Instituto Tecnológico de Costa Rica

Escuela de Ingeniería en Electrónica

Sistema de seguridad en los bastidores de comunicación de la plataforma tecnológica del Sistema Interbancario de Negociación y Pagos Electrónicos del Banco Central de Costa Rica

Informe de Proyecto de Graduación para optar por el título de Ingeniero en Electrónica con el grado académico de Licenciatura

Juan Manuel Fonseca Carvajal

Cartago, Junio de 2006

INSTITUTO TECNOLOGICO DE COSTA RICA

ESCUELA DE INGENIERIA ELECTRONICA

PROYECTO DE GRADUACIÓN

TRIBUNAL EVALUADOR

Proyecto de Graduación defendido ante el presente Tribunal Evaluador como requisito para optar por el título de Ingeniero en Electrónica con el grado académico de Licenciatura, del Instituto Tecnológico de Costa Rica.

Miembros del Tribunal

Ing. Eduardo Interiano Salguero

Profesor lector

Ing. Aníbal Coto Cortés

Profesor lector

TEC
Instituto Tecnológico de Costa Rica
Escuela de Ingeniería Electrónica

Ing. William Marín Moreno

Profesor asesor

Los miembros de este Tribunal dan fe de que el presente trabajo de graduación ha sido aprobado y cumple con las normas establecidas por la Escuela de Ingeniería Electrónica

Cartago, Junio de 2006

Declaro que el presente Proyecto de Graduación ha sido realizado enteramente por mi persona, utilizando y aplicando literatura referente al tema e introduciendo conocimientos propios.

En los casos en que he utilizado bibliografía, he procedido a indicar las fuentes mediante las respectivas citas bibliográficas.

En consecuencia, asumo la responsabilidad total por el trabajo de graduación realizado y por el contenido del correspondiente informe final.

San José, 20 de junio del 2006

Juan Manuel Fonseca Carvajal

Cédula: *1-1133- 0593*

Resumen

El Banco Central de Costa Rica (BCCR) por medio de la plataforma tecnológica del Sistema Interbancario de Negociación y Pagos Electrónicos (SINPE) provee a las entidades financieras del país un mecanismo eficiente para realizar los trámites entre cada una de ellas donde el sistema central de acceso y comunicación se ubica en el BCCR. El BCCR tiene instalado en cada institución financiera un bastidor de comunicaciones. El BCCR requiere que se controle su acceso y su condición ambiental en cuanto a temperatura y flujo de aire, para notificar al BCCR sobre el acceso de personal no autorizado a los bastidores de comunicación localizados en las entidades financieras.

Para el control requerido se ha propuesto un sistema de seguridad cuyos eventos de apertura de puertas, superación de los límites del rango de temperatura e insuficiencia de aire son enviados a un sitio central por medio de un dispositivo instalado en cada bastidor. Este dispositivo es un sistema embebido que envía notificaciones a la estación de administración de red localizado en el BCCR usando mensajes de SNMP. Estos mensajes son enviados a través de la red privada de SINPE, pero también pueden ser enviados por la Internet.

Palabras Claves: SNMP, Notificación SNMP, Sistema Embebido, Microcontrolador, `Ethernet`

Abstract

SINPE (Inter-bank System of Negotiation and Electronic Payments) is a technological platform that belongs to the Costa Rican Central Bank (BCCR). This system provides to the financial organizations of Costa Rica an efficient mechanism of financial proceedings between each of them. The main access and communications system is located in the headquarters of the BCCR. BCCR has installed a networking rack on each financial organization. BCCR require that its access and its environmental condition (in matter of temperature and air flow) to be

controlled, in order to inform BCCR about unauthorized personal access on the racks located on each financial organization.

A security system have been proposed for the required control whose events as doors opening, temperature range exceeded and loss of air flow; are send to a main site by a device installed on each rack. This device is an embedded system that sends messages to a network management system located in BCCR using SNMP traps. These messages are sending through the private network of SINPE, but also it can be send through the Internet.

Keywords: SNMP, SNMP Trap, Embedded System, Microcontroller, Ethernet

ÍNDICE GENERAL

Capítulo 1:	Introducción	13
1.1	Problema existente e importancia de su solución	13
1.2	Solución seleccionada	14
Capítulo 2:	Meta y Objetivos	19
2.1	Meta	19
2.2	Objetivo general	19
2.3	Objetivos específicos	19
Capítulo 3:	Marco teórico	20
3.1	Descripción del sistema	20
3.2	Antecedentes bibliográficos	21
3.3	Sistemas embebidos	21
3.4	Conjunto de protocolos TCP/IP	21
3.5	SNMP	25
Capítulo 4:	Procedimiento metodológico	28
4.1	Reconocimiento y definición del problema	28
4.2	Obtención y análisis de información	28
4.3	Evaluación de las alternativas y síntesis de una solución	28
4.4	Implementación de la solución	29
4.5	Reevaluación y rediseño	29
Capítulo 5:	Descripción detallada de la solución	30
5.1	Análisis de soluciones y selección final	30
5.2	Descripción del hardware	31
5.3	Descripción del firmware	38

Capítulo 6: Análisis de Resultados 52
6.1 Configuración inicial del sistema 54
6.2 Notificaciones de SNMP 57
6.3 Página WEB 60
6.4 Módulo ARP & ICMP 71
6.5 Mediciones del consumo de ancho de banda 72
Capítulo 7: Conclusiones y recomendaciones 75
7.1 Conclusiones 75
7.2 Recomendaciones 75
Bibliografía 76
Apéndices 78
A.1 Glosario, abreviaturas y simbología 78
A.2 Información sobre GGT Solutions 80
A.3 Antecedentes prácticos 81
Anexos 82
B.1 Diagrama esquemático de la tarjeta SBC65EC 82
B.2 Diagrama esquemático del chasis IOR5E 85

ÍNDICE DE FIGURAS

Figura 1.1 Sistema requerido para el sistema de seguridad 16

Figura 1.2 Vista de la tarjeta SBC65EC de Modtronix 17

Figura 1.3 Características de la tarjeta SBC65EC de Modtronix 17

Figura 3.1 Panorama de funcionamiento del sistema de seguridad 20

Figura 3.2 Modelo de SNMP y terminología asociada 25

Figura 3.3 Estructura genérica de un SMI 26

Figura 3.4 Ejemplo de una estructura de información del subárbol parcial de Internet 27

Figura 5.1 Vista del chasis IOR5E de Modtronix para la tarjeta SBC65EC 31

Figura 5.2 Diagrama de bloques del hardware del sistema de seguridad 32

Figura 5.3 Contacto magnético amseco® AMS-10 para puertas 33

Figura 5.4 Circuito para la conexión de cada contacto magnético para puertas 33

Figura 5.5 Circuito para la conexión del sensor de temperatura 34

Figura 5.6 Contacto magnético Stego Inc LC 013 para detectar presencia de flujo de aire 35

Figura 5.7 Circuito para la conexión del sensor de presencia de flujo de aire 35

Figura 5.8 Zumbador magnético empleado como mini sirena 36

Figura 5.9 Circuito para la conexión del zumbador para la mini sirena 36

Figura 5.10 Diagrama de bloques de los módulos principales del sistema de seguridad 38

Figura 5.11 Diagrama de flujo de la inicialización de la aplicación principal 40

Figura 5.12 Diagrama de flujo del ciclo infinito de la aplicación principal 41

Figura 5.13 Menú de configuración del sistema del módulo Terminal 41

Figura 5.14 Diagrama de flujo del proceso de temperatura en el módulo de “Tareas específicas” 43

Figura 5.15 Página WEB de inicio del sistema 45

Figura 5.16 Diagrama de flujo de la construcción de un paquete de notificación de SNMP (I) 48

Figura 5.17 Diagrama de flujo de la construcción de un paquete de notificación de SNMP (II) 49

Figura 5.18 Estructura de la información de administración implementada en el sistema 50

Figura 6.1 Fotografía del sistema de seguridad desarrollado (I) 52

Figura 6.2 Fotografía del sistema de seguridad desarrollado (II) 53

Figura 6.3 Topología de red implementada para la demostración de los resultados 53

Figura 6.4 Mensaje de consola mostrado al instante de restaurar el sistema 55

Figura 6.5 Menú de Terminal del sistema 55

Figura 6.6 Cambios de configuración por consola 56

Figura 6.7 Registro de notificaciones SNMP en la estación de administración de red 58

Figura 6.8 Notificación de SNMP capturada con el analizador de protocolos: Ethereal 59

Figura 6.9 Notificación de SNMP extraída de la aplicación WhatsUp Gold 59

Figura 6.10 Notificación de SNMP capturada con el analizador de protocolos: Ethereal 60

Figura 6.11 Página WEB de inicio 61

Figura 6.12 Página WEB de registro 61

Figura 6.13 Marco interno de la página WEB de soporte 62

Figura 6.14 Marco interno de la página WEB de registro, cuando un usuario se ha registrado 62

Figura 6.15 Marco interno de la página WEB de cambio de usuario y contraseña 63

Figura 6.16 Marco interno de la página WEB de temperatura 63

Figura 6.17 Marco interno de la página WEB de estado de las puertas y flujo de aire 64

Figura 6.18 Marco interno de la página WEB de puertos de salida 65

Figura 6.19 Demostración de los relevadores 2 y 4 encendidos con los LED del chasis IOR5E 65

Figura 6.20 Marco interno de la página WEB de configuración del sistema 67

Figura 6.21 Marco interno de la página WEB de configuración de red y de SNMP 68

Figura 6.22 Marco interno de la página WEB de configuración del puerto serie 68

Figura 6.23 Capturas con Ethereal de la conversación de HTTP para la consulta de la página de temperatura (I) 69

Figura 6.24 Capturas con Ethereal de la conversación de HTTP para la consulta de la página de temperatura (II) 70

Figura 6.25 Captura con Ethereal de una solicitud de ARP 71

Figura 6.26 Captura con Ethereal de una respuesta de ARP 71

Figura 6.27 Muestra del resultado de un ping hacia el sistema 72

Figura 6.28 Captura con Ethereal de una solicitud de ICMP 72

Figura 6.29 Captura con Ethereal de una respuesta de ICMP 72

Figura 6.30 Consumo de ancho de banda cuando se consulta las páginas WEB del sistema 73

Figura 6.31 Consumo de ancho de banda cuando envían paquetes de ICMP y SNMP 74

Figura B.1 Plano de la placa de circuito impreso de la tarjeta SBC65EC 82

Figura B.2 Plano de la placa de circuito impreso del chasis IOR5E 85

ÍNDICE DE TABLAS

Tabla 5.1 Sistemas embebidos consultados para selección de uno para el proyecto 30

Tabla 5.2 Descripción de los archivos que conforman la página WEB 44

Tabla 5.3 Descripción de los comandos de CGI utilizados en el proyecto 46

Tabla 5.4 Mensajes de las notificaciones de SNMP que envía el sistema 47

Tabla 6.1 Parámetros de red y de SNMP asignados por defecto 54

Tabla 6.2 Parámetros del puerto serie para configurar por consola el sistema 54

Capítulo 1: Introducción

Esta sección presenta el problema existente, así como la importancia de su solución. Además, se introduce en breve cuál fue y cómo se llevó a cabo la solución seleccionada.

1.1 Problema existente e importancia de su solución

El Banco Central de Costa Rica (BCCR) es el ente del Estado Costarricense encargado de velar por el buen funcionamiento del Sistema Financiero Nacional. Esta entidad ha integrado de forma eficiente a las entidades financieras (tanto privadas como estatales) del país, por medio de un proyecto llamado Sistema Interbancario de Negociación y Pagos Electrónicos (SINPE). El SINPE es una plataforma tecnológica que provee a las entidades financieras del país un mecanismo eficiente para realizar los trámites entre cada una de ellas donde el sistema central de acceso y comunicación se ubica en el BCCR.

El BCCR tiene instalado en cada institución financiera un bastidor de comunicaciones. En este se almacenan equipos de comunicación como enrutadores, conmutadores de red, entre otros; donde se establecen los enlaces de red de banda ancha al BCCR y los enlaces de red de área local hacia la red interna de la institución financiera.

Actualmente estos bastidores se encuentran asegurados por cerraduras debido a que sólo personal autorizado del BCCR debe tener acceso. Aún así existe la eventualidad de que alguna persona no autorizada pueda forzar el acceso. Además, estos bastidores se encuentran bajo las condiciones de temperatura y flujo de aire del cuarto de comunicaciones. En el caso de que el cuarto tenga una condición cálida, la operación de los equipos de comunicación dentro del bastidor no sería la deseada.

Por lo tanto, si se controlara el acceso a los bastidores, el BCCR se aseguraría que los equipos de comunicación no sean manipulados por personas no autorizadas. Además, si se asegurara que las condiciones ambientales de operación

de los equipos de comunicación sean las esperadas, estos equipos tendrían mayor eficiencia y duración.

1.2 Solución seleccionada

Antes de introducir cuál fue la solución implementada, se detalla cuáles fueron los requisitos del proyecto.

1.2.1 Requisitos

Este proyecto surge debido a una necesidad del Banco Central de Costa Rica como ya se mencionó anteriormente. Para ello, el BCCR invitó a empresas para que participaran en una licitación restringida. La licitación restringida 20053-155 [1]: “Adquisición de Hardware”, en cuanto al renglón No. 2: “Un sistema para control de bastidores”; fue adjudicada a GGT Solutions.

GGT Solutions establece como restricción para la terminación del proyecto que el sistema de seguridad debe cumplir con los requisitos especificados por la licitación. A continuación se muestran las características técnicas mínimas especificadas en la licitación:

En cuanto a la solución en general, el sistema tiene que tener escalabilidad para controlar al menos 250 bastidores, de los cuales GGT Solutions tiene que entregar los dispositivos necesarios para habilitar el control en al menos 60 bastidores. El sistema debe incluir el programa y la licencia necesaria para su correcta operación. Los dispositivos deben ser compatibles al 100% con el programa de administración de redes `WhatsUp Gold®` versión 7.0.4 y superiores. Estos dispositivos deben tener la capacidad para operar sobre una red de banda ancha.

En cuanto a las características del dispositivo, cada dispositivo deberá tener al menos una interfaz `Ethernet` y al menos un puerto serie. Cada dispositivo deberá ser configurable mediante consola local (ya sea por el puerto serie o `Ethernet`) y remotamente a través de la interfaz `Ethernet`. Cada dispositivo deberá tener al

menos 4 puertos de salida digital controlables remotamente desde el sitio central. Dichas salidas se utilizarían en un futuro para abrir remotamente las puertas del bastidor. Cada unidad deberá poseer una mini sirena que se active cuando alguna de las señales controladas cambie de estado, por ejemplo cuando una puerta sea abierta. Además, dicha sirena podría desactivarse local y remotamente desde el BCCR. Cada dispositivo deberá contar con al menos 5 puertos de entrada digitales (para medir el estado de las puertas frontal, trasero, lateral derecha e izquierda, así como la presencia de flujo de aire) y uno analógico (valor de temperatura).

En cuanto a las señales por medir, los dispositivos deben medir señales digitales y analógicas, como por ejemplo cierre/apertura de las puertas y temperatura.

En cuanto a parámetros de configuración en el dispositivo, se le deberá configurar valores de TCP/IP como dirección IP, máscara de subred y puerta de enlace predeterminada. Para valores de SNMP, se debe configurar la comunidad SNMP y la dirección IP de la estación de administración de redes. Para valores de temperatura, se debe configurar el intervalo en cual el dispositivo no generará alarmas.

En cuanto a administración remota de los dispositivos, el sistema deberá incluir el programa y la licencia respectiva para administrar los módulos centralizadamente desde el BCCR. Las alarmas podrán deshabilitarse remotamente desde el BCCR para cuando se brinde servicio al equipo instalado dentro del bastidor.

En cuanto al módulo de generación de alarmas, cada dispositivo deberá notificar mediante tramas SNMP (`traps`) al menos las siguientes condiciones: apertura de la puerta frontal, apertura de la puerta trasera, apertura de alguna de las puertas laterales del bastidor, incremento de la temperatura interna del bastidor sobre el límite configurado previamente y problemas con los ventiladores del bastidor (flujo del aire).

1.2.2 Solución implementada

Según los requisitos del proyecto se necesitaría un sistema como se muestra en la Figura 1.1.

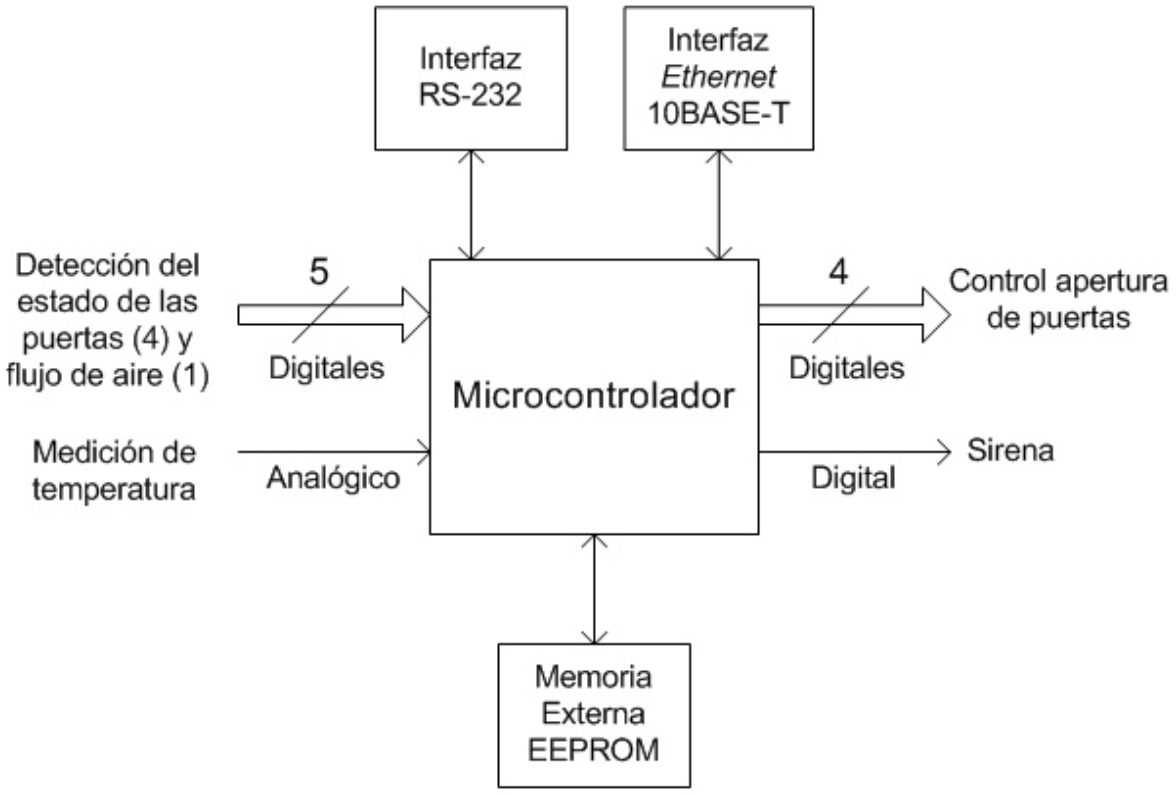


Figura 1.1 Sistema requerido para el sistema de seguridad

Para la implementación del sistema de seguridad se utilizó la tarjeta SBC65EC (ver Figura 1.2) de `Modtronix`, cuyas características se encuentran resumidas en la Figura 1.3. Esta tarjeta usa un microcontrolador PIC18F6621 de `Microchip`®. Esta tarjeta fue seleccionada ya que cumplía con los requisitos físicos del sistema de seguridad, además de un reducido costo. El sistema requiere un puerto analógico de entrada cuando la tarjeta tiene la capacidad de tener 12 entradas analógicas; 10 puertos digitales cuando se pueden tener hasta 32; interfaces tanto serie como `Ethernet` cuando la tarjeta si los contiene.

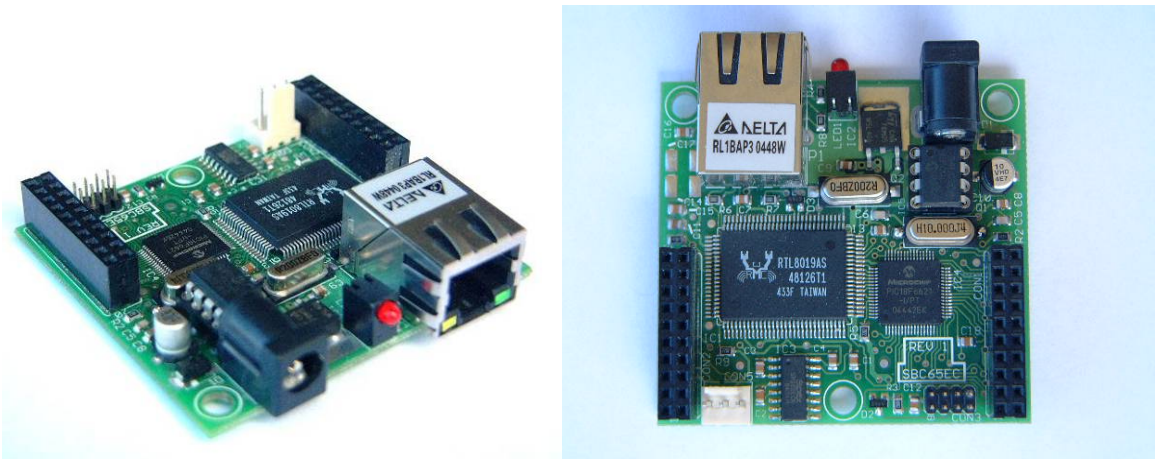


Figura 1.2 Vista de la tarjeta SBC65EC de `Modtronix`

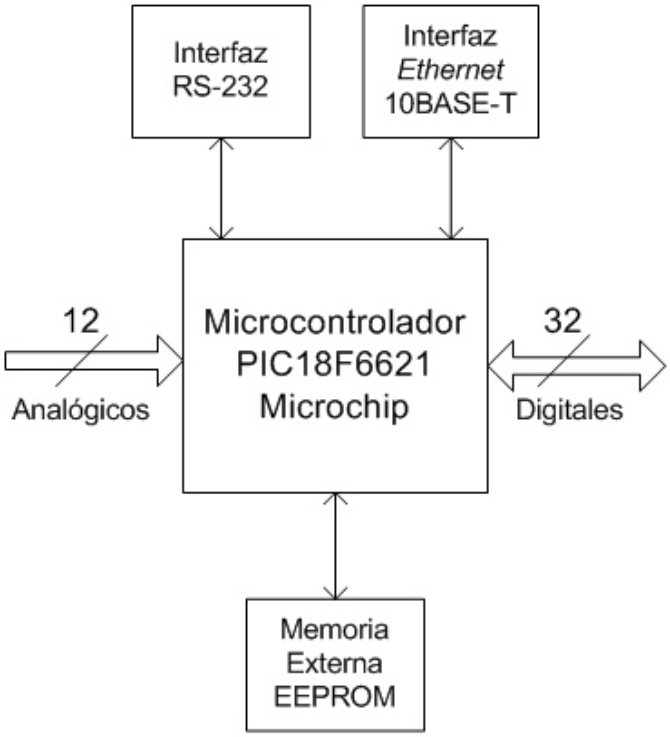


Figura 1.3 Características de la tarjeta SBC65EC de `Modtronix`

Como el sistema involucra el uso de `Ethernet` para la comunicación TCP/IP, se requería de una implementación del conjunto de protocolos TCP/IP. Para ello se utilizó la implementación de `Microchip`®, con la cual se tiene libertad de uso. Así, el

dispositivo puede ser accedido por página WEB implementando un servidor WEB en la tarjeta, donde la página HTML se almacenaría en la EEPROM. Esta EEPROM se comunica al microcontrolador por medio de una interfaz I^2C y la velocidad de acceso del microcontrolador hacia la memoria es de 400kHz. Con este dato, el fabricante asegura que es factible hacer consultas a la EEPROM de la página WEB. Además, el dispositivo puede ser accedido por consola por medio de la interfaz serie.

En cuanto a sensores implementados en el sistema, se incluyen contactos magnéticos (puertas y presencia de flujo de aire) y un sensor de temperatura.

Para la administración remota y local, el sistema debe ser accedido remotamente por medio de una página WEB y localmente por medio de una terminal. En el caso de la página WEB se implementaron páginas generadas dinámicamente (mediante archivos CGI). Esto con el fin de manipular y desplegar información en tiempo real. En el caso de la terminal se empleó una configuración por medio de menú.

Para el envío de notificaciones de SNMP, se uso la convención establecida para la definición de `traps` del RFC 1215 [15]. Las notificaciones que se envían son los eventos cuando se abre alguna puerta, la temperatura supera el rango establecido y cuando no hay presencia de flujo de aire.

Capítulo 2: Meta y Objetivos

2.1 Meta

Notificar al BCCR sobre el acceso de personal no autorizado a los bastidores de comunicación localizados en las entidades financieras.

2.2 Objetivo general

Desarrollar un sistema de seguridad en los bastidores de comunicación que permita notificar ante los eventos de apertura de puertas, superación de los límites de temperatura e insuficiencia de flujo de aire a través de la plataforma SINPE.

2.3 Objetivos específicos

- Desarrollar un sistema de medición para la variable de temperatura.
- Desarrollar un sistema de medición para la variable de flujo de aire.
- Desarrollar un sistema de medición para la variable de apertura de puertas.
- Desarrollar un sistema de notificación compatible con la plataforma SINPE, ante la detección de cambio de estado de las variables.

Capítulo 3: Marco teórico

3.1 Descripción del sistema

En la Figura 3.1 se muestra el panorama del funcionamiento del sistema de seguridad propuesto. El sistema consta de un sistema embebido que está revisando el estado de las puertas, temperatura y flujo de aire. Éste se encuentra dentro de un bastidor de comunicaciones localizado en una entidad financiera. El sistema embebido es capaz de enviar notificaciones de SNMP a través de la plataforma tecnológica de SINPE cuando sucede algún evento como apertura de puertas, la temperatura fuera del intervalo establecido o insuficiencia de aire. Estas notificaciones son recibidas por la estación de administración de red, el cual es una computadora que está ejecutando el programa `WhatsUp Gold®`.

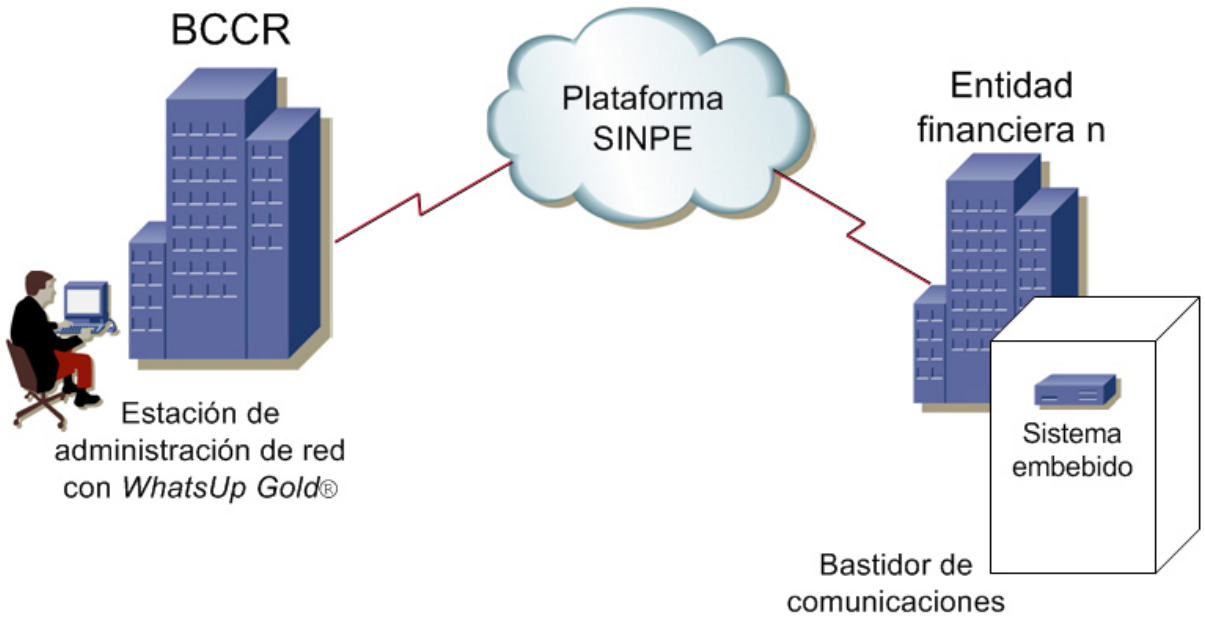


Figura 3.1 Panorama de funcionamiento del sistema de seguridad

3.2 Antecedentes bibliográficos

El desarrollo de este proyecto está asociado a la construcción de un sistema embebido. En la sección 3.3 se hará referencia de porqué el sistema por desarrollar se clasifica como un sistema embebido según los criterios brindados por Catsoulis [4].

El proyecto tiene dos puntos medulares en cuanto a su desarrollo, la implementación del conjunto de protocolos TCP/IP de Microchip®, y la implementación de notificaciones de SNMP. En la sección 3.4 se da un vistazo a la implementación de Microchip [14] y en la sección 3.5 se da un vistazo a la terminología de SNMP.

3.3 Sistemas embebidos

Un sistema embebido normalmente se dedica a una tarea específica y comúnmente carece de un sistema operativo. La aplicación reside en el mismo nivel que el firmware (los programas que inicializan los subsistemas de hardware a un estado conocido y configura el sistema para su correcta operación). Esto se refleja bajo el principio que en un diseño embebido, el sistema debe llegar al objetivo de la forma más simple posible.

El microcontrolador es el procesador llamado a utilizarse en los sistemas embebidos. Éste no sólo es procesador, sino también contiene memoria, y algunos puertos de entrada/salida dentro de un circuito integrado.

3.4 Conjunto de protocolos TCP/IP

A continuación, se muestra las características de la arquitectura del conjunto TCP/IP implementado por Microchip® y luego una descripción de cada uno de sus módulos.

3.4.1 Características de la arquitectura del conjunto TCP/IP de Microchip

- Escrito en el lenguaje de programación C.
- El conjunto TCP/IP de Microchip® es diseñado para ejecutarse en la familia de microcontroladores PIC18 de Microchip®.
- Semejante al modelo TCP/IP en cuanto a separación por capas.
- Existe un código fuente distinto para la implementación de cada capa.
- El conjunto TCP/IP de Microchip® podría ignorar algún módulo para evitar procesamiento inteligente (información en la trama innecesaria).
- Implementa su propio sistema de multitarea cooperativa (una vez que una tarea termina su acción, delega el control a otra tarea).

3.4.2 Descripción de los módulos del conjunto TCP/IP de Microchip

MAC

El archivo MAC.c del conjunto TCP/IP de Microchip® se especifica para utilizarlo con la NIC de Realtek RTL8019AS (esta lo contiene la tarjeta SBC65EC).

El módulo utiliza la SRAM disponible en la NIC como memoria intermedia de espera hasta que un nivel mayor la lea. Además, realiza los cálculos respectivos de FCS en esa memoria intermedia. Para la recepción, la NIC maneja una memoria intermedia FIFO. Para la transmisión, la capa MAC maneja su propia cola de transmisión: cuando se transmite un mensaje requiere averiguar la dirección MAC, entonces almacena el mensaje hasta que reciba la dirección MAC destino.

ARP

Este módulo es llevado a cabo con 2 módulos:

- ARP (ARP.c crea los métodos)

- ARPTask (ARPTsk.c utiliza los métodos y provee los servicios completos de ARP).

ARPTask opera en 2 modos: Servidor y Cliente/Servidor. En Cliente/Servidor se utilizan solicitudes ARP.

IP

Es implementado por IP.c y en IP.h se define los servicios que provee la capa IP. Esta capa IP es pasiva, no es capaz de responder paquetes por sí sola. Capas superiores utilizan los métodos IP y buscan dentro del paquete IP.

ICMP

Es implementado por ICMP.c y en ICMP.h se definen los servicios que provee esta capa. Esta capa es pasiva, hay que usar una capa superior para que use los métodos de ICMP y haga una búsqueda al paquete, para interpretarlo y ejecutar la acción de responder con un eco de ICMP.

TCP

Es implementado por TCP.c y en TCP.h se definen los servicios que provee esta capa. Esta capa es activa, éste busca en los paquetes TCP y responde a la estación remota de acuerdo a la máquina de estados TCP. Es implementado como una tarea cooperativa. TCP.h provee los servicios de los socket de TCP. Se pueden tener desde 2 a 253 socket de TCP. El límite está en la memoria disponible y en el compilador usado. Cada socket consume 36bytes, e incrementa el tiempo de procesamiento general de TCP.

En la transmisión todos los socket en el conjunto TCP/IP de Microchip® comparten uno o más memorias intermedias de transmisión (hay que liberarlos a tiempo). En la recepción sólo hay una memoria intermedia receptora, por lo que, una vez que se recibe el paquete se debe hacer una búsqueda y descartar la memoria intermedia en el mismo tiempo de la tarea. Por especificaciones de TCP, cada segmento debe tener una suma de verificación. Si se usa la NIC, TCP usa el espacio

SRAM de la NIC para guardar y calcular la suma de verificación (se reduce requerimientos de espacio en RAM). El cálculo de estas sumas de verificación está descrito en el RFC1071 [15].

Esta capa implementa la mayoría de los estados de TCP FSM descritos en el RFC793. Por ejemplo, reintentos automáticos y operaciones con tiempo.

UDP

Es implementado por `UDP.c` y en `UDP.h` se definen los servicios de los `socket` que provee esta capa. Esta capa es activa. El módulo UDP se implementa como una tarea cooperativa. Esta capa soporta hasta 254 paquetes UDP. Cada `socket` consume 19bytes.

Para la transmisión dentro del conjunto TCP/IP de `Microchip®` comparte uno o más memorias intermedias de transmisión comunes. Esto reduce requisitos de RAM. Pero hay que asegurarse que hay suficientes memorias intermedias de transmisión para todos los `socket`. Para la recepción, sólo hay una memoria intermedia receptora, por lo que, una vez que se recibe el paquete se debe procesar y descartar la memoria intermedia en el mismo tiempo de la tarea.

Por especificaciones de UDP, no es obligatorio calcular una suma de verificación. Por tanto, el conjunto TCP/IP de `Microchip®` no lo hace, y llena el espacio con ceros. Se supone que la integridad de los datos ya está asegurada por el servicio que la utiliza. Pero existen aplicaciones que sí requieren verificar este campo como medida de integridad.

Administrador del conjunto TCP/IP de Microchip

Este administrador es un conjunto de módulos, que son llamados según el tipo de paquete. En lugar de que la aplicación principal se sature por manejar los módulos individuales, se usa `StackTsk.c`. Éste es una tarea cooperativa que está consultando la capa MAC por paquetes válidos y cuando se recibe y se codifica, se envía al respectivo módulo.

Este administrador no es parte del conjunto TCP/IP de Microchip®, sino lo que hace es suplir a la aplicación principal. Antes de usarlo, se debe inicializar. Luego, la aplicación periódicamente debe llamar al método StackTask().

3.5 SNMP

SNMP (protocolo simple de administración de redes) es un protocolo de Internet que fue originalmente diseñado para administrar diferentes dispositivos de red como servidores de archivos, enrutadores, entre otros. No obstante, también se puede usar en sistemas embebidos que de cierta forma están conectados en una red TCP/IP. Los sistemas se pueden comunicar entre ellos usando SNMP para transferir información de estado y control.

3.5.1 Terminología SNMP

En la Figura 3.2 se muestra el modelo SNMP típico y la terminología asociada.

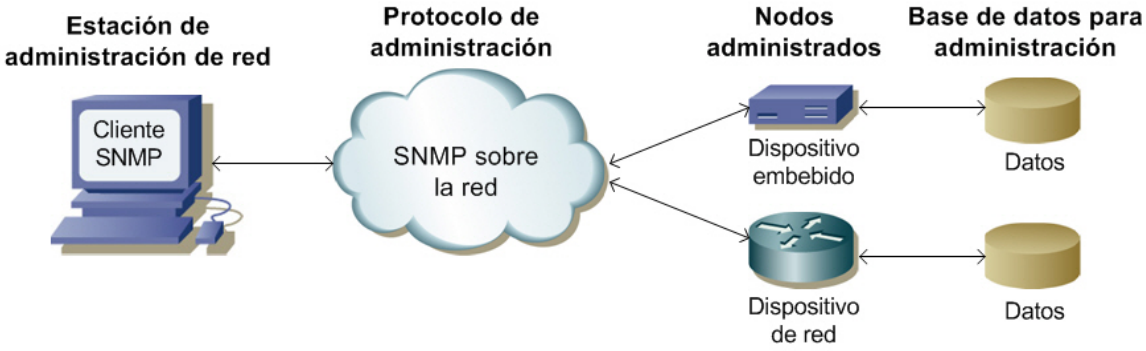


Figura 3.2 Modelo de SNMP y terminología asociada

NMS (Estación de administración de red)

La NMS es una mitad de la instalación de SNMP. La otra mitad es el agente. Normalmente, la NMS es una computadora personal que ejecuta un programa principal. NMS actúa como un cliente SNMP, donde periódicamente consulta al agente SNMP por los datos. La NMS puede usarse para controlar una colección de dispositivos similares o diferentes. Inclusive, la adición de dispositivos en la red no requiere cambios en el programa NMS.

Nodo administrado ó agente SNMP

El nodo administrado (comúnmente llamado agente SNMP) es el dispositivo que es administrado por la NMS. El agente SNMP implementa la porción de servidor al protocolo SNMP, actuando como un agente entre la aplicación del dispositivo y el programa NMS. La relación no es necesariamente uno a uno, como un simple agente puede simultáneamente servir a varios NMS. El agente espera por las solicitudes del NMS. No obstante, el agente SNMP también puede generar notificaciones hacia la NMS.

MIB (Base de datos para administración)

Cada agente maneja su propia colección de variables, llamado MIB. Para organizar la MIB, SNMP define un esquema conocido SMI (Estructura de la información de administración). En la Figura 3.3 se muestra un SMI genérico. La SMI tiene una estructura de árbol donde las hojas son las que contienen los datos. SNMP y otros documentos RFC para la Internet han definido varios MIB. En la Figura 3.4 se muestra un subárbol del actual MIB de la Internet. La estructura de este estándar MIB y otros no deben de ser modificados si el agente SNMP necesita ser compatible con otros programas NMS. Un especial subárbol, es el llamado "enterprises" que es definido para empresas privadas. Cada fabricante de dispositivos con agentes SNMP debe tener su propio número registrado por el IANA. En el caso de Microchip®, se tiene registrado el número 17095.

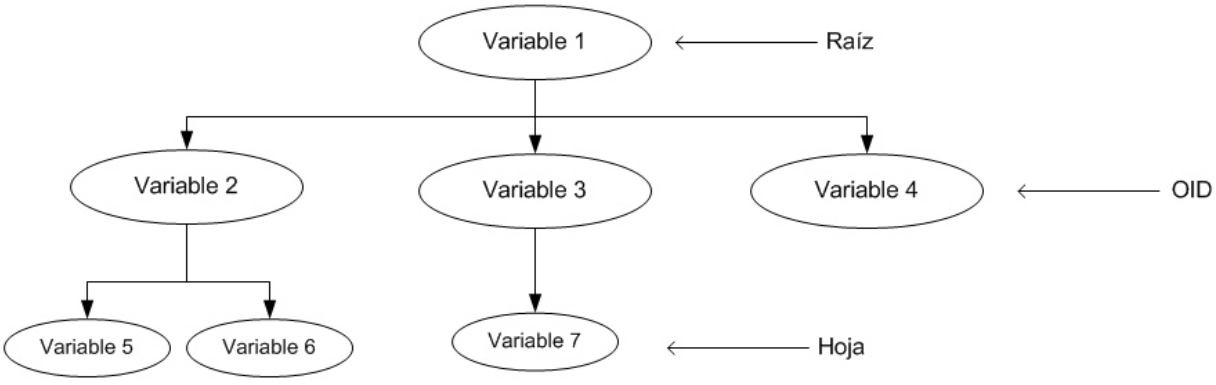


Figura 3.3 Estructura genérica de un SMI

OID (Identificador de objetos)

Cada nodo en el árbol MIB es identificado por una secuencia de números decimales llamado OID. Cada OID es escrito en una notación decimal separado por puntos. Por ejemplo, en la Figura 3.4 el OID para el nodo “mib” se escribe 1.3.6.1.2.1 También, el nodo “mib” puede ser escrito de la siguiente forma: iso(1).org(3).dod(6).internet(1),mgmt(2).mib(1)

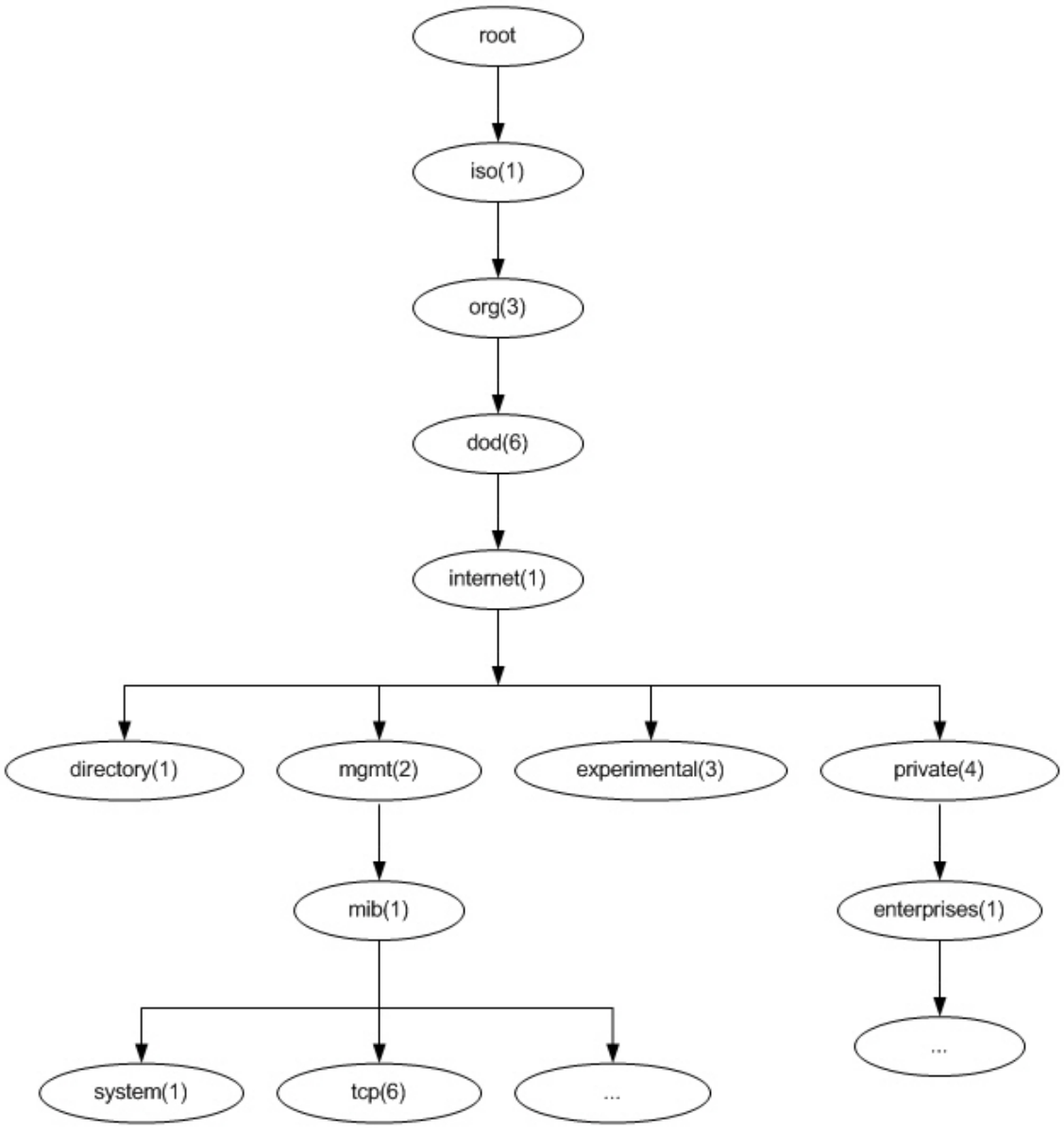


Figura 3.4 Ejemplo de una estructura de información del subárbol parcial de Internet

Capítulo 4: Procedimiento metodológico

4.1 Reconocimiento y definición del problema

Para la definición del problema se planearon las siguientes actividades:

- Entrevista con el Ing. José Pablo Esquivel que conoce sobre el problema debido a que se ha reunido con el Ing. Mario Alabí, encargado de las contrataciones de tecnología del BCCR.
- Visita a la Asociación Bancaria Costarricense con el Ing. Alberto Soto, para conocer uno de los bastidores que pertenece a SINPE.
- Búsqueda de información del proyecto de SINPE del BCCR con el proveedor principal de los equipos de comunicación, Cisco Systems® a través de su página WEB.

4.2 Obtención y análisis de información

Para la obtención de la información relevante acerca del problema se realizó búsquedas por Internet acerca de comunicaciones con TCP/IP en sistemas embebidos.

Para la evaluación de la información encontrada acerca de sistemas embebidos se escogió por aquellos que permitieran cumplir con los requisitos del sistema a un costo menor (mediante análisis de costos).

4.3 Evaluación de las alternativas y síntesis de una solución

La solución del problema ha sido analizada después de una reunión entre los ingenieros del departamento de Proyectos Especiales y el practicante. La validez de la solución optada se determinó bajo un análisis de costos y un estudio de confiabilidad con el fabricante de microcontroladores. Este departamento ya ha tenido experiencia con la programación de microcontroladores de Microchip. Además uno de los puntos importantes es que se requería rapidez de implementación debido

a las restricciones de tiempo de la licitación. La tarjeta de Modtronix seleccionada reduce tiempos en el desarrollo al ofrecer una integración de los componentes requeridos para el proyecto en un circuito impreso ya ensamblado. Inclusive este fabricante tiene un chasis que se adapta a la tarjeta para la interfaz de los sensores.

4.4 Implementación de la solución

El procedimiento seguido para la implementación de la solución consistió en la programación del microcontrolador de cada uno de los módulos requeridos para el proyecto. Por ejemplo, la implementación del conjunto de protocolos TCP/IP, el menú del Terminal, el agente de SNMP, la configuración de páginas WEB dinámicas, detección del estado de puertas y flujo de aire, y medición de temperatura.

Los mecanismos para la evaluación de la propuesta de solución durante el desarrollo se hicieron mediante la simulación de un ambiente de red. Esta red consistió básicamente de un conmutador de red, una computadora ejecutando el programa WhatsUp Gold® versión 8.03 y el dispositivo en desarrollo.

La evaluación de la solución una vez implementada se realizó en un principio con el criterio del departamento de Proyectos Especiales de GGT Solutions. Luego, se realizó contra la aceptación del personal de comunicaciones del Sistema de Pagos del BCCR.

Además, se realizó una exposición al departamento de Proyectos Especiales sobre los detalles del proyecto.

4.5 Reevaluación y rediseño

En cuanto a criterios que se pueden aplicar para determinar posibles mejoras es el uso de una versión más actualizada del protocolo SNMP para agregar métodos de autenticación y cifrado, así como de la implementación en el agente del comando Get, Get-Next y Set. Además, para la programación se utiliza el compilador de MPLAB C18 de Microchip versión 3.02, por lo que habría que estar revisando actualizaciones.

Capítulo 5: Descripción detallada de la solución

Este capítulo expone el diseño e implementación de la solución. Inicialmente se indica la solución que fue seleccionada, y posteriormente se describe la solución a nivel de hardware y firmware.

5.1 Análisis de soluciones y selección final

La validación de la selección del sistema embebido por utilizar en el proyecto se hizo mediante un estudio de costos, es decir se selecciona aquel que sea el de menor precio siempre y cuando pueda cumplir con los requisitos físicos del sistema de seguridad.

En la Tabla 5.1 se resumen los dispositivos consultados en una tienda especializada de microcontroladores [12] en Internet, el cual es el proveedor del sistema embebido utilizado en el proyecto.

Tabla 5.1 Sistemas embebidos consultados para selección de uno para el proyecto

Sistemas Embebidos	SBC65EC de Modtronix®	Ethernut BRD de egnite®	LPC2214 (ARM) BRD de Philips®
Microcontrolador	PIC18F6621 de Microchip®	ATmega128 8-bit AVR RISC de Atmel®	LPC2214 de Philips®
Puerto Ethernet	Sí, 10Mbps	Sí, 10Mbps	Sí, 10Mbps
Puerto Serie	Sí	Sí	Sí
EEPROM Externa	Sí, 512Kb	No	Sí, 512kb
Pines de extensión	40	64	20
Precio (US $)	72	138	160

Los tres sistemas embebidos resumidos en la Tabla 5.1 reúnen las características para la implementación del sistema de seguridad y por costo la tarjeta SBC65EC de Modtronix® fue el sistema embebido seleccionado. Además, este fabricante provee la ventaja de que se pueda utilizar un chasis para colocar dicha tarjeta con el fin de conectar los sensores (véase la Figura 5.1).

Figura 5.1 Vista del chasis IOR5E de Modtronix para la tarjeta SBC65EC

5.2 Descripción del hardware

En la Figura 5.2 se muestra el diagrama de bloques de la solución en hardware del sistema de seguridad. El hardware se constituye de la tarjeta SBC65EC (véase diagrama esquemático en el anexo B.1) como núcleo del sistema, que se encuentra inserto dentro del chasis IOR5E (véase diagrama esquemático en el anexo B.2). Este último provee de forma directa la interfaz de los sensores (puertas, temperatura y flujo de aire), mini sirena, puerto serie y relevadores. Estas interfaces del chasis se conectan de forma indirecta a la tarjeta SBC65EC con algunos circuitos adicionales. La tarjeta SBC65EC provee de forma directa el enlace Ethernet y la alimentación eléctrica.

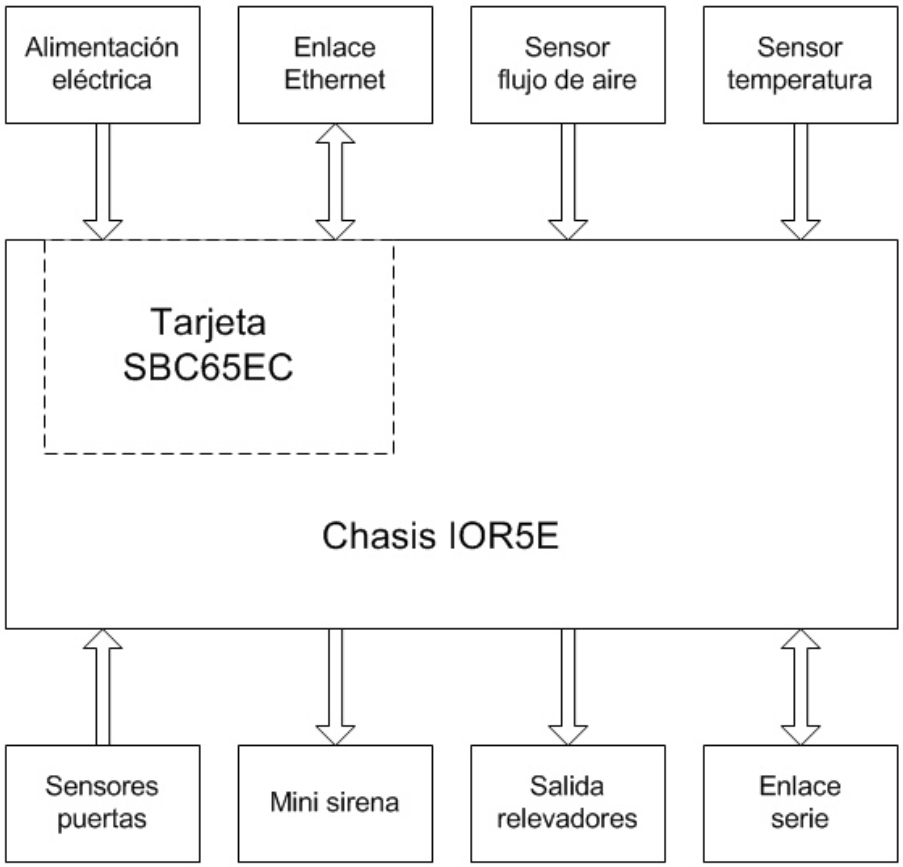


Figura 5.2 Diagrama de bloques del hardware del sistema de seguridad

A continuación, se detalla cada uno de los módulos de hardware implementados.

5.2.1 Sensores de puertas

La detección de apertura de alguna puerta se realizó por medio de un contacto magnético en cada puerta (uno para la puerta frontal, uno para la trasera, uno para la izquierda y uno para la derecha). En el proyecto se utilizó contactos magnéticos de la marca amseco® cuyo modelo es AMS-10. Este contacto magnético se muestra en la Figura 5.3. El comportamiento del interruptor es de “Normalmente Cerrado” el cual funciona así: cuando el imán está enganchado, el contacto está cerrado; y cuando el imán no está enganchado (imán separado a una distancia mayor de 1.9 cm), el contacto está abierto.

Figura 5.3 Contacto magnético amseco® AMS-10 para puertas

El circuito para la conexión de cada uno de los contactos magnéticos se muestra en la Figura 5.4.

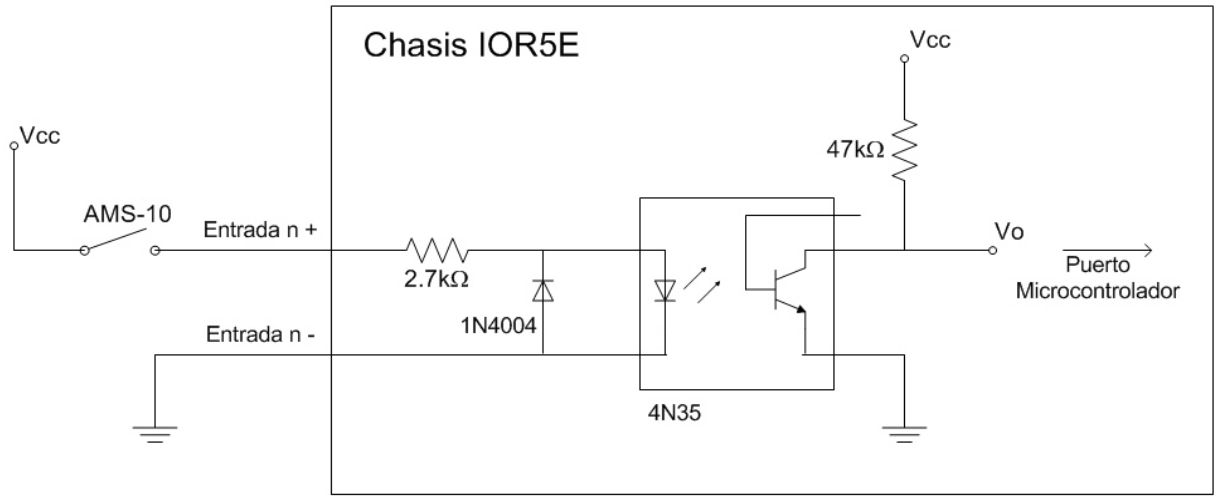


Figura 5.4 Circuito para la conexión de cada contacto magnético para puertas

Este circuito opera de la siguiente forma: si el contacto magnético está cerrado (cuando la puerta está cerrada), existe una excitación en la base del transistor repercutiendo en que el transistor esté en saturación, y así la tensión Vo es aproximadamente cero para una lectura digital en el microcontrolador de 0. Por lo contrario, si el contacto magnético está abierto (cuando la puerta está abierta), no existe excitación en la base del transistor repercutiendo en que el transistor esté en corte, y así la tensión Vo es Vcc para una lectura digital del microcontrolador en 1.

Este circuito tiene la ventaja de que por más que un intruso corte algún cable del contacto magnético, la lectura digital en el microcontrolador siempre sería de 1.

5.2.2 Sensor de temperatura

La medición de temperatura se realizó con el sensor de temperatura LM19 de `National Semiconductor Corporation`. El LM19 tiene una salida análoga de precisión que opera sobre el rango de temperatura de -55°C a +130°C. La función de transferencia es predominantemente lineal, con una curva parabólica predecible. Para medir la temperatura, se utilizó la función de transferencia:

$$V_O = -11.69\text{mV}/^{\circ}\text{C} \times T + 1.8663\text{V} \qquad (2.1)$$

El circuito para la conexión del sensor de temperatura se muestra en la Figura 5.5.

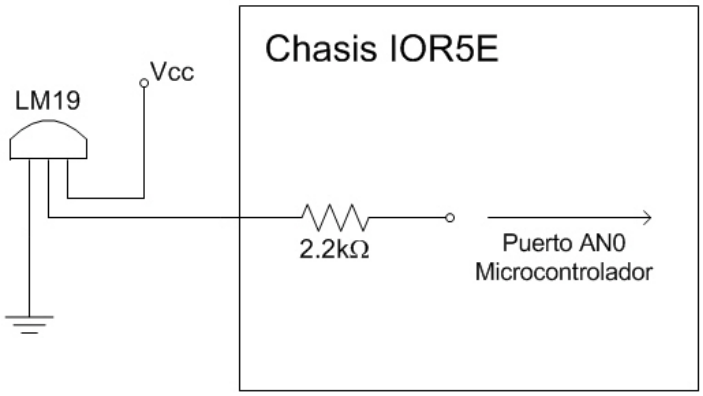


Figura 5.5 Circuito para la conexión del sensor de temperatura

El circuito opera de la siguiente forma: el sensor de temperatura tiene un valor de tensión de salida que depende del valor de temperatura (de acuerdo a la función de transferencia). Esta tensión corresponde al valor analógico en el puerto AN0 del microcontrolador por convertir a digital. En la sección 5.3 se describirá con detalle el módulo ADC.

5.2.3 Sensor de flujo de aire

La detección de la presencia de flujo de aire se realizó con un contacto magnético fabricado por `Stego Inc`. El modelo del sensor de presencia de flujo de aire es LC 013, y éste se muestra en la Figura 5.6. El comportamiento del interruptor

es de “Normalmente Cerrado” el cual funciona así: cuando no hay presencia de aire (velocidad del aire menor o igual a 2.5m/s), el contacto está cerrado; y cuando hay presencia de flujo de aire, el contacto está abierto.

Figura 5.6 Contacto magnético Stego Inc LC 013 para detectar presencia de flujo de aire

El circuito para la conexión del sensor de presencia de flujo de aire se muestra en la Figura 5.7.

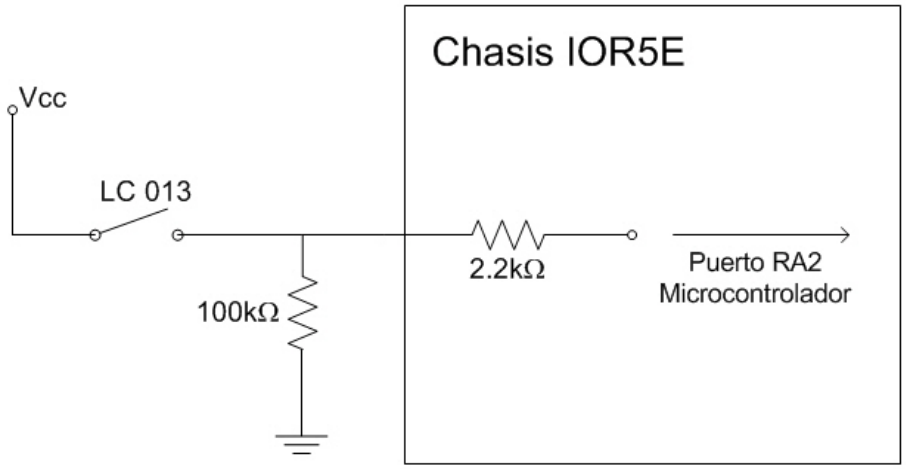


Figura 5.7 Circuito para la conexión del sensor de presencia de flujo de aire

Este circuito opera de la siguiente forma: si el contacto magnético está cerrado (cuando no hay presencia de flujo de aire), el valor de tensión Vcc se refleja en el puerto RA2 para una lectura digital en el microcontrolador de 1. Por lo contrario, si el

contacto magnético está abierto (cuando hay presencia de flujo de aire), el valor de referencia GND (0 V) se refleja en el puerto RA2 para una lectura digital en el microcontrolador de 0.

5.2.4 Mini sirena

La mini sirena se implementó con el zumbador magnético F/TCW 05 de Digisound. Este zumbador se muestra en la Figura 5.8. Este zumbador opera con 5V, genera un sonido cuya frecuencia oscila en 2300 ± 300 Hz con un nivel de presión de sonido de 85dB a 10cm.

Figura 5.8 Zumbador magnético empleado como mini sirena

El circuito para la conexión del zumbador se muestra en la Figura 5.9.

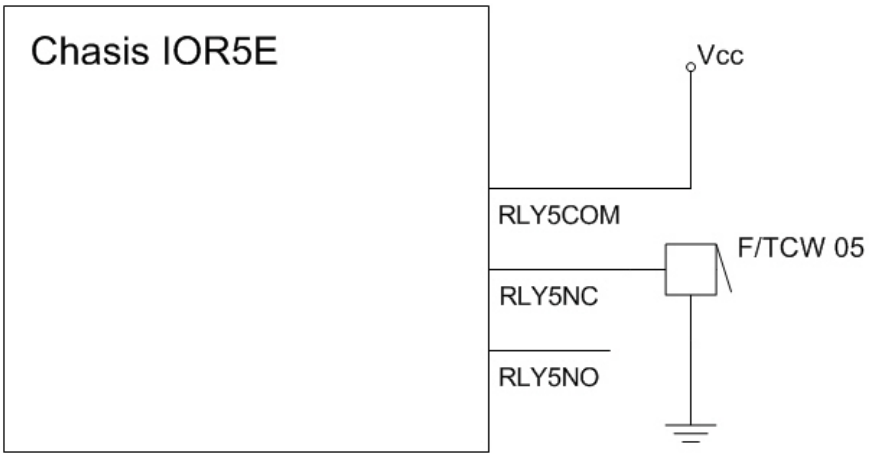


Figura 5.9 Circuito para la conexión del zumbador para la mini sirena

Este circuito opera de la siguiente forma: cuando el sistema requiera activar la mini sirena debe activar el relevador 5 del chasis IOR5E con una entrada lógica de 1

en el relevador (esto hace que el relevador cierre el contacto para que el zumbador reciba Vcc). Si el sistema requiere desactivar la mini sirena debe abrir el contacto del relevador 5 con una entrada lógica de 0 en éste.

5.2.5 Salida de relevadores

El chasis IOR5E contiene 5 relevadores para su activación desde el microcontrolador a través de un convertidor de serie a paralelo (con un circuito integrado de desplazamiento de registro). De estos 5 relevadores, uno (relevador 5) ya está en uso por la mini sirena. Los 4 restantes (relevador 1, 2, 3 y 4) están disponibles para alguna aplicación a futuro. Por ejemplo, que se puedan abrir las puertas remotamente a través de la página WEB del dispositivo.

5.2.6 Enlace Ethernet

La tarjeta SBC65EC tiene un puerto Ethernet de 10Mbps. El conector RJ-45 cumple con los estándares IEEE 802.3. El conector RJ-45 tiene dos LED instalados, un LED verde que indica si hay enlace y un LED amarillo que indica actividad.

5.2.7 Enlace serie

La tarjeta SBC65EC tiene una interfaz USART con protección de descarga electroestática de ± 15kV. Las señales USART están disponibles tanto en la tarjeta SBC65EC como en el chasis IOR5E con un conector de 3 pines tipo Molex. Cuando la tarjeta es insertada en el chasis, solo el conector del chasis está disponible para conectar un cable serie.

5.2.8 Alimentación eléctrica

El sistema de seguridad se alimenta con 12V CD. Por tanto es requerido que se utilice un adaptador de 12V con conector de 5mm con el centro positivo. Esta energía la recibe la tarjeta SBC65EC, el cual regula la tensión para obtener 5V. Los nodos de 12V y de 5V de la tarjeta SBC65EC los comparte con el chasis IOR5E.

5.3 Descripción del firmware

En este proyecto, los programas se almacenan en la memoria Flash del microcontrolador. En esta memoria se guarda el código que se necesita en el arranque del sistema. Según Catsoulis [4], "este software es generalmente conocido como firmware, y contiene el software que inicializa el sistema colocando los dispositivos de entrada/salida en un estado conocido… y en caso de un sistema embebido puede contener la aplicación por sí misma". Bajo esta definición, de ahora en adelante se refiere a firmware al código realizado en el proyecto.

El firmware del sistema de seguridad se compone de 5 módulos principales, los cuales se muestran resumidos en la Figura 5.10.

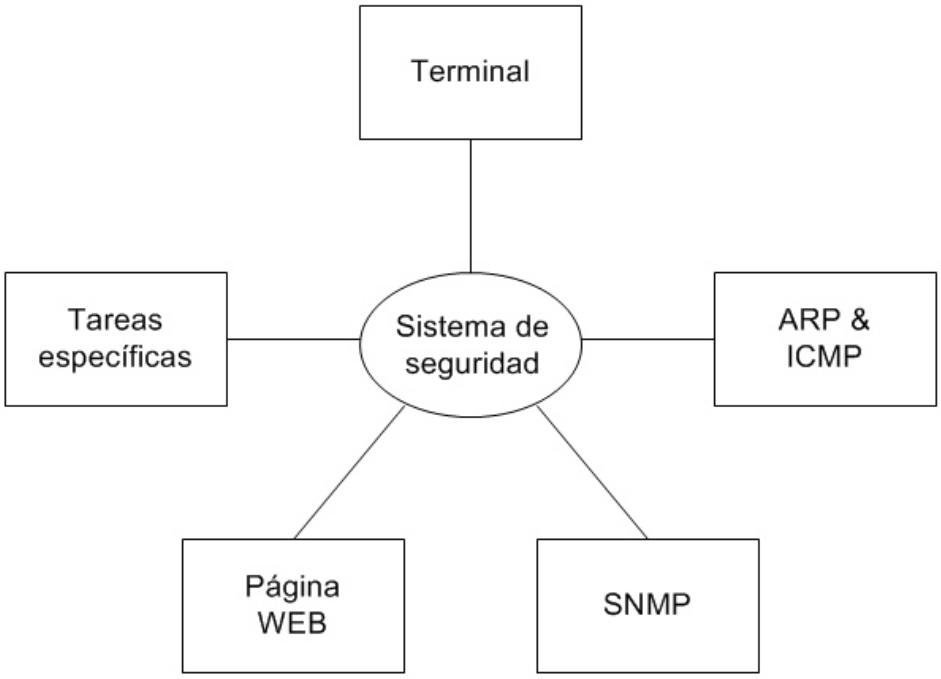


Figura 5.10 Diagrama de bloques de los módulos principales del sistema de seguridad

El módulo de "Aplicación principal" se encarga de controlar los módulos expuestos en el diagrama anterior. En general, el módulo "Terminal" se encarga del despliegue del menú de configuración del dispositivo en un Terminal como el programa HyperTerminal de Hilgraeve. El módulo "Tareas específicas" se

encarga de verificar el estado de las variables (puertas, temperatura y flujo de aire) y de la activación de los relevadores. El módulo “Página WEB” se encarga de recibir los comandos dinámicos de la página WEB que el usuario envía cuando navega sobre la página. El módulo “SNMP” se encarga de enviar las notificaciones a la estación de administración de red cuando se da algún evento apertura de puerta, temperatura fuera de rango y/o insuficiencia de aire. El módulo “ARP & ICMP” se encarga de brindarle al dispositivo la posibilidad de que se pueda comunicar con alguna estación en la red LAN (en el caso de ARP); y en el caso de ICMP, brindarle al dispositivo la posibilidad de que cualquier estación pueda corroborar la conectividad con el sistema.

5.3.1 Aplicación principal

Este módulo se encarga de distribuir las labores. En este se encuentra el ciclo infinito del microcontrolador para ejecutar indefinidamente cada uno de los procesos. En la Figura 5.11 se muestra el diagrama de flujo de la aplicación principal antes de ejecutar el ciclo infinito, es decir el procedimiento de inicialización del sistema de seguridad. Estos procesos se encargan de inicializar el sistema a nivel de `hardware` y las variables de configuración del sistema. Además, una vez inicializado el puerto serie se procede a mostrar el menú de configuración, donde se hace el llamado al módulo de “Terminal”.

En la Figura 5.12 se muestra el diagrama de flujo de los procesos de la aplicación principal que se ejecutan indefinidamente. Los procesos de la aplicación se dividen en tres principales:

- Tareas del conjunto de protocolos TCP/IP: Este proceso hace el llamado al módulo de “ARP & ICMP”.
- Servidor HTTP: Este proceso hace llamado al módulo de “Página WEB”.
- Tareas específicas: Este proceso hace el llamado al módulo “Tareas específicas”, dentro del cual si se da un evento que requiere notificación hace el llamado al módulo de “SNMP”.

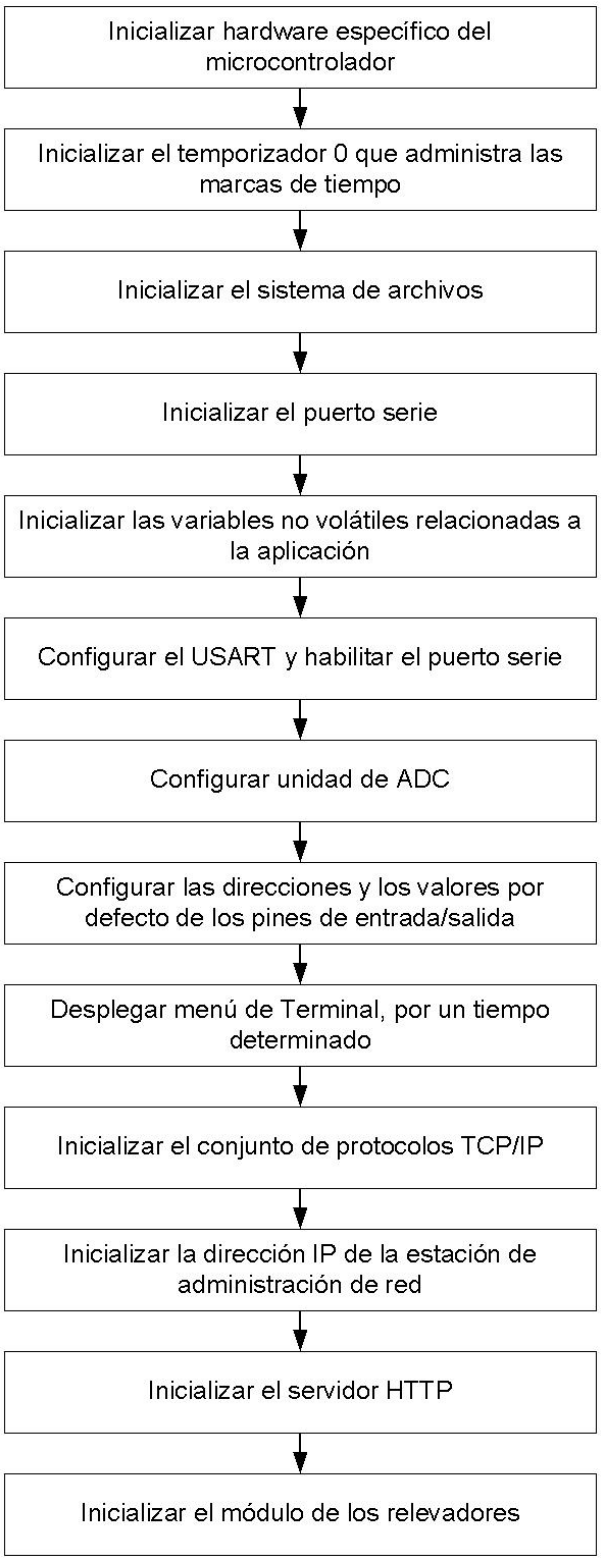


Figura 5.11 Diagrama de flujo de la inicialización de la aplicación principal

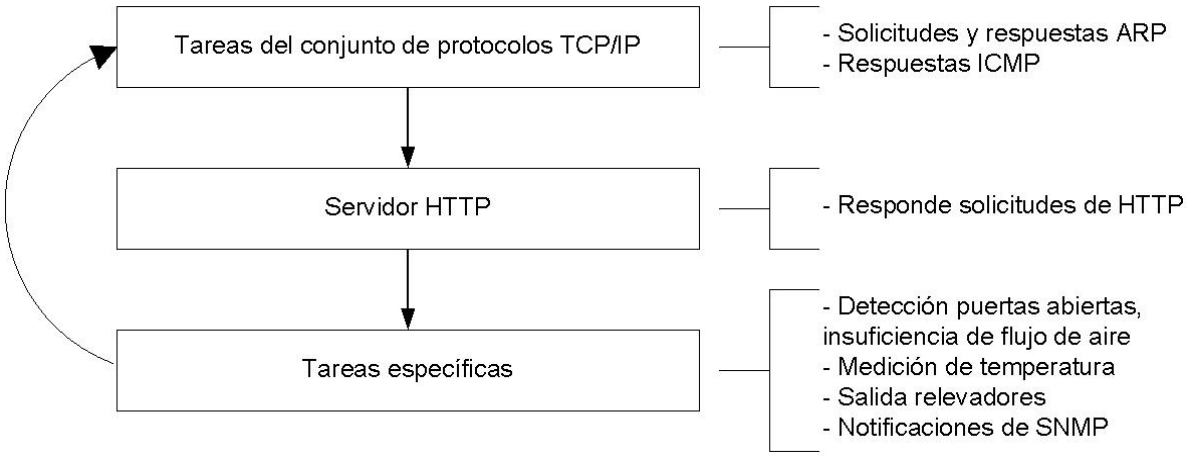


Figura 5.12 Diagrama de flujo del ciclo infinito de la aplicación principal

5.3.2 Terminal

Este módulo se encarga de la configuración del dispositivo por medio de consola con un cable serie conectado a la computadora. Esta configuración se tiene que realizar inmediatamente después de restaurar el sistema (interrumpiendo la secuencia de inicialización del sistema) porque de aquí se almacenan parámetros que se ocupan en el arranque del mismo. En la Figura 5.13 se muestra el menú de configuración del dispositivo.

```
RackMonitor RM-5ID (Version 2) (Globaltech, Jun 20 2006)

        1: Recuperacion de Contrasena
        2: Cambiar la direccion IP por defecto
        3: Cambiar la mascara de subred por defecto
        4: Cambiar la direccion del default gateway
        5: Desactivar la alarma
        6: Cambiar los parametros de SNMP
        7: Cambiar los parametros de Temperatura
        8: Descargar pagina WEB por XModem
        9: Guardar y Salir

Escoja una opcion de menu (1-9): _
```

Figura 5.13 Menú de configuración del sistema del módulo Terminal

Este módulo se encarga escribir en el puerto serie el menú de configuración, para luego esperar la recepción de alguna opción de menú digitado por el usuario (por medio de un número). Una vez recibido la opción, el sistema procede a recibir del usuario la información correspondiente (por ejemplo, si digitó 2 se le pide que digite la dirección IP del dispositivo). En caso de digitar 9, el sistema continúa con la inicialización de la aplicación principal.

5.3.3 Tareas específicas

Este módulo contiene 3 procesos principales: proceso de temperatura, de entrada/salida y de relevadores.

- Proceso de temperatura: Mide la temperatura proporcionada por el sensor colocado en el exterior del chasis usando un canal del ADC del microcontrolador, y en caso de exceder algunos de los límites configurados, se envía una notificación de SNMP llamando al módulo de SNMP. En la Figura 5.14 se muestra el diagrama de flujo de este proceso.
- Proceso de entrada/salida: Este proceso consulta el estado lógico de las entradas proporcionadas por cada contacto magnético. En caso de resultar que la puerta está abierta ó que hay insuficiencia de flujo de aire, se hace un llamado al módulo de SNMP para enviar la notificación. El llamado de SNMP está condicionado a que estén desactivadas las banderas de cada uno de las variables (por ejemplo, si la puerta frontal tiene activada la bandera, entonces por más que se abra la puerta no se envía la notificación). Además, en este proceso se activa la alarma (si y solo si, está desactivado la bandera de sirena).
- Proceso de relevadores: Este proceso verifica el estado de los parámetros de configuración almacenados (específicamente los de relevadores), para activar o desactivar cada uno de los relevadores. Estos parámetros son cambiados desde la página WEB del sistema.

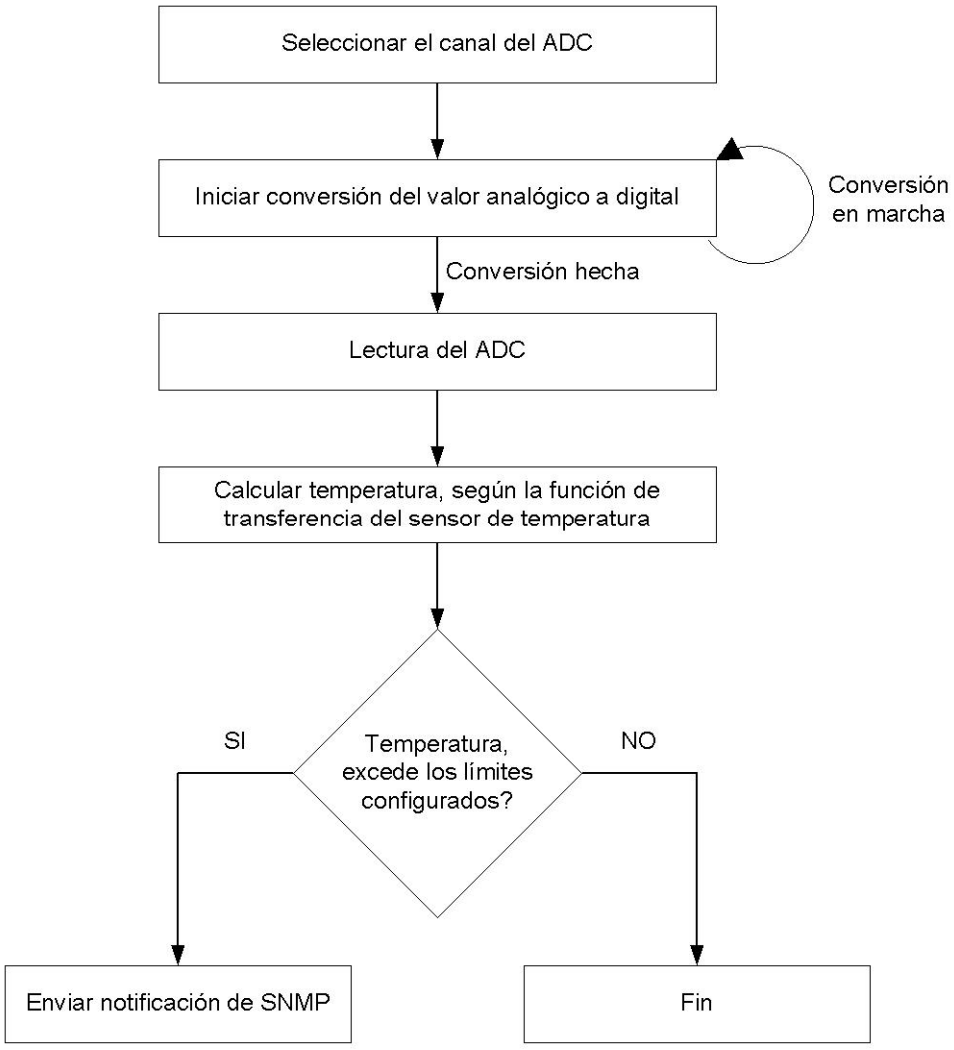


Figura 5.14 Diagrama de flujo del proceso de temperatura en el módulo de “Tareas específicas”

5.3.4 Página WEB

La implementación de la página WEB en el sistema involucra 2 partes:

- Almacenamiento de la página WEB en la EEPROM
- Implementación del servidor HTTP

Con respecto al almacenamiento de la página WEB en la EEPROM, se utilizó el sistema de archivos de `Modtronix` para poder guardar los archivos. En la Tabla 5.2 se muestra los archivos creados para la construcción de la página WEB. Estos

archivos por medio de un programa en la PC se compilaron en un archivo llamado `default.img`, el cual es descargado a la EEPROM con la Terminal (usando el protocolo de transferencia de archivos `xmodem`). Este archivo conocido como imagen es interpretado por el microcontrolador. En la Figura 5.15 se muestra la página WEB de inicio del sistema.

Tabla 5.2 Descripción de los archivos que conforman la página WEB

Archivo	Descripción
`65ec303.js`	Archivo que extiende las capacidades del lenguaje HTML, en el cual los archivos .cgi invocan a una función contenida en este archivo. Dentro de cada función se puede escribir el contenido de la página
`xuser.cgi`	Página para cambio de usuario y contraseña del usuario administrador
`login.cgi`	Página de registro del usuario administrador
`xiocfg.cgi`	Página para cambiar el estado de los relevadores
`xioval.cgi`	Página para ver el estado de las puertas y el flujo de aire
`xucfg.cgi`	Página para cambiar la velocidad del puerto serie
`intro.htm`	Página de introducción del sistema
`mx.css`	Archivo donde se le da estilo a las páginas WEB del proyecto (color, tipo de fuente, entre otros)
`xscfg.cgi`	Página de configuración del sistema
`xncfg.cgi`	Página de configuración de los parámetros de red y de SNMP
`index.htm`	Página de inicio del sistema (en este se muestra `intro.htm`)
`xtcfg.cgi`	Página de configuración de los parámetros de temperatura
`contact.htm`	Página de información de contacto

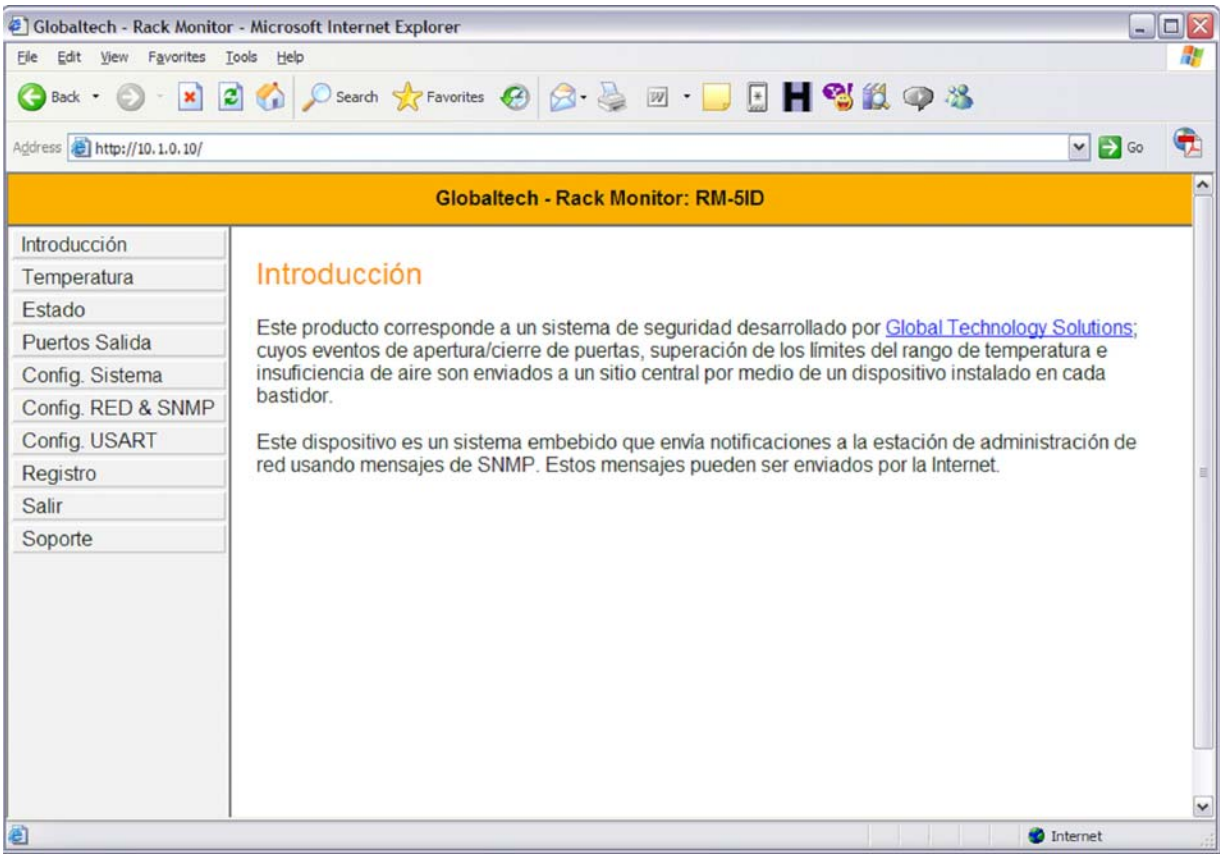


Figura 5.15 Página WEB de inicio del sistema

Con respecto a la implementación del servidor HTTP, el servidor HTTP implementado no cubre todas las funcionalidades de HTTP, más bien corresponde a una implementación mínima por ser un sistema embebido. Las características principales de este servidor:

- Soporta múltiples conexiones HTTP (específicamente 8)
- Soporta que las páginas WEB estén ubicadas en memoria EEPROM
- Contiene un sistema de archivos simple, el cual la imagen tiene que ser creada con un programa de PC
- Soporta el método de HTTP `Get`
- Soporta CGI para el uso de páginas dinámicas

La implementación de este servidor requería incluir el archivo `http.c` en el proyecto de desarrollo del `firmware`. En la parte de aplicación, uno requería implementar los métodos `HTTPGetVar()` y `HTTPExecGetCmd()`. Estos métodos son llamados por el servidor HTTP cuando éste ha recibido un comando de CGI. Cuando se hace referencia al primer método retorna el valor solicitado (por ejemplo, '%T54' que indica que se solicita el valor actual del límite inferior de temperatura). Cuando se hace referencia al segundo método escribe un nuevo valor para ese campo (del ejemplo, 'T54=18' indica que el usuario ha digitado en ese campo un valor de 18, por lo cual éste debe ser guardado). Por tanto, a los parámetros de configuración del proyecto se les asignó un comando de CGI como se muestra en la Tabla 5.3.

Tabla 5.3 Descripción de los comandos de CGI utilizados en el proyecto

Comando	Descripción
a	Estado de algún pin del puerto A del microcontrolador Por ejemplo: %a2, consulta el pin 2 del puerto A
b	Estado de algún pin del puerto B del microcontrolador Por ejemplo: %b1, consulta el pin 1 del puerto B
k	Parámetros de configuración de red Por ejemplo, %k00, consulta el primer octeto de la dirección IP
l	Parámetros de usuario y contraseña
m	Comandos para restaurar el sistema y salir de la sesión
T	Parámetros de temperatura
S	Parámetros de la dirección IP de la estación de administración de red
C	Parámetro de la comunidad de SNMP
U	Parámetro de la ubicación
R	Estado de los relevadores
F	Estado de las banderas de desactivación de las notificaciones y alarma
P	Configuración de los periodos de notificación y de inactividad de la sesión de administrador

5.3.5 SNMP

El módulo de “SNMP” se constituye de un método llamado `EnviarTRAP(int CODIGO_TRAP).` El módulo de “Tareas específicas” cuando detecta un evento al cual hay que notificar (se abre alguna puerta, la temperatura supera el rango establecido o cuando no hay presencia de flujo de aire.), hace un llamado a este método. Según el parámetro de código, envía el mensaje correspondiente. En la Tabla 5.4 se muestran los mensajes que se envían según su código. Además, se muestra el número de puerto fuente de UDP utilizados en cada mensaje. Estos puertos están dentro del rango de uso libre, según el IANA [8]. Los mensajes se construyen con el puerto destino de UDP 162, el cual es reservado para el uso de `traps` de SNMP según el IANA [8]. El campo dentro del mensaje que dice “Ubicación” es configurable con el fin de que se identifique más rápido de dónde proviene el mensaje cuando se observan en la estación de administración de red.

Tabla 5.4 Mensajes de las notificaciones de SNMP que envía el sistema

Código	Número de puerto UDP fuente	Mensaje
1	45001	“Ubicación: Pta Frontal Abierta”
2	45002	“Ubicación: Pta Trasera Abierta”
3	45003	“Ubicación: Pta Izquierda Abierta”
4	45004	“Ubicación: Pta Derecha Abierta”
5	45005	“Ubicación: No hay flujo de aire”
6	45006	“Ubicación: Temperatura fuera de rango”

Estos mensajes de notificación de SNMP respetan la convención establecida para la definición de `traps` del RFC 1215 [15]. En la Figura 5.16 y en la Figura 5.17 se muestra el diagrama de flujo de cómo se construyeron los mensajes de notificación de SNMP. En la Figura 5.18 se muestra la estructura de la información de administración implementada en el sistema.

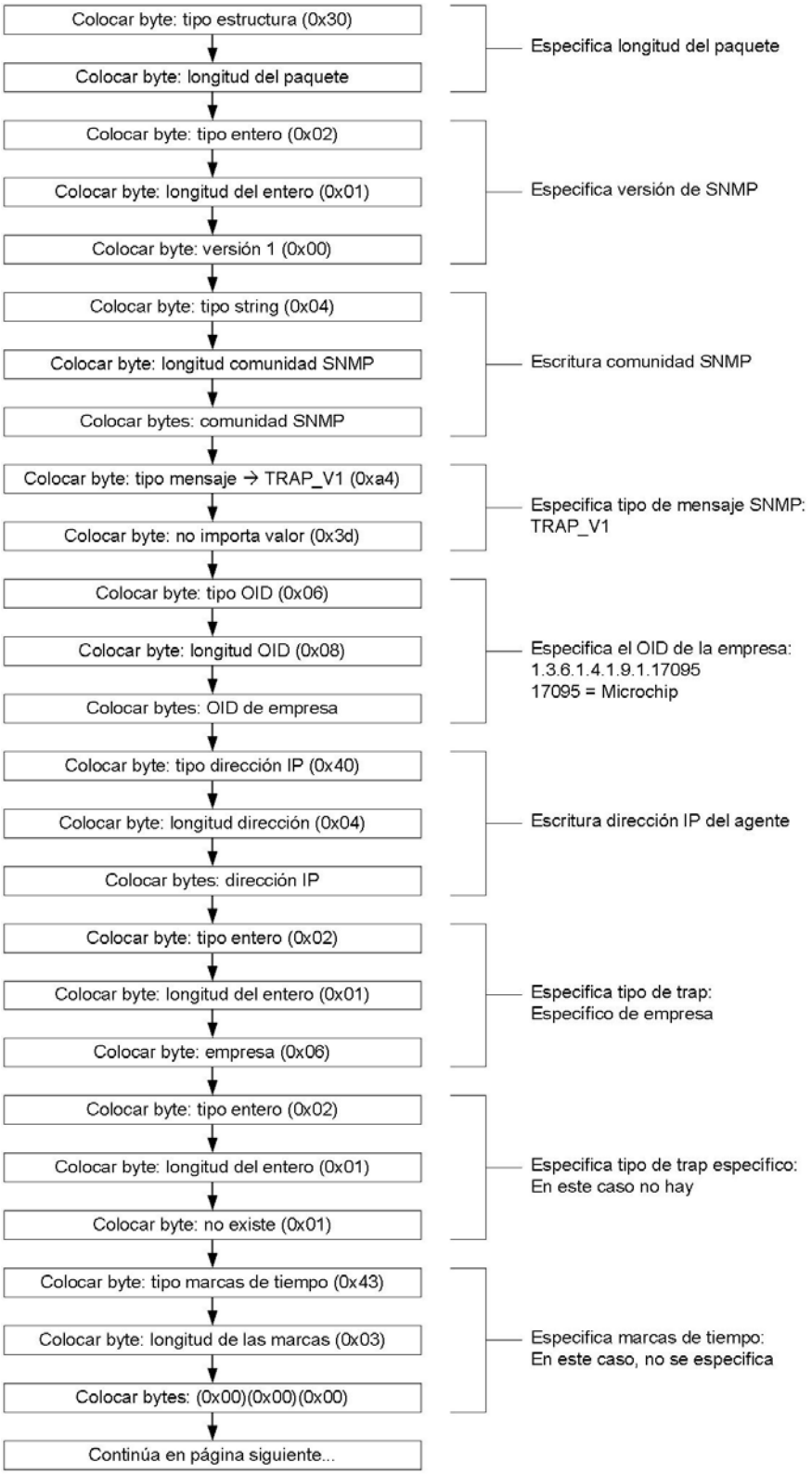


Figura 5.16 Diagrama de flujo de la construcción de un paquete de notificación de SNMP (I)

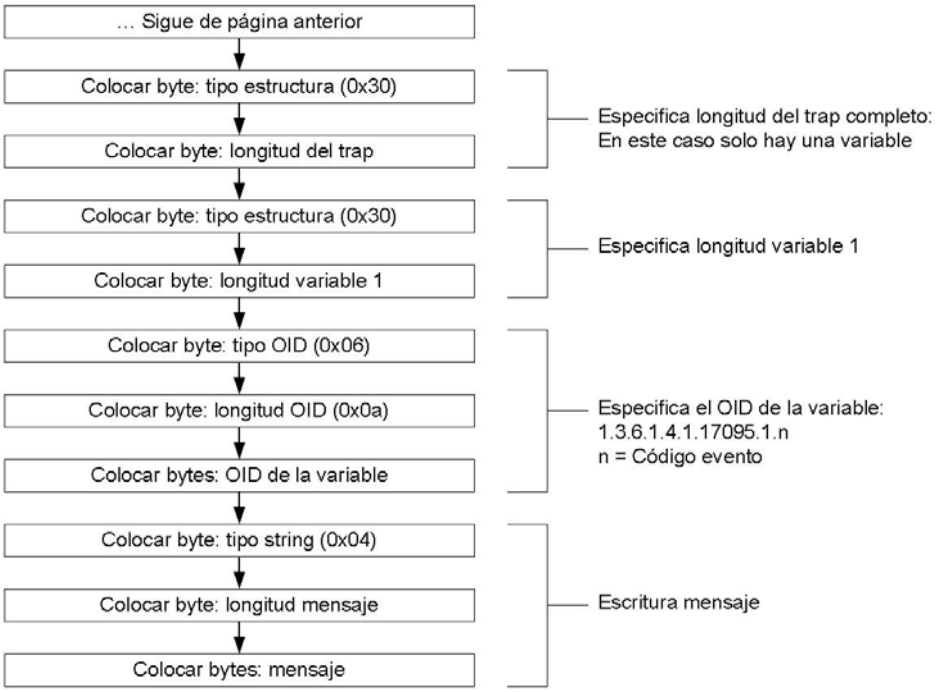


Figura 5.17 Diagrama de flujo de la construcción de un paquete de notificación de SNMP (II)

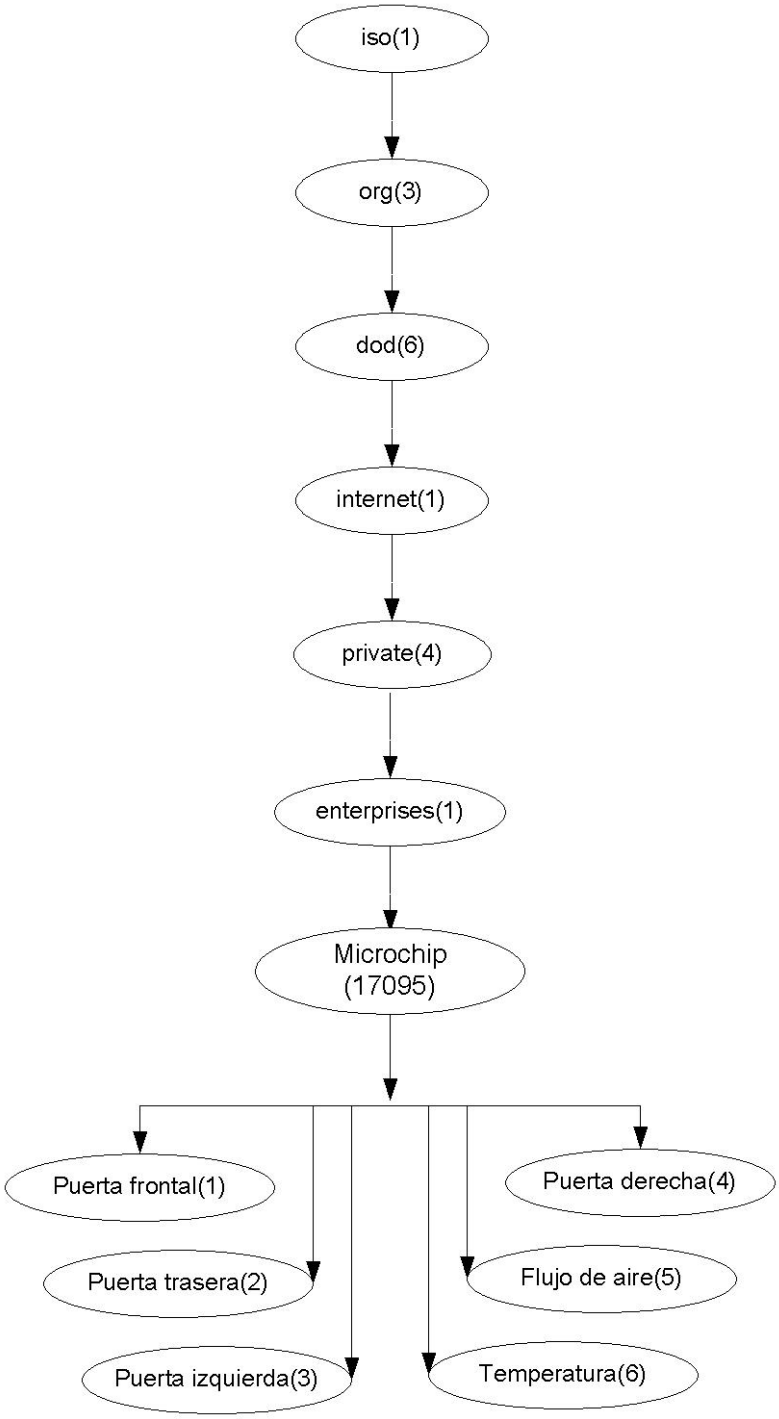


Figura 5.18 Estructura de la información de administración implementada en el sistema

5.3.6 ARP & ICMP

Este módulo consta de dos componentes del conjunto de protocolos de TCP/IP:

- ARP: Se encarga de que el sistema se pueda comunicar con otras estaciones dentro de la red LAN. Si el sistema desconoce la dirección MAC dada una dirección IP conocida, este módulo realiza una solicitud de ARP. Por ejemplo, si el sistema tiene que enviar los paquetes de SNMP y la estación de administración de red se encuentra en otra red, el módulo se ocupa de encontrar la dirección MAC de la puerta de enlace predeterminada. Además, si alguna estación no conoce la dirección MAC del sistema, dicha estación hará una solicitud de ARP y este módulo se encargará de responder.
- ICMP: Se encarga de responder las solicitudes de `ping` de cualquier estación para verificar su conectividad.

Capítulo 6: Análisis de Resultados

En esta sección se muestran los resultados del proyecto con su respectivo análisis. Para observar los resultados, se mostrará paso a paso lo que puede hacer el sistema.

El sistema de seguridad desarrollado se muestra en la Figura 6.1 y en la Figura 6.2. Esto es una demostración ya que los contactos magnéticos no están sujetos a las puertas de un bastidor. No obstante, con sólo quitar un imán se simula que esa puerta ha sido abierta. En estas figuras, se muestra el dispositivo conectado con un cable de red UTP y con el cable de alimentación. En los exteriores, se visualizan los contactos magnéticos (puertas y flujo de aire), el sensor de temperatura y la mini sirena.

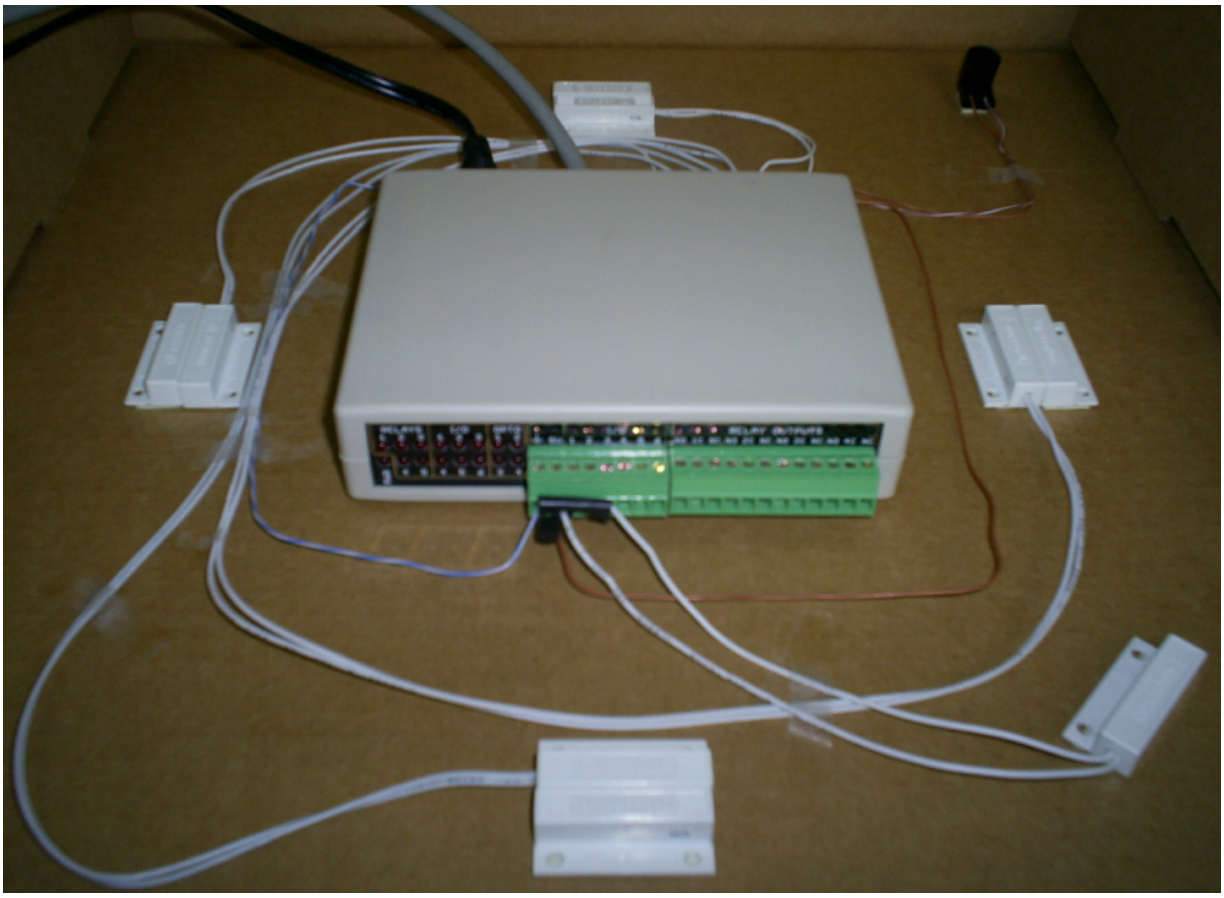


Figura 6.1 Fotografía del sistema de seguridad desarrollado (I)

Figura 6.2 Fotografía del sistema de seguridad desarrollado (II)

La topología de red implementada para la demostración de los resultados se muestra en la Figura 6.3. Esta topología simula el ambiente típico donde se instala cada sistema de seguridad, ya que el sistema ("`RM-5ID`") se le configura una dirección IP privada. Y por medio de una estrategia de traducción de direcciones (NAT) en el dispositivo de comunicación (ya sea enrutador, `firewall`, entre otros), el sistema es localizado desde afuera (SINPE ó Internet) por la dirección IP pública asignada.

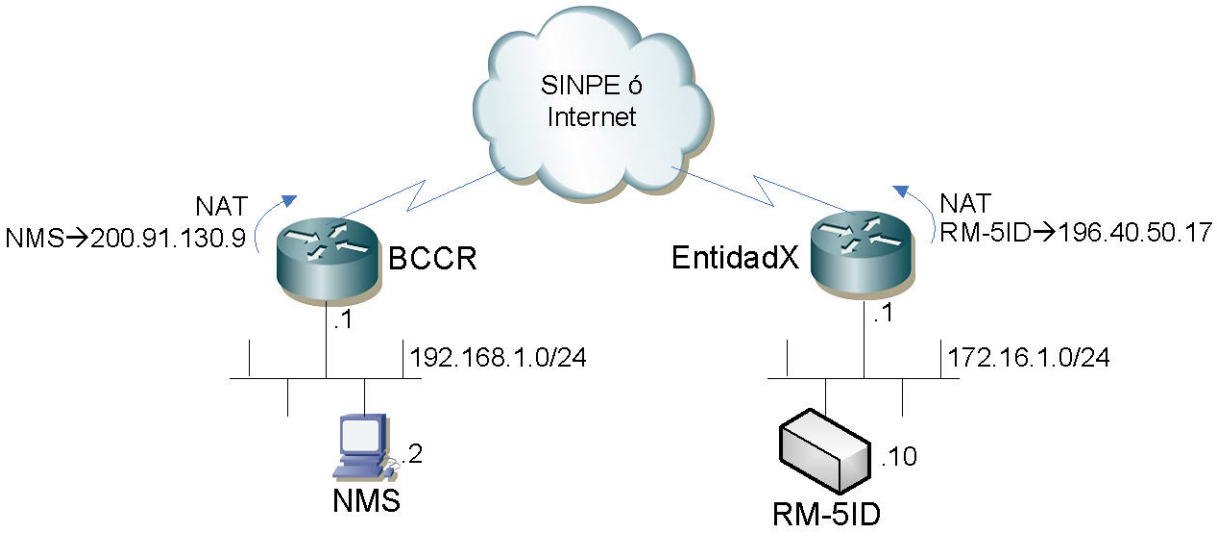


Figura 6.3 Topología de red implementada para la demostración de los resultados

6.1 Configuración inicial del sistema

En un inicio, el sistema tiene parámetros de red y de SNMP asignados por defecto (cuando es la primera vez que se pretende configurar el sistema). Estos parámetros por defecto se resumen en la Tabla 6.1. Es importante destacar que todos los cambios de configuración que se realizan se guardan en la memoria EEPROM del microcontrolador, y en dado caso que el sistema se reinicie carga la última configuración.

Tabla 6.1 Parámetros de red y de SNMP asignados por defecto

Parámetro	**Valor**
Dirección IP	10.1.0.10
Máscara de subred	255.255.255.0
Puerta de enlace predeterminada	10.1.0.1
Dirección IP de NMS	10.1.0.16
Comunidad SNMP	Public

Para iniciar la configuración del sistema, se puede optar por dos opciones:

- Configuración por consola
- Configuración por página WEB

En el caso de configuración por consola, hay que tener la Terminal de consola preparada con los parámetros del puerto serie que se muestran en la Tabla 6.2.

Tabla 6.2 Parámetros del puerto serie para configurar por consola el sistema

Parámetro	**Valor**
Bits por segundo	57600
Bits de datos	8
Paridad	Ninguna
Bits de parada	1
Control de flujo	Ninguno

Una vez conectado la Terminal, se procede a restaurar el sistema (desconectando y luego conectando la alimentación eléctrica) y en la Terminal aparece el mensaje que se muestra en la Figura 6.4. Si en 2 segundos (valor por defecto, este intervalo se puede cambiar en la “Configuración del sistema” de la página WEB) no se presiona cualquier tecla, la aplicación principal se ejecuta. En caso de presionar cualquier tecla antes de que caduque ese tiempo, se muestra el menú de Terminal (ver Figura 6.5).

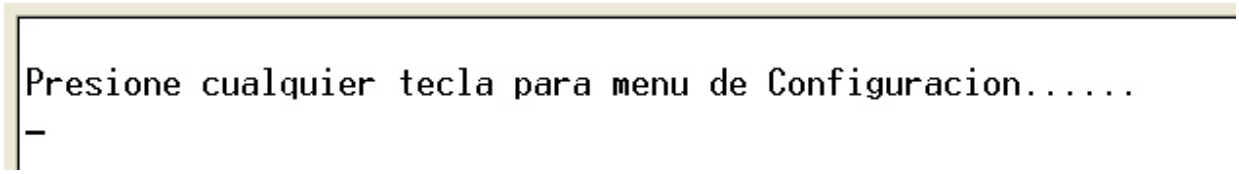


Figura 6.4 Mensaje de consola mostrado al instante de restaurar el sistema

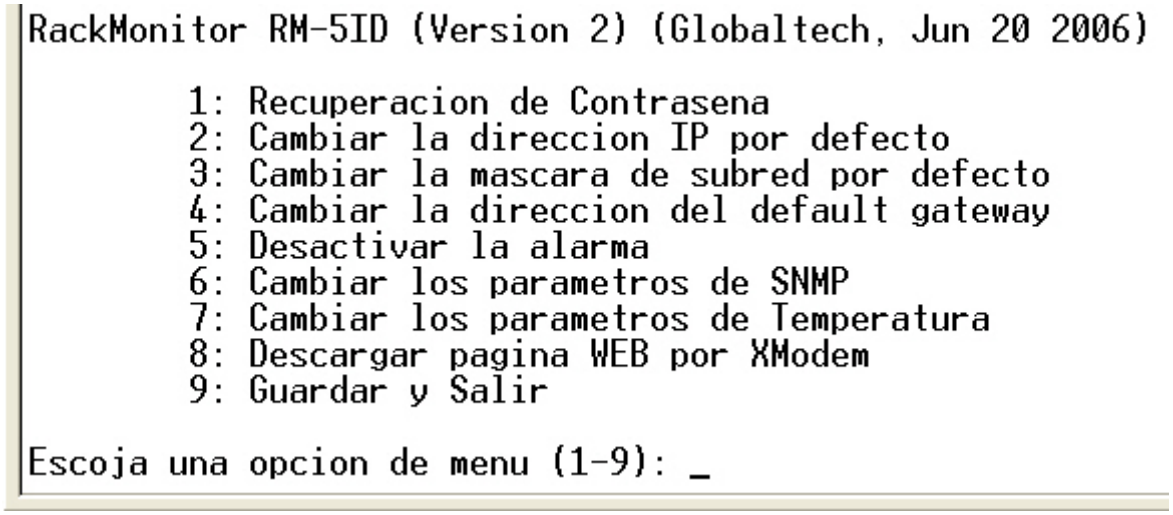


Figura 6.5 Menú de Terminal del sistema

Ahora se procede a cambiar los parámetros de red y de SNMP desde la consola. En la Figura 6.6 se muestra la captura de texto de los cambios realizados. Nótese que para efectos de documentación, en estos cambios se omite la salida correspondiente al menú (ver Figura 6.5). Cuando en la consola aparece el mensaje de “Entrada inválida recibida…” se debe a que no se digitó correctamente lo que se pedía. Por ejemplo, si hay que poner la dirección IP y si se digita incorrectamente ó si se presiona la tecla `Enter` sin haber digitado algo, aparece dicho mensaje. Además,

el sistema ignora esa entrada. Para que el sistema se ponga en marcha, se debe presionar la opción 9 (“Guardar y salir”), y luego aparece un mensaje que informa que la aplicación se está ejecutando.

```
RackMonitor RM-5ID (Version 2) (Globaltech, Jun 20 2006)
!---Salida omitida para la documentación (menú)
La direccion IP por defecto (10.1.0.10): 172.16.1.10

RackMonitor RM-5ID (Version 2) (Globaltech, Jun 20 2006)
!---Salida omitida para la documentación (menú)
La direccion IP por defecto (172.16.1.10):
Entrada invalida recibida - Entrada ignorada.
Presiones cualquier tecla para continuar...

RackMonitor RM-5ID (Version 2) (Globaltech, Jun 20 2006)
!---Salida omitida para la documentación (menú)
La mascara de subred por defecto (255.255.255.0):
Entrada invalida recibida - Entrada ignorada.
Presiones cualquier tecla para continuar...

RackMonitor RM-5ID (Version 2) (Globaltech, Jun 20 2006)
!---Salida omitida para la documentación (menú)
La direccion del default gateway (10.1.0.1): 172.16.1.1

RackMonitor RM-5ID (Version 2) (Globaltech, Jun 20 2006)
!---Salida omitida para la documentación (menú)
Digite la comunidad SNMP (SINP3): public
Digite la direccion IP de la estacion SNMP (10.1.0.16): 200.91.130.9

RackMonitor RM-5ID (Version 2) (Globaltech, Jun 20 2006)
!---Salida omitida para la documentación (menú)
La aplicacion se esta ejecutando...
```

Figura 6.6 Cambios de configuración por consola

En caso de que se quisiera configurar inicialmente el dispositivo por página WEB, la estación que utilizaría el explorador de Internet tiene que estar en el mismo segmento de red donde está el sistema. Además, a esta estación hay que configurarle una dirección IP estática perteneciente a la red 10.1.0.0/24, y que no sea la dirección IP del sistema (10.1.0.10/24). Luego, en la barra de direcciones del explorador se procede a digitar la dirección IP del sistema. Para más información de cómo hacer configuraciones en la página WEB, refiérase a la sección 6.3.

6.2 Notificaciones de SNMP

Las notificaciones de SNMP se pueden mostrar en la estación de administración de red (NMS). En este caso, se empleó el programa `WhatsUp Gold®` [10] versión 8.0.3 para ejecutar el servidor de `trap` de SNMP. En este programa, se puede mostrar el registro de notificaciones que se han enviado (ver Figura 6.7).

En ese registro se muestran cada uno de los eventos posibles. Es importante destacar que el sistema indica en los mensajes de donde proviene la notificación. Esto tiene la ventaja de que los administradores de la plataforma SINPE eviten tener una tabla de direcciones IP con la respectiva ubicación para descifrar cual sistema lo envía. En la página WEB hay un campo de texto donde se puede especificar la ubicación del sistema (refiérase a la sección 6.3). Del registro mostrado se observa en los dos mensajes más antiguos (los dos de abajo hacia arriba), que el sistema instalado en la “EntidadX” notifica que la puerta izquierda y la trasera se han abierto. Luego aparecen más mensajes que provienen desde “BP-SanJose”. Si se observan los mensajes, estos provienen de la misma dirección IP pública. Lo que sucedió, es que se modificó el campo de ubicación.

En la Figura 6.8 se muestra una captura de un mensaje con el analizador de protocolos `Ethereal` [7] donde se examina el cuerpo de la notificación. Y en la Figura 6.9, se muestra el mismo mensaje pero con la aplicación `WhatsUp Gold®`.

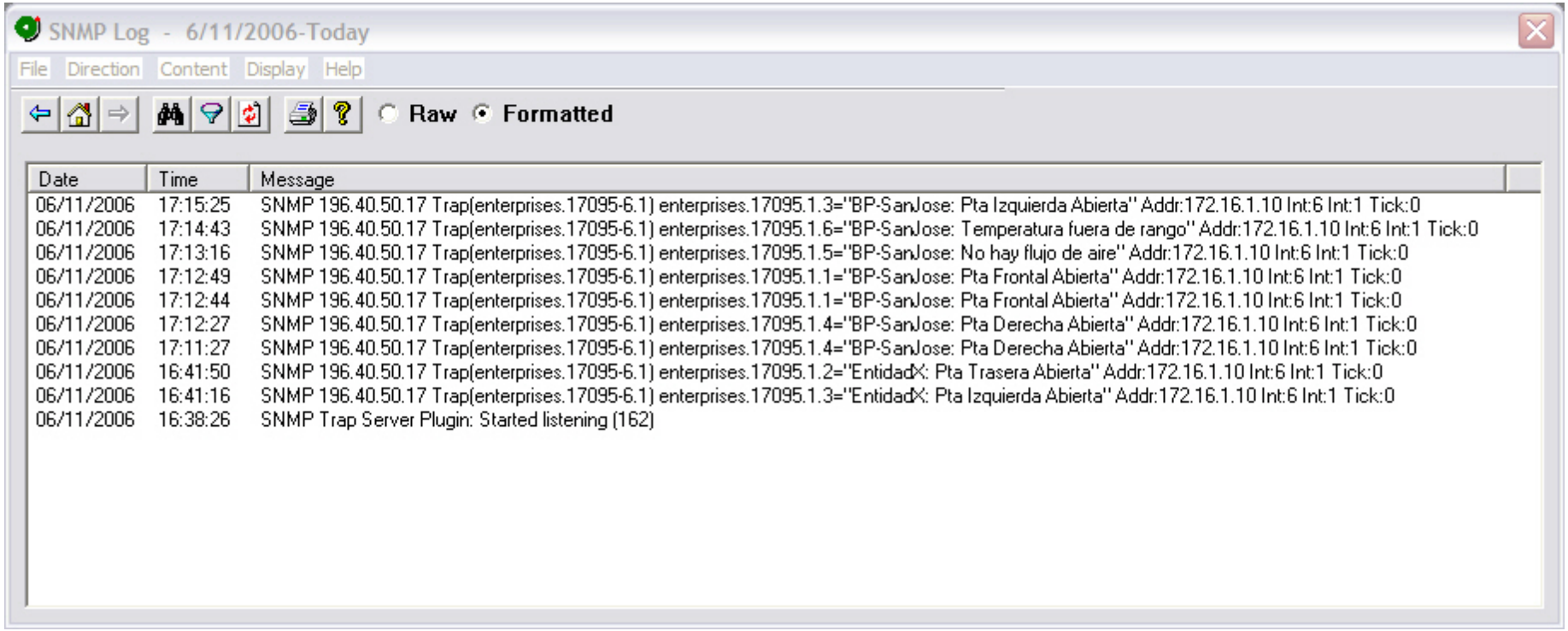


Figura 6.7 Registro de notificaciones SNMP en la estación de administración de red

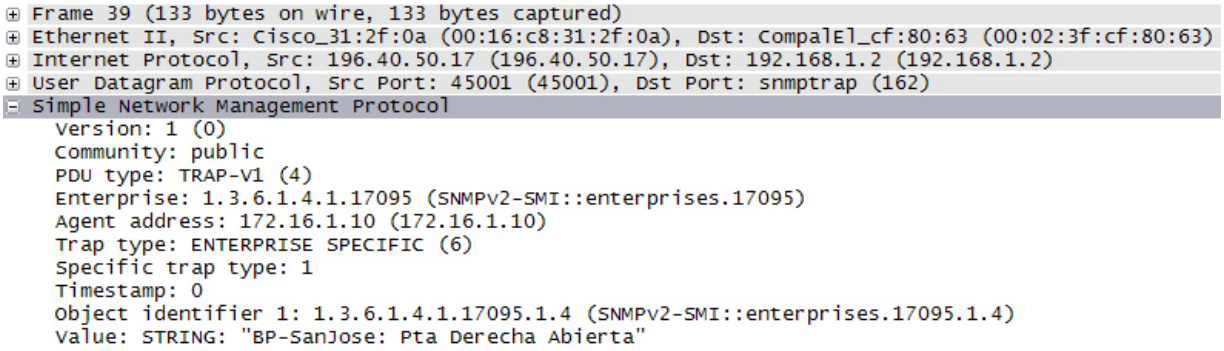


Figura 6.8 Notificación de SNMP capturada con el analizador de protocolos: Ethereal

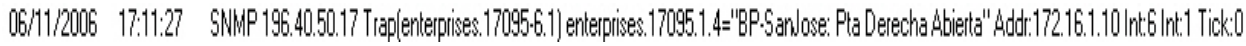


Figura 6.9 Notificación de SNMP extraída de la aplicación WhatsUp Gold

Al examinar el mensaje capturado con el `Ethereal`, se puede extraer que es una notificación de SNMP de versión 1, con la comunidad “public”, cuyo OID de empresa es 1.3.6.1.4.1.17095, la dirección IP del agente es 172.16.1.10, el código de la notificación es específico de la empresa, no hay marca de tiempo especificada, y solo hay una variable dentro de la notificación cuyo OID es 1.3.6.1.4.1.17095.1.4 y cuyo valor es “BP-SanJose: Pta Derecha Abierta”. Además, este paquete proviene de una dirección IP pública 196.40.50.17. Resulta que si se observa la información desde `WhatsUp Gold`®, no se muestra la comunidad SNMP; lo demás si aparece.

Del registro de notificaciones de SNMP de la Figura 6.7, se observa que el mensaje de puerta derecha abierta aparece dos veces con un minuto de diferencia. El sistema tiene la característica de que si la puerta permanece abierta se envía un mensaje cada minuto (valor por defecto, pero puede ser configurable por la página WEB). Ahora observe los dos mensajes de puerta frontal abierta. Este mensaje no se le ha cambiado el periodo de un minuto, y aparece el mismo mensaje después de 5 segundos. Cuando sucede esto, es que la puerta se ha abierto una vez, se cerró y se volvió abrir.

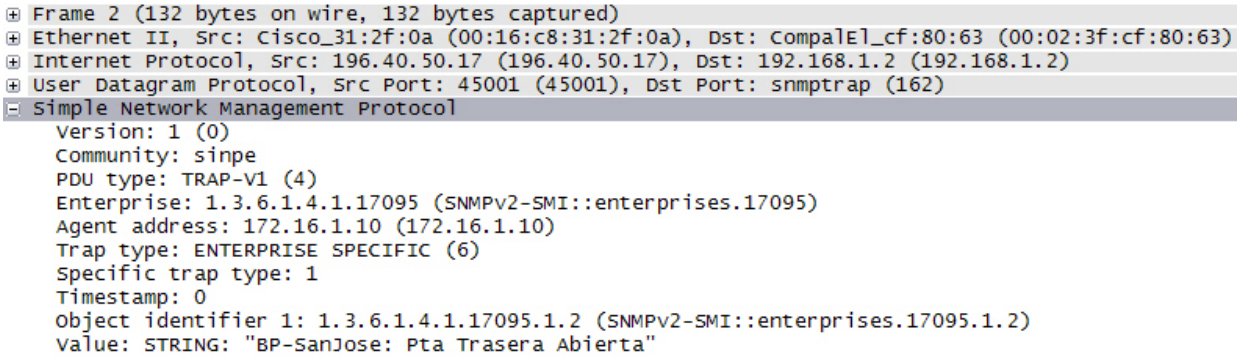


Figura 6.10 Notificación de SNMP capturada con el analizador de protocolos: Ethereal

En la Figura 6.10 se observa que se envía una notificación donde la comunidad SNMP ha cambiado a “sinpe”. Este cambio se pudo haber realizado desde la consola o por la página WEB.

6.3 Página WEB

En la Figura 6.11 se muestra la página de inicio del sistema. Note que esta página es desplegada desde la estación de administración de red (se abre la página cuyo servidor WEB tiene la dirección IP pública 196.40.50.17). La página se compone de un marco externo estático donde aparece el título (parte superior) y el menú (parte izquierda), y de un marco interno donde se muestran la página de cada sección. Por ejemplo, si se presiona el botón de menú de “Registro” aparece la página de la Figura 6.12. Con estas figuras se pueden comparar para notar lo que cambia (marco interno). Es importante destacar que si usted presiona los botones “Temperatura”, “Estado”, “Puertos Salida”, “Config. Sistema”, “Config. RED & SNMP”, “Config. USART”, no se puede mostrar estas secciones hasta que el usuario se haya registrado con privilegios de administrador. Esto es un punto favorable de seguridad porque si se permitiera a estas secciones el ingreso a cualquiera puede alterar el funcionamiento del sistema cambiando sus parámetros. Si el usuario no se ha registrado, aparece la página de la Figura 6.12. Las páginas que se pueden ver sin haberse registrado son “Introducción”, “Registro”, “Salir” y “Soporte”. El marco interno de la página de “Soporte” es la que se muestra en la Figura 6.13.

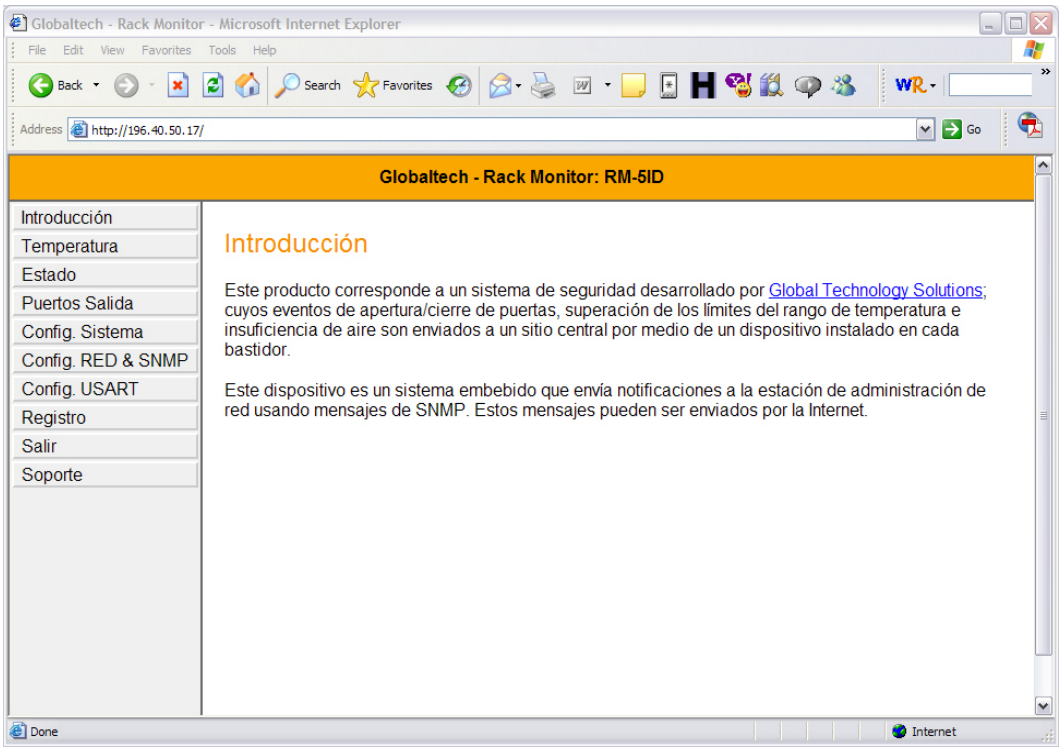


Figura 6.11 Página WEB de inicio

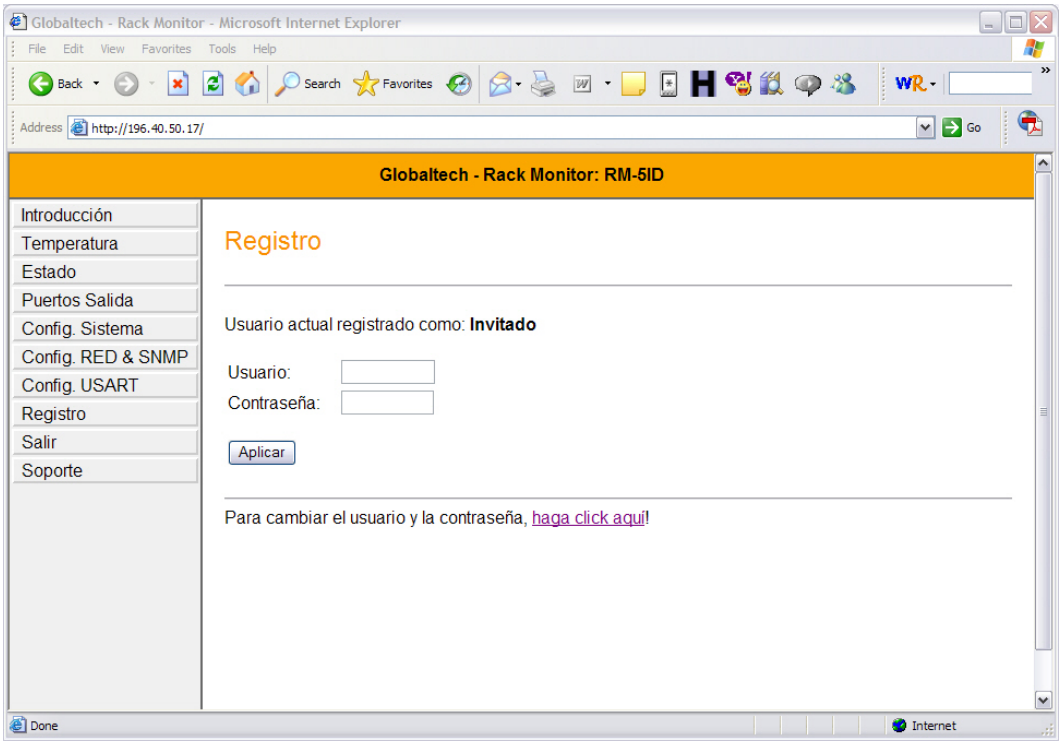


Figura 6.12 Página WEB de registro

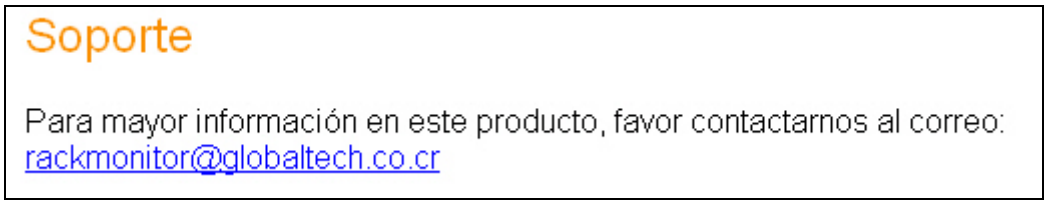


Figura 6.13 Marco interno de la página WEB de soporte

Cuando un usuario se ha registrado correctamente, la página de “Registro” se muestra como en la Figura 6.14. En este caso, el usuario es “admin” (usuario por defecto). No obstante este usuario por seguridad se puede cambiar. Para poder cambiar el usuario y la contraseña, el usuario tiene que estar registrado. En la Figura 6.15 se muestra la página de “Cambio de usuario y contraseña”. En esta página hay que ingresar el nuevo usuario y la nueva contraseña dos veces (para evitar errores de escritura del humano). En esta figura se muestra que el nuevo usuario ya cambiado es “juan”.

Figura 6.14 Marco interno de la página WEB de registro, cuando un usuario se ha registrado

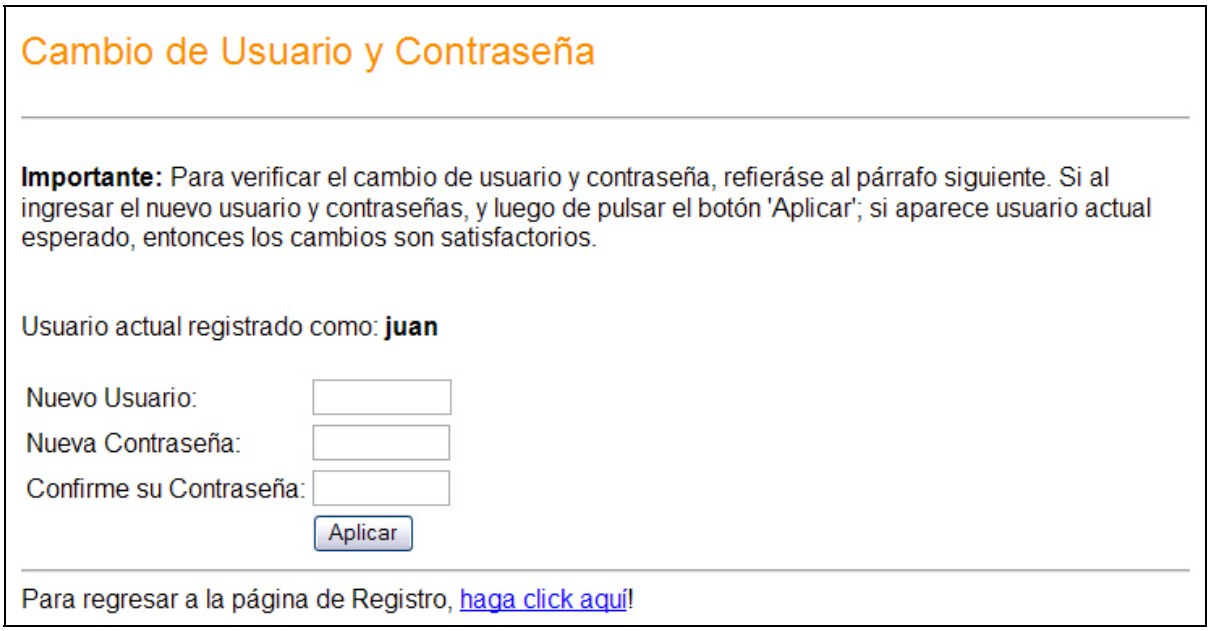


Figura 6.15 Marco interno de la página WEB de cambio de usuario y contraseña

Una vez registrado el usuario, se pueden ver las demás páginas. En la Figura 6.16 se muestra el marco interno de la página WEB de “Temperatura”. En esta página se muestra la temperatura actual y los campos de texto para modificar el rango de temperatura. Esta página se refresca automáticamente cada 30 segundos.

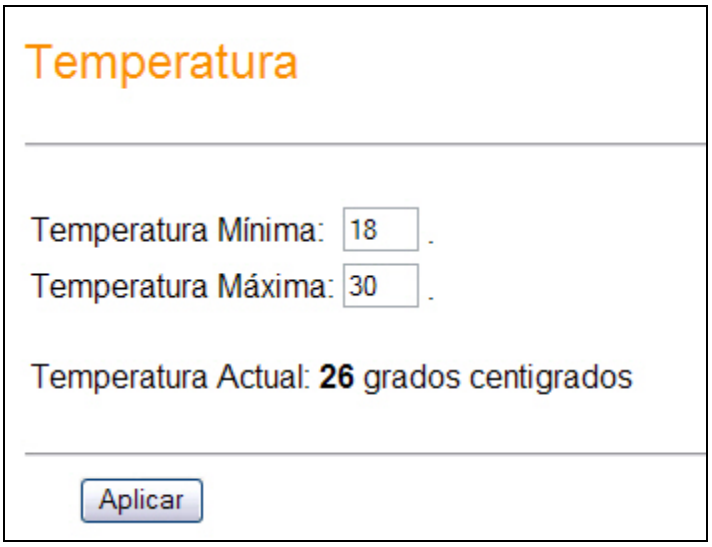


Figura 6.16 Marco interno de la página WEB de temperatura

En la Figura 6.17 se muestra la página WEB de “Estado”, el cual se encarga de mostrar el estado de las puertas y el flujo de aire. Esta página se refresca automáticamente cada 10 segundos.

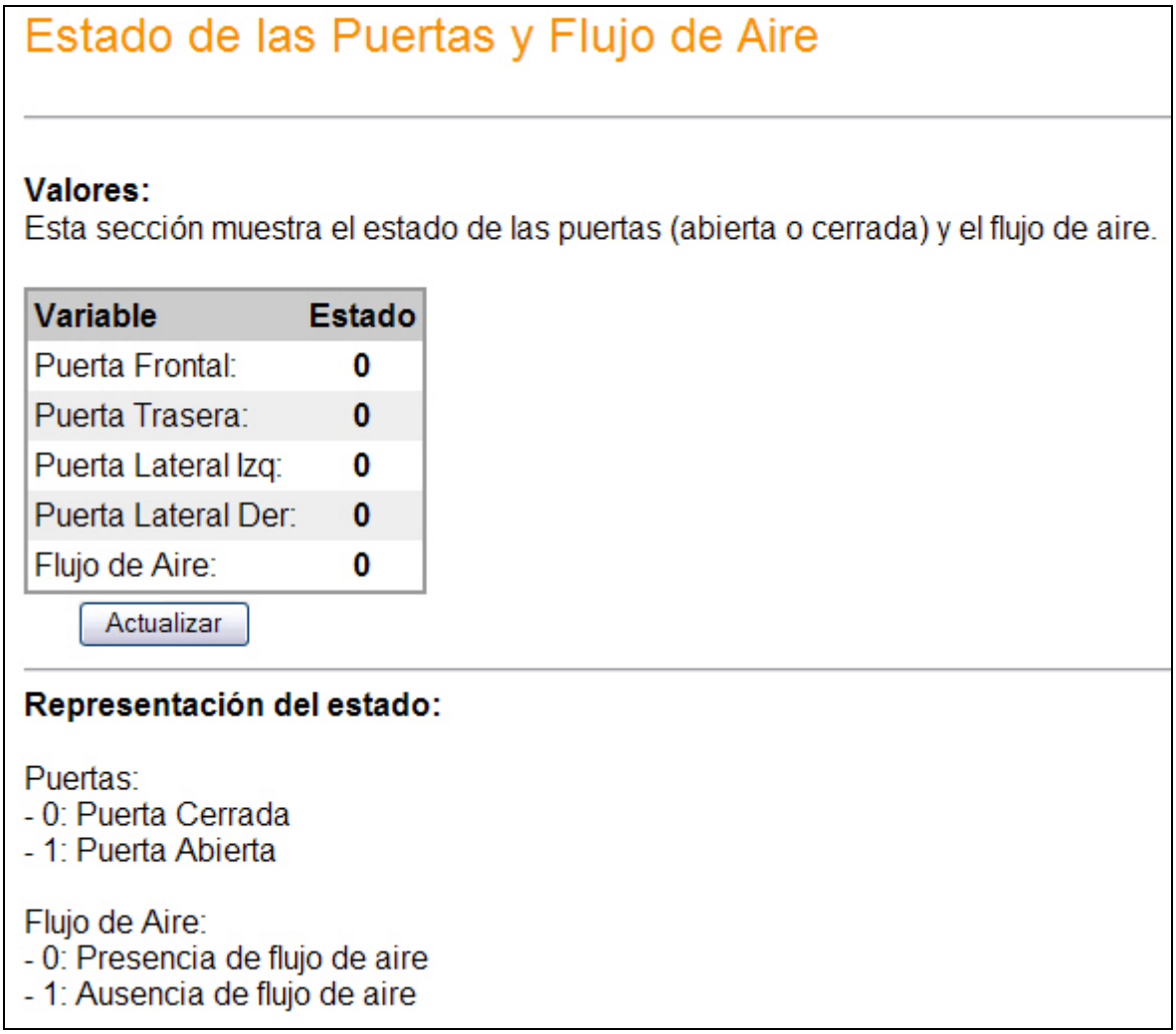


Figura 6.17 Marco interno de la página WEB de estado de las puertas y flujo de aire

En la Figura 6.18 se muestra la página WEB de “Puertos Salida”, el cual se encarga de cerrar o abrir el interruptor de los 4 relevadores disponibles en el chasis IOR5E. En esta página WEB se visualiza que los relevadores 2 y 4 están encendidos, y esta configuración se refleja en los LED del chasis IOR5E (ver Figura 6.19).

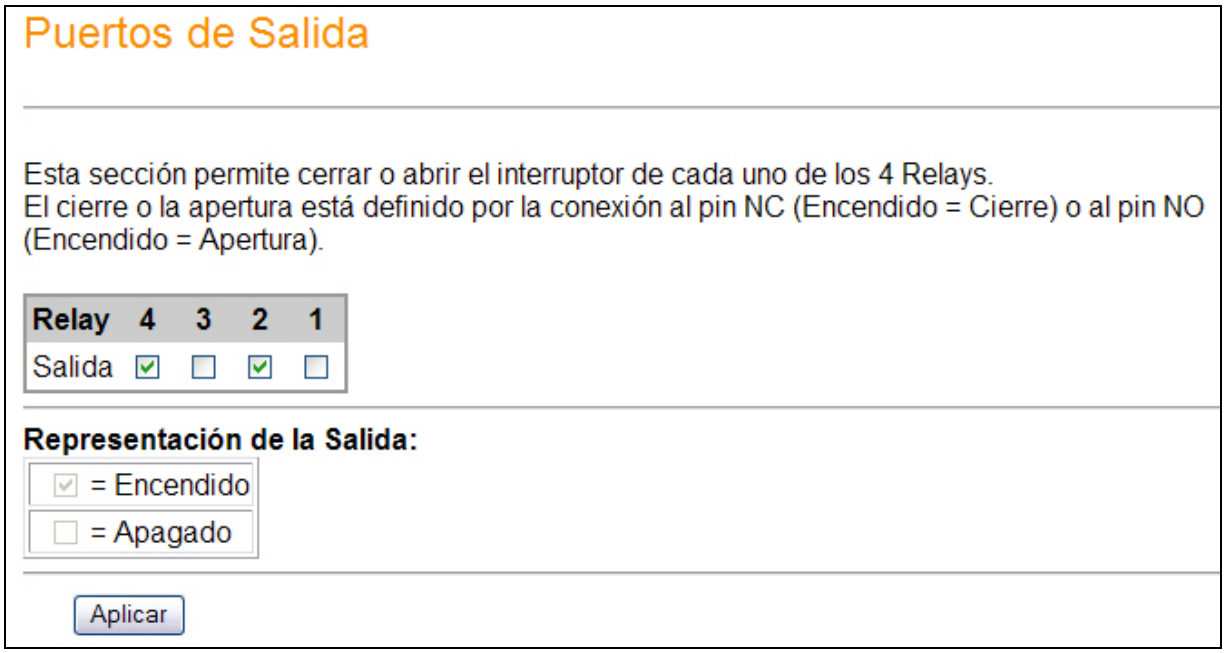


Figura 6.18 Marco interno de la página WEB de puertos de salida

Figura 6.19 Demostración de los relevadores 2 y 4 encendidos con los LED del chasis IOR5E

En la Figura 6.20 se muestra la página WEB donde se configura el sistema. En esta página se puede configurar lo siguiente:

- Retardo al inicio de la Terminal: Se puede configurar el intervalo para ingresar a la consola del sistema
- Desactivación de las notificaciones y la mini sirena: Se puede deshabilitar al sistema del envío de alguna notificación en particular debido a mantenimiento. Por ejemplo, si es sabido que el contacto magnético de la puerta derecha se ha dañado y para no estar recibiendo notificaciones de un evento que ya es conocida su causa, entonces se puede deshabilitar ese envío. Lo mismo

sucede con la mini sirena, en caso de que se le vaya a dar un mantenimiento a algunos de los equipos de ese bastidor, se puede deshabilitar la alarma.

- Periodos de las notificaciones: Se puede configurar el periodo de envío de notificaciones cuando el evento generado permanece en el mismo estado. Por ejemplo, si alguna puerta permanece aún abierta en ese periodo, se procede al envío de la notificación otra vez. Por defecto, los periodos son de 60 segundos.
- Tiempo de desactivación automática de la alarma: Cuando la alarma suena es porque alguna puerta se ha abierto, y se puede configurar el tiempo en que la alarma sigue sonando después de estar cerradas todas las puertas. Por defecto, este tiempo es de 60 segundos.
- Tiempo de expiración de la sesión administrador: Cuando el servidor HTTP deja de percibir tráfico por este tiempo configurado, la sesión de administrador expira. Y por ende, si se desea realizar un cambio de configuración hay que registrase de nuevo. Esto es un punto favorable de seguridad porque si el administrador deja la sesión abierta y dicha persona se retira, podría llegar otra persona que aún así, esta persona no podría hacerle cambios al sistema. Por defecto, este tiempo es de 120 segundos.

En la Figura 6.21 se muestra la página WEB de “Configuración RED & SNMP”. En esta página se puede modificar los parámetros TCP/IP del sistema, así como los parámetros de SNMP. Para reflejar los cambios en el sistema (excepto comunidad SNMP y ubicación) se debe presionar el botón “Aplicar” y luego “Resetear dispositivo”.

En la Figura 6.22 se muestra la página WEB de “Configuración USART”. En esta página se puede cambiar la tasa de bits por segundo de la consola. Por defecto, el valor es de 57600 bits por segundo.

Por último si el usuario está registrado y desea salir de la sesión, la persona debe presionar el botón de menú “Salir”. Luego, aparece la página de “Registro”.

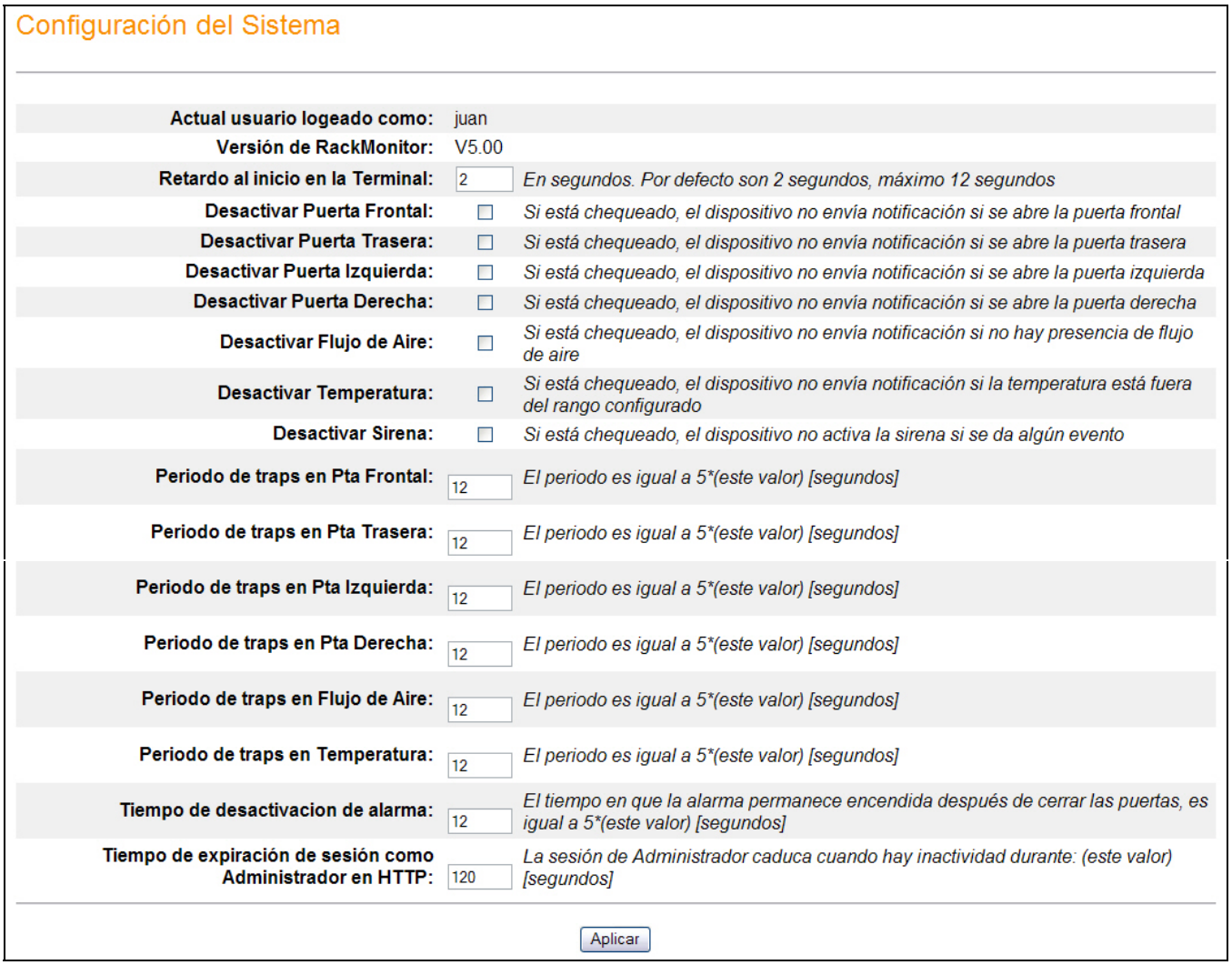


Figura 6.20 Marco interno de la página WEB de configuración del sistema

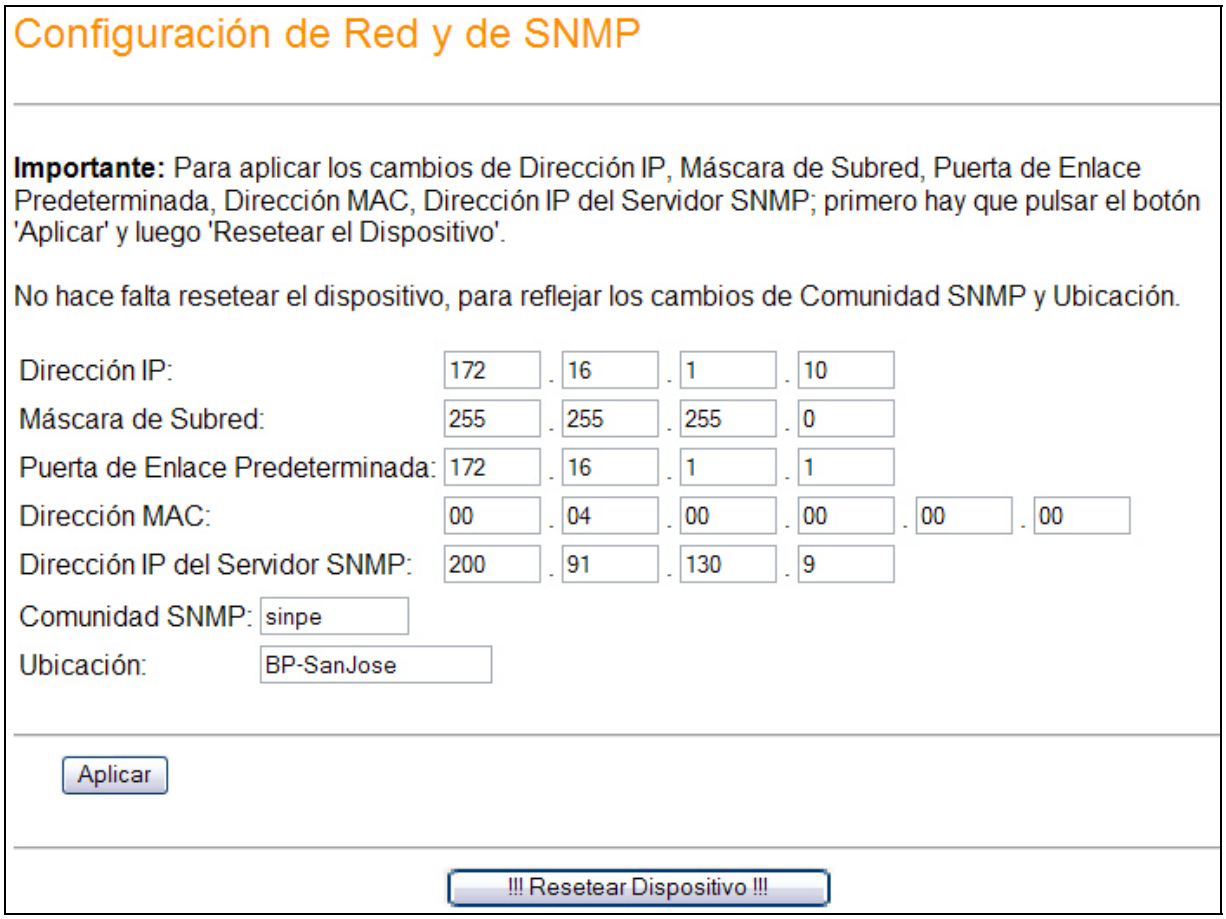


Figura 6.21 Marco interno de la página WEB de configuración de red y de SNMP

Figura 6.22 Marco interno de la página WEB de configuración del puerto serie

Para verificar el funcionamiento del servidor WEB implementado en el sistema se muestran a continuación las capturas de los paquetes con el analizador de protocolos `Ethereal` de la consulta de la página WEB de “Temperatura”. En la Figura 6.23 se muestra que la estación cliente pide una solicitud al servidor WEB (con el comando de HTTP `Get`) de la página que está contenida en el archivo `xtcfg.cgi`. El servidor responde con el archivo solicitado. Este archivo tiene como propiedades de textura las contenidas en el archivo `mx.css`. Por lo que, la estación cliente solicita al servidor WEB este archivo (ver Figura 6.24). Además, en el contenido del archivo `xtcfg.cgi` se hace un llamado a la función `tcfg()`que está contenida en el archivo `65ec303.js`. Por tanto, la estación cliente también solicita este archivo al servidor WEB, y este último le responde.

```
⊞ Frame 80 (518 bytes on wire, 518 bytes captured)
⊞ Ethernet II, Src: CompalEl_cf:80:63 (00:02:3f:cf:80:63), Dst: Cisco_31:2f:0a (00:16:c8:31:2f:0a)
⊞ Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 196.40.50.17 (196.40.50.17)
⊞ Transmission Control Protocol, Src Port: 3605 (3605), Dst Port: http (80), Seq: 1, Ack: 1, Len: 464
⊟ Hypertext Transfer Protocol
  ⊞ GET /XTCFG.CGI?T54=18&T55=30 HTTP/1.1\r\n
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, applic
    Referer: http://196.40.50.17/xtcfg.cgi\r\n
    Accept-Language: en-us\r\n
    XXXXXXXXXXXXXXX: XXXXXXXXXXXXX\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705; Media Cente
    Host: 196.40.50.17\r\n
    Connection: Keep-Alive\r\n
    \r\n
⊞ Frame 82 (418 bytes on wire, 418 bytes captured)
⊞ Ethernet II, Src: Cisco_31:2f:0a (00:16:c8:31:2f:0a), Dst: CompalEl_cf:80:63 (00:02:3f:cf:80:63)
⊞ Internet Protocol, Src: 196.40.50.17 (196.40.50.17), Dst: 192.168.1.2 (192.168.1.2)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 3605 (3605), Seq: 1, Ack: 465, Len: 364
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.0 200 OK\r\n
    Content-type: text/html\r\n
    \r\n
⊟ Line-based text data: text/html
    <html>
    <head>
    <meta http-equiv="refresh" content="30">
    <link href="mx.css" rel="stylesheet" type="text/css">
    <script type="text/javascript" src="65ec303.js"></script>
    </head>

    <body onLoad="ifrmOl()">
    <script type="text/javascript">
    \t/*tcfg(Tmin,Tmax,Tactual);*/
    \ttcfg(18,30,26);
    </script>
    </body>
    </html>
```

Figura 6.23 Capturas con Ethereal de la conversación de HTTP para la consulta de la página de temperatura (I)

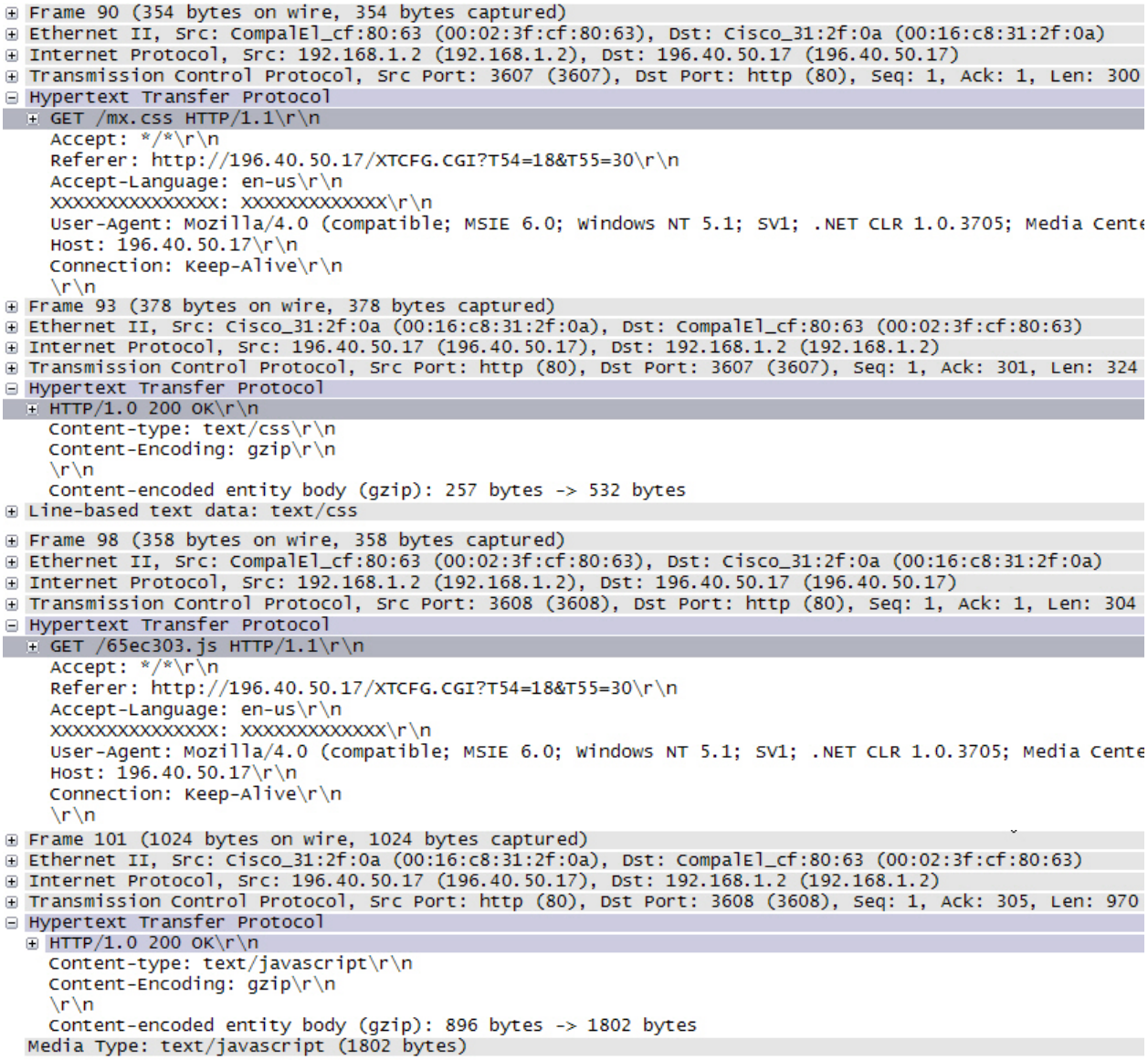


Figura 6.24 Capturas con Ethereal de la conversación de HTTP para la consulta de la página de temperatura (II)

6.4 Módulo ARP & ICMP

En la Figura 6.25 y en la Figura 6.26 se muestran las capturas con el analizador de protocolos `Ethereal` de una solicitud y una respuesta de ARP respectivamente. Esta solicitud la envió el sistema porque necesitaba encontrar la dirección MAC de la puerta de enlace predeterminada (en este caso, el enrutador) para poder enviar las notificaciones de SNMP. La respuesta de ARP mostrada corresponde al paquete enviado por el enrutador.

```
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 172.16.1.10 (00:04:00:00:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 172.16.1.10 (00:04:00:00:00:00)
    Sender IP address: 172.16.1.10 (172.16.1.10)
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 172.16.1.1 (172.16.1.1)
```

Figura 6.25 Captura con Ethereal de una solicitud de ARP

```
⊞ Frame 2 (64 bytes on wire, 64 bytes captured)
⊞ Ethernet II, Src: 172.16.1.1 (00:14:a9:b6:46:f0), Dst: 172.16.1.10 (00:04:00:00:00:00)
⊞ 802.1Q Virtual LAN
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: 172.16.1.1 (00:14:a9:b6:46:f0)
    Sender IP address: 172.16.1.1 (172.16.1.1)
    Target MAC address: 172.16.1.10 (00:04:00:00:00:00)
    Target IP address: 172.16.1.10 (172.16.1.10)
```

Figura 6.26 Captura con Ethereal de una respuesta de ARP

En la Figura 6.28 y en la Figura 6.29 se muestran las capturas con el analizador de protocolos `Ethereal` de una solicitud y una respuesta de ICMP respectivamente. Esta solicitud la envió la estación NMS porque ocupaba verificar la conectividad con el sistema. Esto lo hizo mediante el ping que se muestra en la Figura 6.27. La respuesta de ICMP mostrada corresponde al paquete enviado por el sistema.

```
C:\Documents and Settings\Juan Manuel>ping 196.40.50.17

Pinging 196.40.50.17 with 32 bytes of data:

Reply from 196.40.50.17: bytes=32 time=7ms TTL=98
Reply from 196.40.50.17: bytes=32 time=2ms TTL=98
Reply from 196.40.50.17: bytes=32 time=5ms TTL=98
Reply from 196.40.50.17: bytes=32 time=2ms TTL=98

Ping statistics for 196.40.50.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 7ms, Average = 4ms
```

Figura 6.27 Muestra del resultado de un ping hacia el sistema

```
⊞ Frame 32 (78 bytes on wire, 78 bytes captured)
⊞ Ethernet II, Src: 172.16.1.1 (00:14:a9:b6:46:f0), Dst: 172.16.1.10 (00:04:00:00:00:00)
⊞ 802.1Q Virtual LAN
⊞ Internet Protocol, Src: 200.91.130.9 (200.91.130.9), Dst: 172.16.1.10 (172.16.1.10)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2a5c [correct]
    Identifier: 0x0300
    Sequence number: 0x2000
    Data (32 bytes)
```

Figura 6.28 Captura con Ethereal de una solicitud de ICMP

```
⊞ Frame 33 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: 172.16.1.10 (00:04:00:00:00:00), Dst: 172.16.1.1 (00:14:a9:b6:46:f0)
⊞ Internet Protocol, Src: 172.16.1.10 (172.16.1.10), Dst: 200.91.130.9 (200.91.130.9)
⊟ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x325c [correct]
    Identifier: 0x0300
    Sequence number: 0x2000
    Data (32 bytes)
```

Figura 6.29 Captura con Ethereal de una respuesta de ICMP

6.5 Mediciones del consumo de ancho de banda

Es importante especificar cuánto de ancho de banda se requiere para consultar la página WEB, el envío de notificaciones de SNMP y el envío de paquetes de ICMP. En la Figura 6.30 se muestra un gráfico del ancho de banda medido con la aplicación `BWMeter` [6] cuando se realizó consultas en la página WEB. En este gráfico, se tiene una escala cuyo valor máximo en el eje vertical es de 64kb. Además, se muestra dos ráfagas de tráfico, en el cual el primero (ráfaga izquierda) se aplicó un filtro para medir el tráfico de bajada y el segundo mide el tráfico de subida con

respecto a la estación NMS. Es importante determinar que es suficiente con que se tenga un enlace de 64kbps a nivel WAN para no experimentar atrasos en la descarga de la página WEB. Nótese que se requirió como máximo un 80% de 64kb. Este consumo, es sólo en el instante que se consultan las páginas WEB.

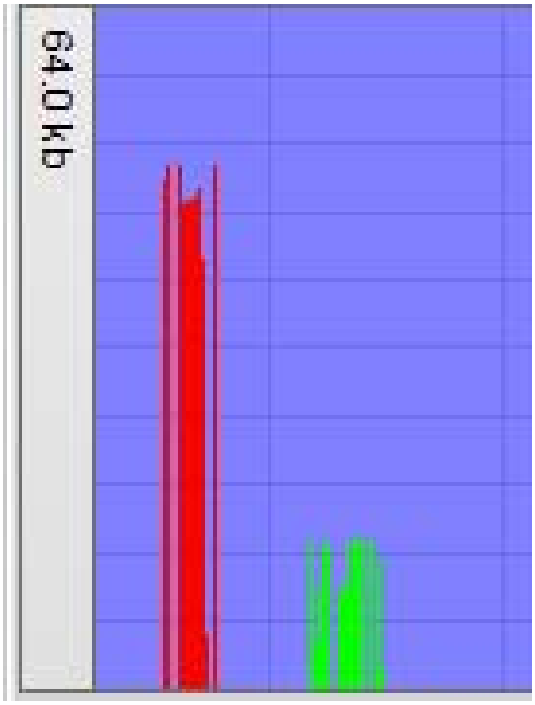


Figura 6.30 Consumo de ancho de banda cuando se consulta las páginas WEB del sistema

En la Figura 6.31 se muestra un gráfico del ancho de cuando se enviaron paquetes de ICMP y SNMP. En este gráfico, se tiene una escala cuyo valor máximo en el eje vertical es de 1kb. Además, se muestra dos ráfagas de tráfico, en el cual el primero (ráfaga izquierda) corresponde a los paquetes de ICMP enviados y el segundo, a los paquetes de SNMP recibidos con respecto a la estación NMS. Es importante determinar que el envío de paquetes ICMP y SNMP por cualquier enlace WAN no afecta el ancho de banda de forma significativa (tanto ICMP como SNMP consumen poco ancho de banda). Nótese que se requirió como máximo de 60% para ICMP y 95% para SNMP de 1kb.

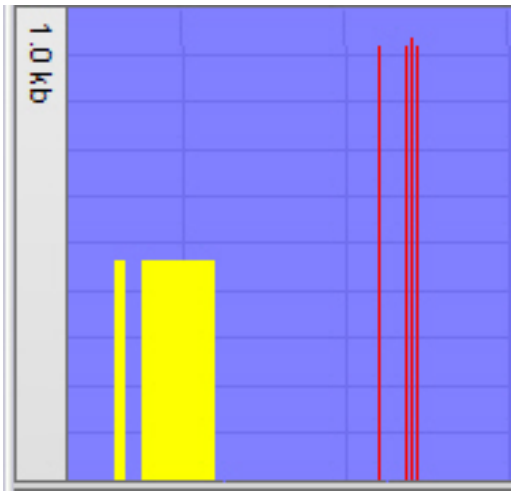


Figura 6.31 Consumo de ancho de banda cuando envían paquetes de ICMP y SNMP

Capítulo 7: Conclusiones y recomendaciones

7.1 Conclusiones

- El sistema desarrollado es capaz de medir la variable de temperatura de cualquier bastidor de comunicaciones de la plataforma SINPE.
- El sistema desarrollado es capaz de detectar la insuficiencia de flujo de aire y apertura de puertas de cualquier bastidor de comunicaciones de la plataforma SINPE.
- El sistema de seguridad desarrollado permite que se notifique los eventos de cambio de estado de las variables, al sitio central de la plataforma SINPE.
- El sistema de seguridad desarrollado es autosuficiente al no requerir de la instalación de algún programa propietario para su configuración.
- La configuración del sistema por página WEB hace que se adapte el producto a los tiempos modernos.
- La aplicación de administración de red no se ve afectado por la cantidad de productos que se puedan instalar, al ser cada sistema independiente.

7.2 Recomendaciones

- Implementar los métodos de SNMP de `Get`, `Get-Next` y `Set` en el sistema, para que la aplicación de administración de red pueda consultar al sistema sobre su estado.
- Implementar mecanismos de autenticación y cifrado en los paquetes de SNMP provistos por las versiones de SNMP 2 y 3.
- Implementar un registro de eventos que se almacenen localmente en la memoria EEPROM externa y que pueda ser consultado desde la página WEB.
- Implementar la página WEB con el protocolo HTTPS.

Bibliografía

[1] Banco Central de Costa Rica. *Licitación Restringida 20053-155: Adquisición de Hardware.* Costa Rica: Departamento de Proveeduría, 2005.

[2] Banco Central de Costa Rica. *Sitio WEB* [en línea]. San José, Costa Rica. <http://www.bccr.fi.cr> [Consulta: 8 enero 2006].

[3] Campos, Julio; Monge, Gustavo. *Diseño e implementación de un prototipo de sistema de alarma para armarios de equipos de redes incorporado sobre una red TCP/IP existente.* Informe de proyecto de graduación para optar por el título de ingeniero en Electrónica con el grado académico de Licenciatura. Costa Rica: TEC, 2003.

[4] Catsoulis, John. *Designing Embedded Hardware.* USA: O'Reilly, 2003.

[5] Cisco Systems. *Solución para el BCCR con el proyecto SINPE.* Costa Rica. 2001. <http://www.cisco.com/global/LA/cisco/exito/ind/sfi/costarica.shtml> [Consulta: 8 enero 2006].

[6] Desksoft. *BW Meter* [en línea]. Kansas, USA. 2006. < http://www.desksoft.com/BWMeter.htm> [Consulta: 30 marzo 2006].

[7] Ethereal Software, Inc. *Ethereal*® [en línea]. Kansas, USA. 2006. < http://www.ethereal.com/download.html> [Consulta: 30 marzo 2006].

[8] IANA Consulta de asignación de números de puertos. *Sitio WEB* [en línea]. USA. 2006 <www.iana.org/assignments/port-numbers> [Consulta: 20 enero 2006].

[9] IANA Consulta de asignación de códigos de empresa para SNMP. *Sitio WEB* [en línea]. USA. 2006 <www.iana.org/assignments/enterprise-numbers> [Consulta: 20 enero 2006].

[10] Ipswitch, Inc. *WhatsUp Gold*® [en línea]. Massachusetts, USA. 2006. <http://www.ipswitch.com/products/whatsup/index.asp> [Consulta: 10 enero 2006].

[11] Microchip Technology Inc. *Sitio WEB* [en línea]. Arizona, USA. 2006. <http://www.microchip.com > [Consulta: 9 enero 2006].

[12] MicroController Pros Corporation. *Sitio WEB* [en línea]. California, USA. 2006. <http:// www.ucpros.com > [Consulta: 9 enero 2006].

[13] Modtronix Engineering. *Sitio WEB* [en línea]. Australia. 2006 <http://www.modtronix.com > [Consulta: 9 enero 2006].

[14] Rajbharti, Nilesh. *AN833: The Microchip TCP/IP Stack.* USA: Microchip, 2002.

[15] RFC Consultas. *Sitio WEB* [en línea]. USA. 2006 <http://www.ietf.org/rfc.html > [Consulta: 9 enero 2006].

Apéndices

A.1 Glosario, abreviaturas y simbología

ADC: Convertidor de analógico a digital

ARP: Protocolo de resolución de direcciones

BCCR: Banco Central de Costa Rica

C: Lenguaje de programación de alto nivel

CGI: Interfaz de enlace común; para páginas WEB dinámicas

EEPROM: Memoria de solo lectura programable y eléctricamente volátil

Ethernet: Tecnología LAN

FCS: Suma de verificación de tramas (Mecanismo de detección de errores)

FIFO: Estrategia de colas, primero que entra primero que sale

Firewall: Cortafuegos, dispositivo de seguridad en redes de comunicación

Flash: Memoria cuya tecnología ROM es la más nueva. Es reprogramable.

FSM: Máquina de estados finita

HTML: Lenguaje de etiquetado de documentos hipertexto

HTTP: Protocolo de transferencia de hipertexto

HTTPS: HTTP seguro

IANA: Autoridad de asignación de números de Internet

Internet: Red de redes

Intranet: Conjunto de redes bajo una misma administración

ITCR: Instituto Tecnológico de Costa Rica

LAN: Red de área local

LED: Diodo emisor de luz

MIB: Base de datos para administración

NAT: Traducción de direcciones de red

NIC: Tarjeta de interfaz de red

NMS: Estación de administración de red

OID: Identificador de objetos

PC: Computadora personal

PDU: Unidad de datos de protocolo

RFC: Documentos donde se estandariza la evolución de Internet

RJ-45: Conector de 8 pines estandarizado para conexiones `Ethernet`

SINPE: Sistema Interbancario de Negociación y Pagos Electrónicos

SMI: Estructura de información de administración

SNMP: Protocolo simple de administración de redes

Socket: Asociación de una dirección IP y un número de puerto

SRAM: Memoria de acceso aleatorio estático

TCP/IP: Protocolo de control de transmisión / Protocolo de Internet

Trap: Mensaje de notificación en SNMP

USART: Transmisor receptor síncrono universal

WAN: Red de banda ancha

WEB: Sistema de hipertexto que funciona sobre Internet

A.2 Información sobre GGT Solutions

A.2.1 Descripción de la empresa

GGT Solutions es una empresa que cuenta con cuatro áreas de servicio, las cuales en algunos casos se complementan entre sí, buscando siempre satisfacer las necesidades particulares de sus clientes. Las áreas de servicios son:

- Comunicaciones IP
- Infraestructura de Red
- Seguridad de la información
- Proyectos Especiales

Esta empresa se encuentra ubicada en Curridabat, específicamente 400 metros al Sur y 15 metros al Este de la Pops, Edificio Alfavia. GGT Solutions cuenta con 15 empleados.

El departamento donde se realiza el proyecto es el de Proyectos Especiales.

A.2.2 Descripción del departamento de Proyectos Especiales

La función principal de este departamento es el desarrollo de proyectos que estén relacionados con la ingeniería en electrónica.

En este departamento se encuentran el Ing. José Pablo Esquivel Escalante y el Ing. Olger Pérez Sánchez, ambos ingenieros en electrónica.

A.3 Antecedentes prácticos

Este proyecto tiene como antecedente práctico el proyecto de graduación elaborado por los estudiantes Julio Campos y Gustavo Monge [3] en el año 2003, cuyo nombre del proyecto es "*Diseño e implementación de un prototipo de sistema de alarma para armarios de equipos de redes incorporado sobre una red TCP/IP existente".*

El proyecto actual surge debido a que el proyecto anterior se quedó en la fase de prototipo y no fue implementado en escala. Por ello, el BCCR solicitó una licitación para que este proyecto sea ejecutado en escala. En cuanto a los requisitos solicitados en el proyecto anterior permanecen en el actual. Aún así, a continuación se describen algunas limitaciones del proyecto realizado anteriormente:

En la parte de aplicación para configurar el dispositivo, para accesar al dispositivo se necesitaba instalar un programa en alguna computadora. Esto implica que el dispositivo depende de que instalen un programa para configurarlo, es decir, el dispositivo por si sólo no es autosuficiente. Llámese autosuficiente a un dispositivo que pueda ser configurado por medio de una aplicación estándar como lo es un explorador de Internet, sin requerir de algún protocolo de comunicación propietario.

En cuanto a seguridad para configurar el dispositivo no existía un mecanismo de autenticación para validar al usuario que quiere hacer cambios de configuración. Solo bastaba con tener el instalador del programa y ya se podía tener acceso.

En cuanto al conjunto de protocolos TCP/IP, el sistema no hacía solicitudes del protocolo de resolución de direcciones (ARP) para encontrar la dirección MAC de la puerta de enlace predeterminada dada la dirección IP del enrutador. Esto implica que si había un cambio de enrutador, había que configurarle la dirección MAC del nuevo enrutador. Usando ARP, el sistema no necesitaría de configuración frecuentemente.

Anexos

B.1 Diagrama esquemático de la tarjeta SBC65EC

En la Figura B.1 se muestra el plano de la placa de circuito impreso de la tarjeta SBC65EC de Modtronix®. En las siguientes páginas se muestra el diagrama esquemático de dicha tarjeta.

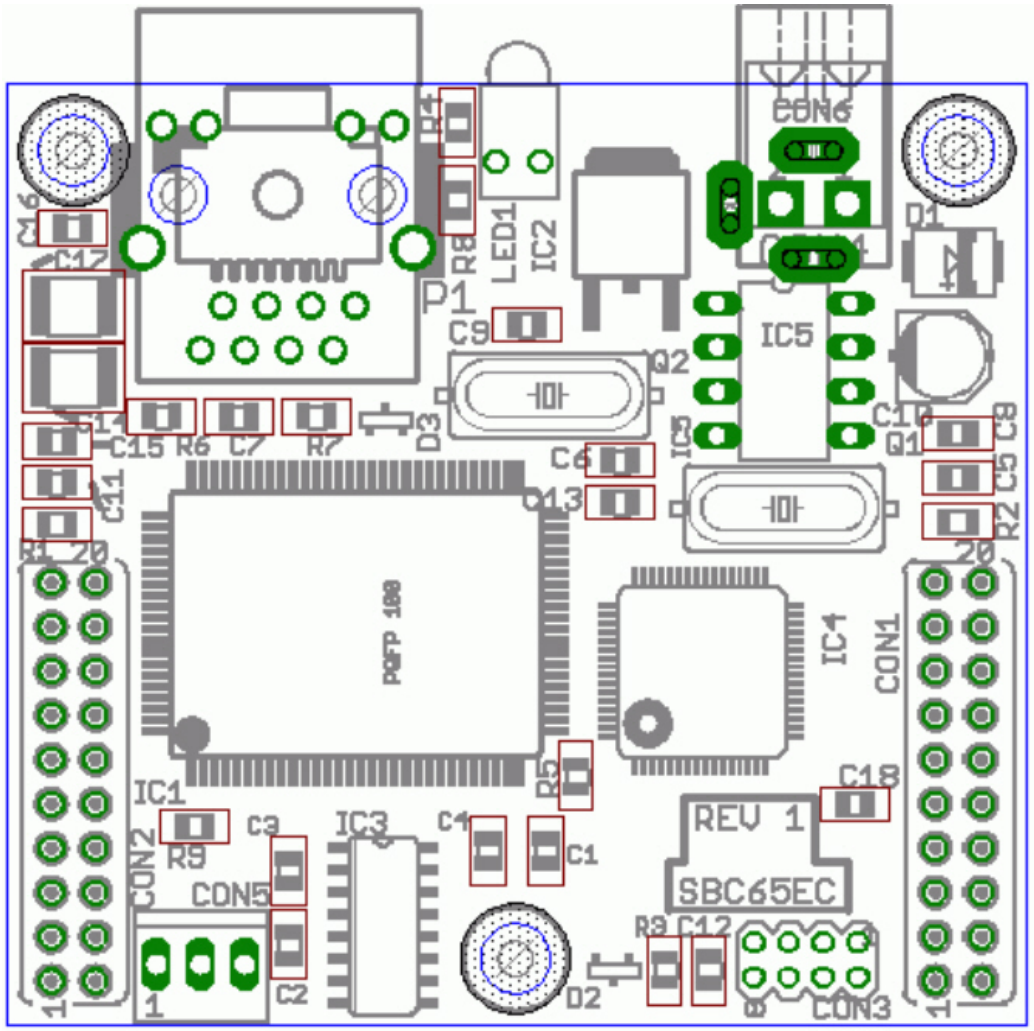
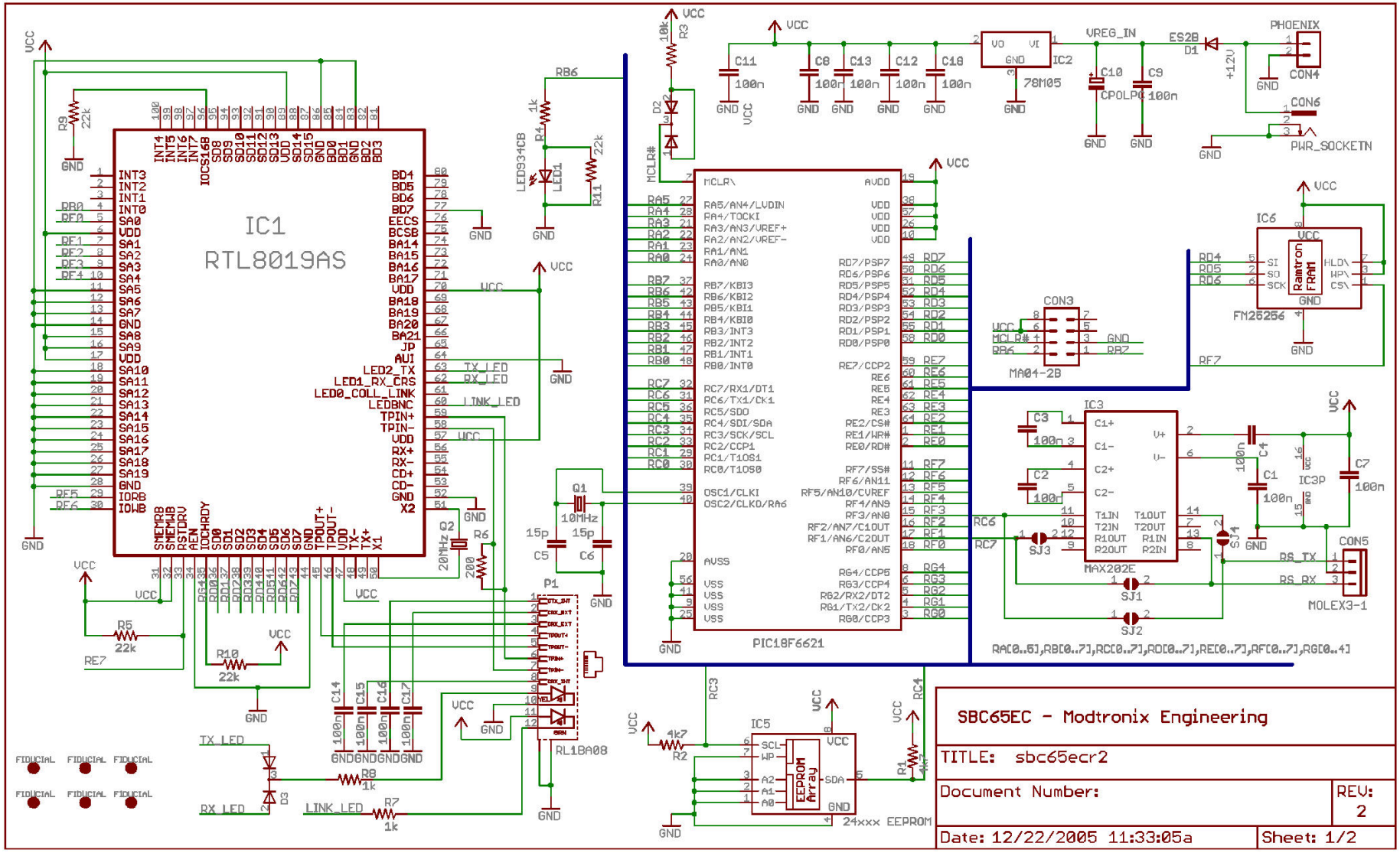
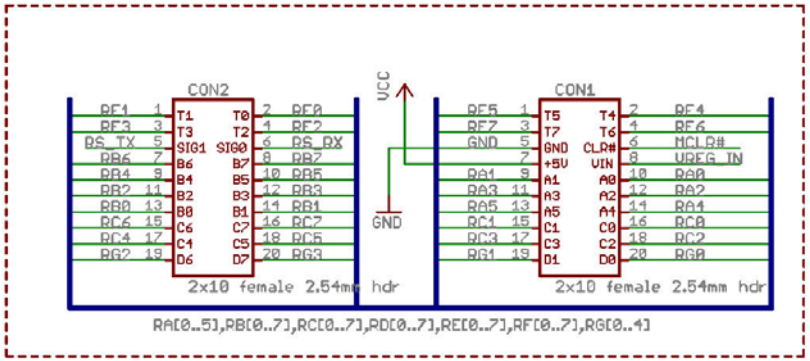


Figura B.1 Plano de la placa de circuito impreso de la tarjeta SBC65EC


IC1
RTL8019AS
PIC18F6621
SBC65EC - Modtronix Engineering
TITLE: sbc65ecr2
Document Number:
REV: 2
Date: 12/22/2005 11:33:05a
Sheet: 1/2

Daughter Board Connector



SBC65EC - Modtronix Engineering		
TITLE: sbc65ecr2		
Document Number:		REV: 2
Date: 12/22/2005 11:33:05a	Sheet: 2/2	

B.2 Diagrama esquemático del chasis IOR5E

En la Figura B.2 se muestra el plano de la placa de circuito impreso del chasis IOR5E de Modtronix®. En las siguientes páginas se muestra el diagrama esquemático de dicho chasis.

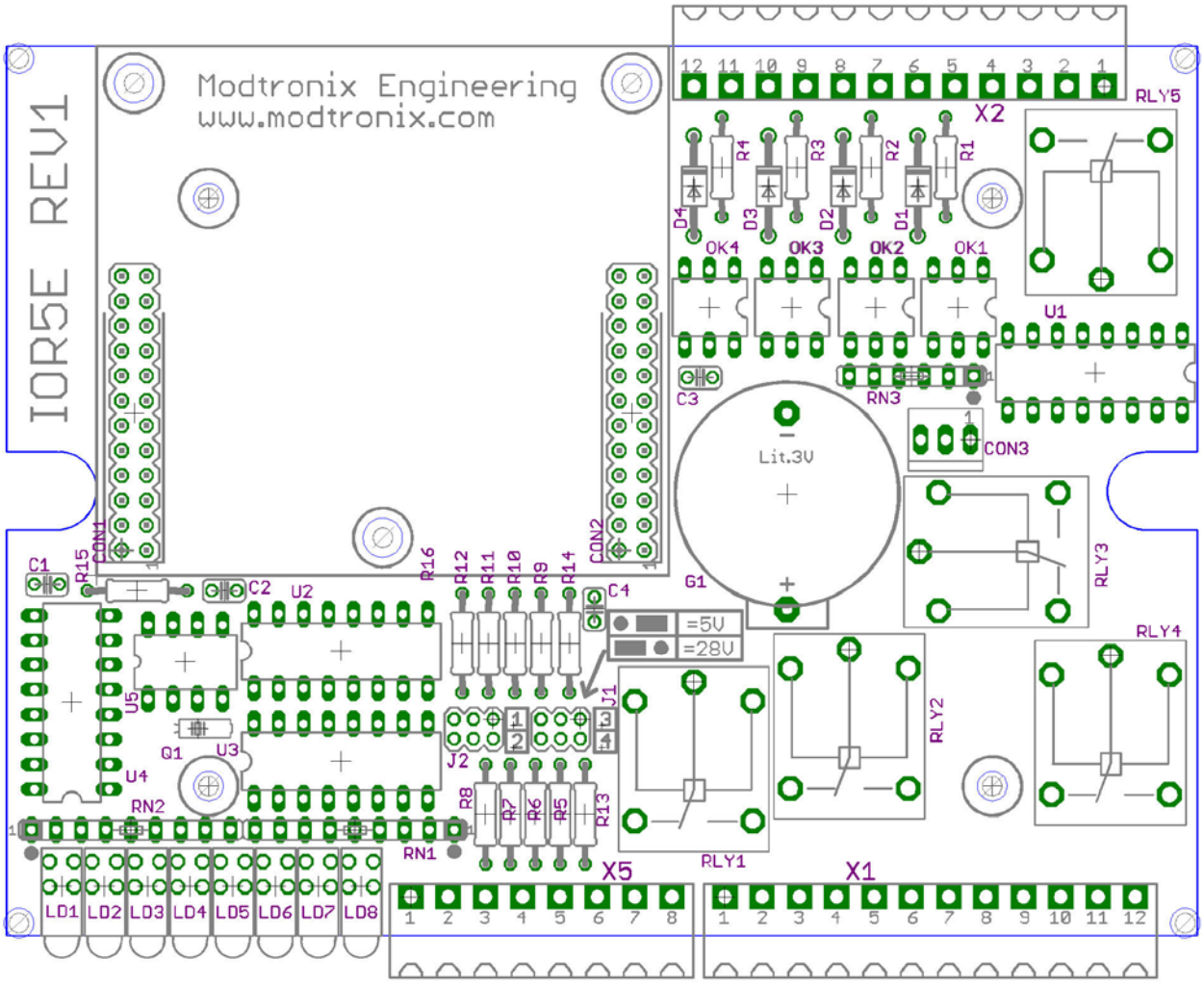
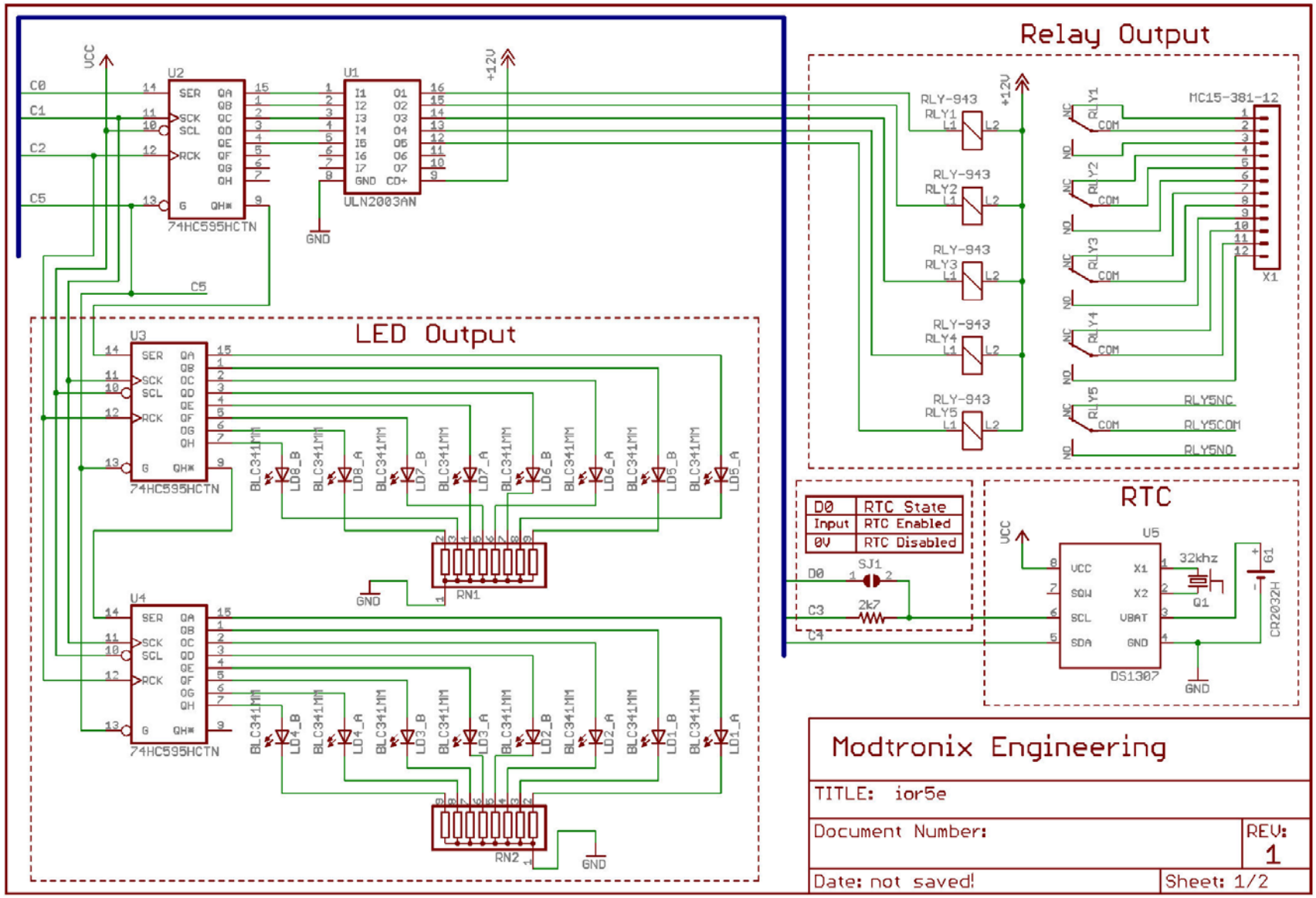
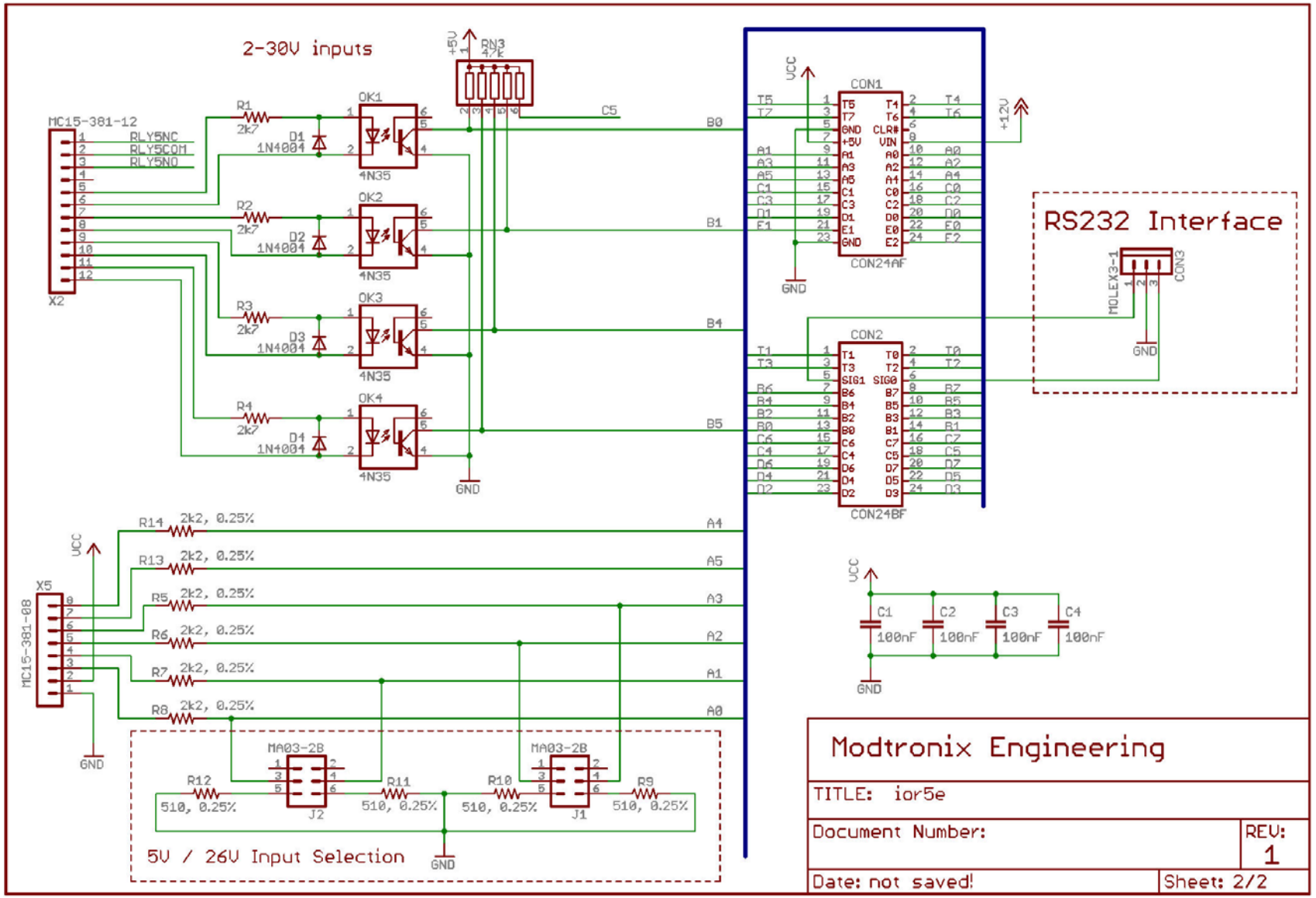


Figura B.2 Plano de la placa de circuito impreso del chasis IOR5E


Relay Output
LED Output
RTC
U1
U2
U3
U4
U5
ULN2003AN
74HC595HCTN
RN1
RN2
RLY-943
MC15-381-12
X1
DS1307
32khz
Q1
CR2032H
SJ1
2k7
D0
C3
C4
C5
+12V
VCC
GND
RLY5NC
RLY5COM
RLY5NO
D0 | RTC State
Input | RTC Enabled
0V | RTC Disabled
Modtronix Engineering
TITLE: ior5e
Document Number:
REV: 1
Date: not saved!
Sheet: 1/2


2-30V inputs
MC15-381-12
RLY5NC
RLY5COM
RLY5NO
X2
R1
2k7
D1
1N4004
OK1
4N35
R2
2k7
D2
1N4004
OK2
4N35
R3
2k7
D3
1N4004
OK3
4N35
R4
2k7
D4
1N4004
OK4
4N35
+5V
RN3
4.7K
C5
GND
B0
B1
B4
B5
UCC
CON1
CON24AF
CON2
CON24BF
+12V
RS232 Interface
MOLEX3-1
CON3
X5
MC15-381-08
R14 2k2, 0.25%
R13 2k2, 0.25%
R5 2k2, 0.25%
R6 2k2, 0.25%
R7 2k2, 0.25%
R8 2k2, 0.25%
A4
A5
A3
A2
A1
A0
MA03-2B
J2
J1
R12
510, 0.25%
R11
510, 0.25%
R10
510, 0.25%
R9
510, 0.25%
5V / 26V Input Selection
C1
C2
C3
C4
100nF
Modtronix Engineering
TITLE: ior5e
Document Number:
REV: 1
Date: not saved!
Sheet: 2/2