.x08 only. In all other cases, use the CE command to enable a Coordinator.

AT Command: ATSM

Parameter Range: 0 - 6

Parameter	Configuration
0	Disabled
1	Pin Hibernation
2	Pin Doze
3	(reserved)
4	Cyclic Sleep Remote
5	Cyclic Sleep Remote with Pin Wake-up
6	Sleep Coordinator*

Default Parameter Value: 0

Related Commands: SP (Cyclic Sleep Period), ST (Time before Sleep)

**SP (Cyclic Sleep Period) Command**

<Sleep Mode (Low Power)> The SP command is used to set and read the duration of time in which a remote RF module sleeps. After the cyclic sleep period is over, the module wakes and checks for data. If data is not present, the module goes back to sleep. The maximum sleep period is 268 seconds (SP = 0x6880).

The SP parameter is only valid if the module is configured to operate in Cyclic Sleep (SM = 4-6), Coordinator and End Device SP values should always be equal.

To send Direct Messages, set SP = 0.

**Nonbeacon Firmware**

**End Device** - SP determines the sleep period for cyclic sleeping remotes. Maximum sleep period is 268 seconds (0x6880).

**Coordinator** - if non-zero, SP determines the time to hold an indirect message before discarding it. A Coordinator will discard indirect messages after a period of (2.5 \* SP).

AT Command: ATSP

Parameter Range: NonBeacon Firmware: 1 - 0x6880 (a 10 milliseconds)

Default Parameter Value: NonBeacon Firmware: 0

Related Commands: SM (Sleep Mode), ST (Time before Sleep), DP (Disassociation Cyclic Sleep Period), BE (Beacon Order)

**ST (Time before Sleep) Command**

<Sleep Mode (Low Power)> The ST command is used to set and read the period of inactivity (no serial or RF data is sent or received) before activating Sleep Mode.

**NonBeacon Firmware**

Set/read time period of inactivity (no serial or RF data is sent or received) before activating Sleep Mode. ST parameter is only valid with Cyclic Sleep settings (SH = 4 - 5).

Coordinator and End Device ST values must be equal.

AT Command: ATST

Parameter Range	NonBeacon Firmware: 1 - 0xFFFF (x 1 millisecond)
Default Parameter Value	NonBeacon Firmware: 0x1388 (5000 decimal)
Related Commands: SM (Sleep Mode), ST (Time before Sleep)	

**T0 - T7 ((D0-D7) Output Timeout) Command**

<I/O Settings (I/O Line Passing)> The T0, T1, T2, T3, T4, T5, T6 and T7 commands are used to set/read output timeout values for the lines that correspond with the D0 - D7 parameters. When output is set (due to I/O line passing) to a non-default level, a timer is started which when expired, will set the output to its default level. The timer is reset when a valid I/O packet is received. The Tn parameter defines the permissible amount of time to stay in a non-default (active) state. If Tn = 0, Output Timeout is disabled (output levels are held indefinitely).

AT Commands: ATTO - ATTY

Parameter Range	0 - 0xFF (x 100 msec)
Default Parameter Value	0xFF
Minimum Firmware Version Required: v1.x80	

**VL (Firmware Version - Verbose)**

<Diagnostics> The VL command is used to read detailed version information about the RF module. The information includes: application build date; MAC, PHY and bootloader versions; and build dates.

AT Command: ATVL

Parameter Range	0 - 0xFF (x 100 milliseconds)
Default Parameter Value	0x28 (40 decimal)
Minimum Firmware Version Required: v1.x80	

**VR (Firmware Version) Command**

<Diagnostics> The VR command is used to read which firmware version is stored in the module.

XBee version numbers will have four significant digits. The reported number will show three or four numbers and is stated in hexadecimal notation. A version can be reported as "ABC" or "ABCD". Digits ABC are the main release number and D is the revision number from the main release. "D" is not required and if it is not present, a zero is assumed for D. "B" is a variant designator. The following variants exist:

- "0" = Non-Beacon Enabled 802.15.4 Code
- "1" = Beacon Enabled 802.15.4 Code

AT Command: ATVR

Parameter Range: 0 - 0xFFFF (read only)

**WR (Write) Command**

<(Special)> The WR command is used to write configurable parameters to the RF module's non-volatile memory. Parameter values remain in the module's memory until overwritten by subsequent use of the WR Command.

AT Command: ATWR

If changes are made without writing them to non-volatile memory, the module reverts back to previously saved parameters the next time the module is powered-on.

NOTE: Once the WR command is sent to the module, no additional characters should be sent until after the "OK/r" response is received.