Instituto Tecnológico de Costa Rica

Escuela de Ingeniería Electrónica

Banco Popular y de Desarrollo Comunal

Subproceso de Administración y Operación de Redes

Ampliación de funcionalidad de la herramienta de monitoreo de redes IP del Banco Popular y de Desarrollo Comunal usando Simple Network Management Protocol (SNMP) e Internet Control Message Protocol (ICMP) Fase II

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

Ariel Sánchez Mora

Cartago, Marzo 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. William Marín Moreno

Profesor lector

Ing. Julio Córdoba Arce

Profesor lector

Ing. José Faustino Montes de Oca

Profesor asesor

TEC
Instituto Tecnológico de Costa Rica
Escuela de Ingeniería Electrónica

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, 23 de marzo, 2006

Declaro que el presente informe de proyecto de graduación ha sido realizado por mi persona, utilizando y aplicando literatura referente al tema, así como la información que haya suministrado la institución para la que se realizó el proyecto, y aplicando 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 por el contenido de este informe de proyecto de graduación.

San José, Costa Rica
Marzo 2006

Firma del autor:

Ariel Sánchez Mora
Cédula: 1 1329 0487

Resumen

El Subproceso de Administración y Operación de Redes (SAOR) del Banco Popular y de Desarrollo Comunal (BPDC) desea ampliar las capacidades de su sistema actual de monitoreo de redes. El sistema actual fue desarrollado hace dos años por dos practicantes de ingeniería electrónica del Instituto Tecnológico de Costa Rica (ITCR); permite monitorear el estado del enlace de cada sucursal del banco con las oficinas centrales en San José. Utiliza para ello principalmente ICMP (Internet Control Message Protocol) y SNMP (Simple Network Management Protocol) v1; esta versión se ha vuelto obsoleta a nivel mundial.

La ampliación del sistema representa la segunda fase del mismo. Para esta fase se recreó enteramente la estructura interna de la herramienta. Se cambió el motor de la base de datos para permitir más flexibilidad, confiabilidad y funciones nuevas. También se implementó un uso más complejo del protocolo SNMP, con la opción de usar la versión vigente, versión 3. Se hizo un análisis de las debilidades y fortalezas de la primera etapa, de manera que los mejores atributos de la primera fase se incluyeron en la segunda versión. Se ha logrado que la herramienta sea más interactiva, informativa, configurable y adaptable, incorporando mejores políticas de seguridad en su uso. Es una herramienta hecha a la medida de las necesidades del SAOR y reemplaza a la primera fase. Se ha capacitado a un ingeniero del SAOR para que pueda dar mantenimiento al código fuente.

Palabras Clave:
SNMP,SNMPv3,Synapse,MySQL,Delphi,dbExpress,ICMP,NMS,Cisco,monitoreo

Abstract

The Subproceso de Administración y Operación de Redes (SAOR), network administrating entity of the Banco Popular y de Desarrollo Comunal (BPDC), wishes to expand the possibilities of its current network monitoring tool. The current tool was developed two years ago by two electronics engineering students from the Instituto Tecnológico de Costa Rica (ITCR). It informs the network administrator the communication capabilities of every communication link between the bank's branch and central offices, in San José. To accomplish this, it relies on ICMP (Internet Control Message Protocol) and SNMP (Simple Network Management Protocol) v1, version which is obsolete.

This project is centered on the second phase of the bank's proprietary network monitoring tool. For this phase, the tool was recreated using a more capable database engine and a more complex implementation of the SNMP protocol, with the option of using version 3 to fix security vulnerabilities. An analysis of the previous phase's strengths and weaknesses was taken into account in the development of this phase so that the previous tool's best attributes are preserved. A more interactive, informative, adaptable and configurable tool has been developed that deploys standard security measures in its use. One of the bank's engineers has been instructed so that the source code can be properly maintained.

Keywords:
SNMP,SNMPv3,Synapse,MySQL,Delphi,dbExpress,ICMP,NMS,Cisco,management

Dedicatoria

Le dedico este trabajo a mi abuela, Adina Cárdenas Flores. Fue mi segunda madre y más abuela para mí de lo que normalmente le toca a un nieto; murió en Enero del 2006, durante el transcurso de este proyecto.

También se lo dedico a mis padres, que con mucho esfuerzo y no poca paciencia, han aprendido a respetar mis decisiones y valorar mis fortalezas. A ellos y a mis hermanos, con amor.

Agradecimiento

Quiero agradecer de manera muy especial al Subproceso de Administración y Operación de Redes por la oportunidad que me dieron para hacer este proyecto. Sin recursos verdaderos, me dieron más de lo que necesitaba, a costa suya. Al Msc. Rodrigo Vargas por cuidarme como a un hijo; al Ing. Alfonso Quesada por ser mi compañero y guía; al Ing. Claudio Regueyra, CCNA, por compartir su sabiduría y buen humor; Al Msc. David Vargas por su orientación y ejemplo profesional. Al Msc. Sergio Cambronero y al Ing. Mario Bruzaferri por su compañerismo y devoción al trabajo, y a Sonia Sánchez por su gentil cortesía.

Quiero también agradecer al Subproceso de Soporte Técnico por los innumerables consejos y momentos compartidos. De manera muy especial, a los Ing. Ignacio León y Miguel Campos por sus explicaciones y tiempo brindado.

Deseo también agradecer a los amigos profesionales que me ayudaron a llegar donde estoy hoy: Msc. Javier Chang, del Banco Popular; Elías García, de la academia Cisco, y Hernán Rojas, de Unisys, vecino y amigo de mi familia. Estoy profundamente agradecido por sus consejos, ejemplo y tiempo conmigo. Quiero también agradecer de manera muy especial al Ing. Faustino Montes de Oca, asesor, profesor y guía. En innumerables ocasiones ha confiado plenamente en mí y le estoy muy agradecido por su apoyo, ejemplo y sabios consejos.

Quiero agradecer a todos mis contemporáneos, profesores, personal administrativo, que he conocido a lo largo de la carrera; especialmente a Viviana Artavia y familia, con quien compartí muchas horas de trabajo a través de estos años de estudio.

Gracias a mis amigos cercanos: Nogui y familia, Alberto y familia, Lindsay, Leonardo, Verónica, Lester, Nydia, Álvaro, José Vicente y Amy. Finalmente, a toda mi extensa y grandiosa familia, sin olvidar a mi madrina Zuray; y a Dios, que nos cuida a todos.

ÍNIDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Capítulo 1: Introducción

En este capítulo se expone el problema que da origen al proyecto, y en forma general, la solución realizada para solventarlo. En los capítulos siguientes se ahonda más en estos temas y se analiza la calidad de la solución implementada.

1.1 Problema existente e importancia de su solución

Este trabajo se ubica en el campo de software de monitoreo de redes IP. Las redes IP son uno de los principales sistemas de comunicación usado en empresas de diversos tamaños a nivel mundial. Debido a los múltiples beneficios en productividad que conlleva el uso de sistemas de computación en el ambiente empresarial, los sistemas de cómputo y de interconexión de redes IP aumentan en número, capacidad, pero también, complejidad; este crecimiento se da en proporción al crecimiento de cualquier organización.

El correcto funcionamiento de estos recursos se hacen más críticos a medida que la oferta de servicios de una organización se expande; más procesos se digitalizan y la comunicación eficaz entre oficinas es indispensable para el flujo normal del negocio. La tarea de soporte y administración de recursos IP demanda más personal y mejor calificado.

Hay un punto en el crecimiento de una red IP donde el administrador necesita valerse de medios automatizados para poder manejar adecuadamente todos los recursos de la misma. El administrador de redes usa software para reconocer y corregir problemas en la red antes de que sean perceptibles para los usuarios de la misma, o en el caso de fallas imprevistas, para efectuar las acciones correctivas a la mayor brevedad.

El Banco Popular y de Desarrollo Comunal (BPDC en adelante) posee una red grande a nivel nacional. Cuenta con 82 oficinas bancarias en todo el país, cajeros automáticos, y conexiones con socios, todos conectados directamente a la sede central en San José. Como en todo banco, su servicio y disponibilidad completa es prioridad a toda hora.

La red es manejada por el Subproceso de Administración y Operación de Redes (SAOR en adelante) del BPDC. El Subproceso es dirigido por el Msc. Rodrigo Vargas y se concentra en el mantenimiento, soporte, planeamiento e implementación de mejoras en la red interna del BPDC. Cuenta con dos ingenieros en sistemas y cuatro ingenieros en electrónica, capacitados con los cursos de redes de Cisco. La decisión de capacitarse en tecnologías IP con los cursos de Cisco no es arbitraria: además de ser la marca de equipo en la que han confiado, estos cursos gozan de excelente reputación a nivel mundial.

El sistema actual de monitoreo de redes fue desarrollado en el año 2004 por dos estudiantes del ITCR como proyecto de graduación, los licenciados Alfonso Quesada Fernández y David Vargas Pereira. Ambos trabajan actualmente en este subproceso, y junto al coordinador, Msc. Rodrigo Vargas Vásquez, son los impulsores del presente trabajo.

La primera fase del sistema consistió en cuatro aplicaciones que permitían al usuario:

- Graficar el uso de ancho de banda instantáneo de una interfaz.
- Utilizar una base de datos en Ms Access ® para llevar el registro del uso de ancho de banda y poder presentar informes cronológicos.
- Saber qué enlaces superaban actualmente un tiempo de espera agotado especificado por el usuario y cuáles líneas de respaldo estaban activas.
- Monitorear la temperatura de los enrutadores principales.

Estos sistemas evolucionaron posteriormente a una aplicación que permite al usuario ver el estado encendido/apagado de las interfaces de los equipos de enrutamiento de la topología de red del Banco Popular con el protocolo ICMP, por medio de luces indicadoras de diferentes colores. Algunas aplicaciones desarrolladas encontraron problemas y entraron en desuso.

Se ha determinado que algunas de las fases anteriores del sistema, como la base de datos, dejaron de funcionar con el paso del tiempo, por lo que se espera se corrijan en la segunda fase. Se espera que la aplicación sea más pro-activa al detectar un problema, y que reúna la información de más relevancia para el Subproceso en una sola interfaz. También es deseable que cuando haya un cambio en la red, la aplicación pueda ser actualizada sin devolverse al código, pues esto es inconveniente si el programador no se encuentra disponible.

Construyendo sobre lo ya logrado, se integrarán las ideas de las aplicaciones existentes junto con nuevos requerimientos, definidos por el SAOR, que brinden mayor capacidad de monitoreo a la aplicación. En vez de tener aplicaciones separadas, se espera tener una sola y eficiente aplicación que presente una interfaz más completa y versátil que la que hay actualmente.

La importancia de un sistema de monitoreo versátil y adaptable es que facilita la adquisición de datos al administrador. Con ello se puede alcanzar un mejor manejo de recursos, sabiendo qué oficinas necesitan más potencia de procesamiento y cuáles ocupan menos del que tienen actualmente. Esto ayuda a tener sistemas de comunicación más estables y mejores bases para la planificación del crecimiento futuro de la red. Además, un sistema de monitoreo combinado con una base de datos permite investigar el comportamiento de un equipo antes de una falla o cuando se hacen pruebas de impacto por nuevas aplicaciones entre oficinas.

El SAOR desea obtener, además de datos ya explorados en la primera fase como ancho de banda y tiempo productivo, datos como el consumo de memoria RAM, porcentaje de utilización de CPU y la existencia o no de errores en una interfaz; éstos datos son accesibles a través de una implementación más amplia de SNMP (Protocolo Simple de Administración de Red, por sus siglas en inglés). El sistema actual no permite añadir nuevas variables al monitoreo; esto representa una falta de flexibilidad en la herramienta y afecta las posibilidades de acción del administrador.

La última versión del sistema de monitoreo no incluye la posibilidad de acceder remotamente a equipos remotos desde las oficinas centrales y no toma en cuenta a los conmutadores de la red. Estas características son deseables para el administrador.

El sistema de monitoreo actual también puede mejorarse en el área de seguridad, pues utiliza una versión de SNMP que transmite contraseñas en texto ASCII sin ningún tipo de codificación, lo que permite a un usuario malicioso interceptarla. Además, no necesita ningún tipo de contraseña para su operación una vez que se ha conseguido el ejecutable. En cualquier empresa es importante seguir lineamientos de seguridad, especialmente en un banco, para evitar que información del departamento sea interceptada por entes exteriores al mismo y pueda ser usada con otros fines.

El BPDC es de especial importancia pues es una institución semi-pública ligada a todos los trabajadores del país. Cualquier problema serio en su capacidad de operación es un asunto delicado que tiene la capacidad de transformarse en un evento financiero a nivel nacional. Las mejoras en su servicio benefician finalmente a la sociedad costarricense. El BPDC, con este proyecto, promueve el uso de soluciones nacionales, en vez de comprarlas a empresas extranjeras.

Beneficios de una mejor herramienta de monitoreo de red:

- Mayor cantidad de información disponible al administrador de redes.
- Mayor capacidad del administrador para diagnosticar problemas (mantenimiento preventivo).
- Más facilidad de interpretación y de recolección de datos para el administrador.
- Mejor nivel de seguridad en el monitoreo.
- Mejor planificación futura de la red.
- Más tiempo productivo para el usuario final.
- Mejor control sobre los activos de la empresa.
- Menor complejidad en la administración de la red.
- Eficiencia y claridad en el trabajo del departamento de redes.
- Maximización de la eficiencia en el uso de recursos del Banco.

1.2 Solución elegida

Este trabajo representa la segunda fase del sistema de monitoreo de redes del BPDC. Los requerimientos definidos por la institución para esta etapa fueron:

- Añadir funcionalidad al sistema actual para recopilar y guardar variables SNMP adicionales a las posibles en la primera fase.
- Implementar un sistema de recolección de información en una base de datos más robusta y eficaz.
- Implementar la capacidad de presentar informes cronológicos con los datos de la base de datos.
- Otorgar opciones de configuración a la aplicación para que el administrador de redes posea una herramienta flexible de monitoreo.
- Reunir las aplicaciones desarrolladas en una sola y eficiente interfaz.
- Diseñar e implementar el ambiente visual de manera que permita un fácil y completo uso del sistema.

- Implementar prácticas de seguridad en la aplicación.
- Permitir la corrección de problemas remotos de configuración accediendo al equipo desde la aplicación.
- Incluir los conmutadores además de los enrutadores dentro de los equipos monitoreados.

La solución final respetó el criterio de la fase anterior en usar Delphi 7 como herramienta de desarrollo. Sin embargo, las bibliotecas Indy, componente elegido para implementar SNMP, se descartaron en esta versión debido a que no daban soporte a SNMPv3, versión que si tiene soporte para proteger la contraseña de monitoreo.

Se decidió utilizar al motor de base de datos MySQL para solventar las deficiencias de Ms Access ® en capacidad. La elección se fundamentó en que MySQL es reconocida a nivel mundial por su excelente desempeño en ambientes con mucho volumen, excelente soporte y documentación, variedad de ejemplos y costo nulo o bajo de adquisición. Se utilizó la última versión garantizada por el fabricante como estable, y Delphi, como aplicación especializada de desarrollo en ambientes de bases de datos, para hacer la conexión.

Para lograr los objetivos de versatilidad y disponibilidad de información, el diseño se apoyó fuertemente en usar la base de datos como centro de todos los procesos. La información de los equipos del banco popular se almacenó en tablas, y a partir de estas tablas se crean las siguientes tablas necesarias para el funcionamiento del programa; así el programa obedece a lo que encuentra en las tablas y no guarda información en el código, sólo procedimientos. Esto permite que después se pueda cambiar la información de la red del BPDC con software, no actualizando el código fuente.

Se recreó la interfaz gráfica de manera que ahora los equipos están ordenados por oficina, y desde el panel de monitoreo central se puede acceder un equipo y ver su información, diagrama de red, gráficos de los valores guardados en su base de datos, y ejecutar pruebas de diagnóstico; por ejemplo, ping a cada interfaz. Se hicieron tablas separadas para enrutadores y conmutadores, por la diferencia de tipos de monitoreo que el SAOR definió para cada uno.

Al monitorear más variables con SNMP, se cambió el funcionamiento del monitoreo periódico de las oficinas remotas, pues ahora se puede saber si un enlace está verdaderamente caído a pesar de que por ICMP se dé un tiempo de espera agotado, lo que puede pasar por saturación del enlace. Se implementó una bitácora cuando un enlace se cae o vuelve en operación, con alarma audible y correo al SAOR con los datos importantes del mismo. Esto hace que la aplicación sea mucho más útil para todo el departamento.

La aplicación crea una tabla por equipo y por mes. Finalizado el mes, exporta la tabla a un archivo CSV de fácil importación a Ms Excel para futuros análisis, y descarta la tabla del mes anterior. En el CSV se incluye un reporte de promedios de los valores monitoreados.

La solución tiene dos partes. Consta de un recolector de datos, que recoge los datos por ICMP y SNMP, y la interfaz, que usa los datos recogidos por el recolector y los despliega. Se dividió la aplicación puesto que una vez que el recolector tiene datos, se puede desarrollar cualquier interfaz que use dichos datos, aprovechando la flexibilidad de MySQL. La interfaz puede ejecutarse en la misma PC o en otras PCs que tengan acceso al mismo servidor MySQL. Por ello, se orientó la solución a un GUI separado del servidor que pueda servir como herramienta LAN si se decide adaptar.

A través de los pasos necesarios para completar la solución, se notó la necesidad real de que la aplicación usará varios hilos de procesamiento, debido a la naturaleza del trabajo en ambientes con sockets; el uso de hilos es esencial para obtener una aplicación ágil y eficiente de monitoreo.

Finalmente, se documentó la solución y su arquitectura para que el ingeniero a cargo de la primera versión mantenga el programa funcionando a través de nuevos requerimientos, con acceso al código fuente para implementar nuevas funciones o diagnosticar futuras fallas.

Capítulo 2: Meta y objetivos

En este capítulo se enumeran las razones de ser del proyecto. La meta y el objetivo general se utilizan para valorar si la solución alcanzada cumplió con los requerimientos de la institución, y en qué grado. Los objetivos específicos son una guía para revisar el objetivo general.

2.1 Meta:

Implementar la segunda fase del desarrollo de la herramienta de monitoreo de redes del Banco Popular y de Desarrollo Comunal, alcanzando mejores niveles de flexibilidad, funcionalidad, confiabilidad, seguridad y facilidad de manejo.

2.2 Objetivo General:

Desarrollar la segunda fase del sistema de monitoreo de redes del BPDC con el objetivo de que sea más versátil en el alcance de sus funciones, ampliar el monitoreo de equipo, hacer la aplicación más amigable, configurable y segura, y facilitar un mejor aprovechamiento por parte del ente administrador de redes.

2.3 Objetivo Específicos:

2.3.a Objetivos de software:

1 Crear una aplicación recolectora de variables de específico interés para el administrador, como uso de CPU, RAM, temperatura, ancho de banda, que opere sobre la red actual del Banco Popular y de Desarrollo Comunal, usando SNMP.

2 La información de monitoreo debe guardarse en una base de datos de alto desempeño.

3 Crear una aplicación de monitoreo que utilice los datos recogidos en la base de datos para informar al administrador del estado de la red. La presentación de los datos debe ser con gráficos, de forma instantánea e histórica y con información estadística básica que el administrador determine durante el desarrollo del sistema.

4 Permitir al administrador añadir o borrar variables a ser monitoreadas.

5 Implementar las funciones nuevas y existentes en una sola y efectiva interfaz.

6 Desarrollar en la aplicación un modo de operación visual que facilite el uso y la navegación a través de la información de las oficinas del Banco Popular y de Desarrollo Comunal.

7 La aplicación debe estar adaptada para desplegarse en monitor de PC normal y de 42 pulgadas.

8 Permitir al administrador suficiente grado de control sobre el programa para que pueda modificar la información de sucursales, equipo existente y datos recolectados, así como la frecuencia con la que se recolectan los datos, para optimizar el uso del ancho de banda.

9 Permitir la función de emulación de terminal de equipos remotos para la configuración a distancia desde la interfaz visual.

10 Añadir funciones de seguridad a la base de datos y al tráfico del sistema que permitan regular su uso al Subproceso de Administración y Operación de Redes.

2.3.b Objetivos de documentación:

Debe entregarse un informe final, un manual de usuario y un manual para administrador que explique la programación para cualquier cambio que el Banco desee hacer al programa.

2.3.c Objetivos de implementación:

Se espera que la segunda etapa de la herramienta se implemente totalmente y reemplace satisfactoriamente a la primera etapa.

Capítulo 3: Marco Teórico

En esta sección se introducen los conceptos necesarios para entender el problema y los pasos necesarios para alcanzar su solución.

3.1 Descripción del sistema o proceso a mejorar

Se desea mejorar la herramienta que ejecuta el monitoreo de la red IP del BPDC. La red tiene la arquitectura propia de una entidad bancaria: mainframes, servidores internos, internet y portal de servicios internet, etc. Posee tecnologías variadas y algunas adaptaciones a sistemas de computación de legado, pero en lo que respecta a su equipo de red, todo es relativamente nuevo y de un solo fabricante, Cisco ®.

El monitoreo de red se puede explicar brevemente como el acto de recolectar los parámetros de funcionamiento del equipo de la red en un sólo lugar para comparar los datos actuales con lo esperado. El centro de monitoreo le brinda información al administrador de la red, quien es responsable de tomar las acciones necesarias para garantizar el correcto desempeño del equipo.

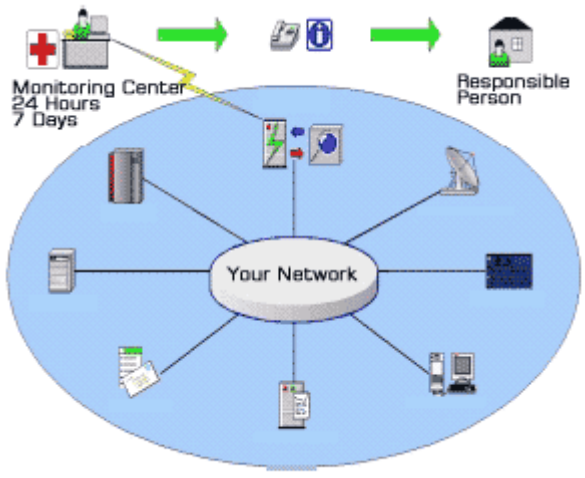


Figura 3. 1 Diagrama representativo de la función de una herramienta de monitoreo de red [9]

Aunque el monitoreo de red, en sentido amplio, incluye el monitoreo de servidores, UPS, mainframes, impresoras, entre otros, en el caso del SAOR el interés es monitorear los equipos de las primeras tres capas del modelo OSI. Los equipos administrables en estas capas son los conmutadores y enrutadores, y son los equipos que están bajo la supervisión del SAOR.

Actualmente la red se monitorea con la primera fase del sistema, elaborada como práctica de graduación de dos estudiantes en el 2004 (únicamente enrutadores). El sistema actual tiene alcances limitados en su funcionalidad y opciones al administrador, pero alcanzó satisfactoriamente los objetivos planteados para una primera fase. Esta nueva fase busca mejorar la herramienta para facilitar el trabajo de la administración de la red del Banco.

3.2 Antecedentes Bibliográficos

Existen sistemas de monitoreo, con algunas de las características buscadas por el Banco Popular, en el mercado internacional. Los fabricantes de equipo de red, como Cisco y Hewlett Packard (HP) han desarrollado sus aplicaciones de monitoreo para empresas de gran tamaño. Estas soluciones tienen precios altos para lo que el BPDC necesita; muy altos cuando se considera que por la cantidad de equipo que se desea monitorear, los licenciamientos no son los más modestos. Además, se ha comprobado, con demos que han instalado vendedores, que no satisfacen los requerimientos de SAOR. Se ocupa una herramienta hecha a la medida, altamente configurable y adaptable, que además, sea más económica.

Es importante mencionar que el trabajo y la investigación realizados en la primera etapa son muy importantes para comprender el enfoque y las particularidades de la red que se maneja. Este trabajo está disponible a través de la biblioteca José

Figueres Ferrer del Instituto Tecnológico de Costa Rica [13] y explica en buen detalle el manejo de las variables en SNMP y particularidades de la red del BPDC.

El estado del arte del monitoreo de redes en la actualidad es SNMPv3, la versión más reciente del estándar, con sus mejoras en seguridad. SNMP es un estándar internacionalmente reconocido, no atado a ningún vendedor y muy usado en el desarrollo de soluciones de monitoreo.

A pesar de que Delphi ha probado ser un lenguaje excelente para desarrollos en ambientes Windows y Linux (Kylix), el mundo se mueve más hacia soluciones .net, Java y ANSI C. Sin embargo, todavía Delphi es una buena elección de lenguaje por la cantidad asombrosa de código libre y usuarios experimentados que están dispuestos a ayudarse uno al otro.

Un factor a considerar en este trabajo es que el mundo de la computación se mueve hacia los códigos abiertos y a los grupos de soporte gratuitos por listas de correo. Esto es, las personas interesadas mandan un correo con su problema a un grupo grande de subscriptores de un tema que les interesa. Muchos expertos se ayudan en secciones de código problemáticas, indicando un problema de diseño o apuntando hacia una página Web; no se ofrecen a desarrollar aplicaciones gratis para terceros. Internet ha abierto la puerta a que gente desinteresada publique y comparta sus conocimientos, simplemente por la posibilidad de que ayude a otro. Es conveniente aprovechar la inteligencia de expertos que se contactan de forma gratuita en Internet para generar las características deseadas en la aplicación.

La elección de MySQL obedece a un ejemplo claro de lo que la cooperación de código abierto puede lograr. Este motor ha logrado quitar mercado a empresas grandes como Oracle por su excepcional desempeño, excelente soporte y política de continuas mejoras, junto con una solución que es escalable a múltiples entornos y usos. Además de ser la norma en diseño de forums web en conjunto con php, este

motor de base de datos tiene entre sus usuarios corporativos a Nasa, Alcatel y Yahoo. Dispone de varias soluciones, entre las cuales está una versión gratuita con garantía de estabilidad; esta garantía se da tras un año de pruebas intensas.

3.3 Descripción de los principales principios de software y electrónicos relacionados con la solución del problema

3.3.1 Monitoreo de redes

Existen dos estándares reconocidos para el proceso de monitorear una red: SNMP, el más popular, y CMIP (Common Management Information Protocol). La mayoría de las aplicaciones de monitoreo desarrolladas comercialmente, y las herramientas disponibles en Web gratuitas o como código abierto, utilizan SNMP.

Uno de los mayores problemas para un administrador de redes es cuando un equipo de enrutamiento falla. En un equipo configurado y que ha estado funcionando correctamente, esto normalmente se debe a que el tráfico que está procesando es mayor al que puede soportar. Los equipos de enrutamiento, como cualquier computadora, poseen memoria y capacidad de procesamiento limitadas, y cuando el flujo de información en una red es mayor a la capacidad del equipo, pueden perder datos o dejar de enrutar información completamente.

Los administradores de red buscan conocer la tasa de flujo de información a través de los enlaces de red para conocer qué equipos están operando a capacidades excesivas (donde pueden desconectarse o perder la información) o el caso contrario: cuando un equipo está siendo desaprovechado. El sistema debe guardar una relación costo-beneficio con el ancho de banda disponible; con esta información se pueden prevenir cuellos de botella o reubicar enlaces alquilados para mejorar el desempeño de la red. También se desea conocer el

porcentaje de utilización de memoria y CPU de los equipos por las mismas razones.

Una red con los equipos adecuados a las necesidades, no sólo instantáneas, sino también según picos de uso, permite ahorrar costos pues el administrador compra sólo los equipos y anchos de banda óptimos para mantener a la red funcionando como se espera. Asimismo, el estudio de los comportamientos del flujo de información permite al administrador tomar decisiones acertadas cuando hay que expandir la infraestructura.

Al recoger información de la red, se debe tener en cuenta que se genera tráfico que también va a cargar los enlaces y el nivel de procesamiento de los equipos, por lo que se deben tomar medidas para controlar el tráfico de monitoreo. Esto se puede hacer variando los tiempos de muestreo de los equipos y asegurarse que los datagramas utilizados sean lo más pequeños posible, y con técnicas de manejo de tráfico por políticas de prioridad.

3.3.2 Protocolo Simple de Administración de Red (SNMP)

El protocolo simple de administración de red (Simple Network Management Protocol, SNMP) fue creado por petición de la Organización de Estándares Internacionales (ISO) con el fin de crear un modelo estandarizado de administración de redes. La Fuerza de Obras de Ingeniería de Internet (Internet Engineering Task Force, IETF) desarrolló la colección de estándares que se conoce como SNMP y la publicó en RFC1157. Consiste de un protocolo, una especificación de estructura de base de datos y un juego de objetos de datos. En 1989 se adoptó como un estándar para redes TCP/IP; en 1993 con el RFC 1905 se creó la segunda versión del estándar, que aumentó funcionalidad, y actualmente el estándar es SNMPv3, que permite autenticación y encriptación de paquetes, definido en 11 RFCs.

El protocolo SNMP define 4 elementos:

- Estación de monitoreo
- Agente de monitoreo
- Base de información de monitoreo
- Protocolo de monitoreo de redes

La administración de redes con el protocolo SNMP se basa en una PC que funciona como estación de monitoreo de red (Network Management Station) ejecutando una aplicación de monitoreo de red (Network Management Application, NMA). Esta aplicación recoge los datos de los agentes monitoreados con 3 comandos: *get*, para recoger un dato; *set*, para establecer un valor en un equipo; y *trap*. Los comandos *get* y *set* son ejecutados a modo de sondeo, mientras los comandos tipo *trap* son datos enviados desde el agente sin previa consulta a modo de notificación.

SNMP es un estándar mundial entre fabricantes; por ello los vendedores de equipo incluyen un agente de monitoreo (cliente SNMP) en sus equipos, en este caso, en los enrutadores y conmutadores Cisco. Este agente es el que se encarga de obedecer a la estación de monitoreo de red.

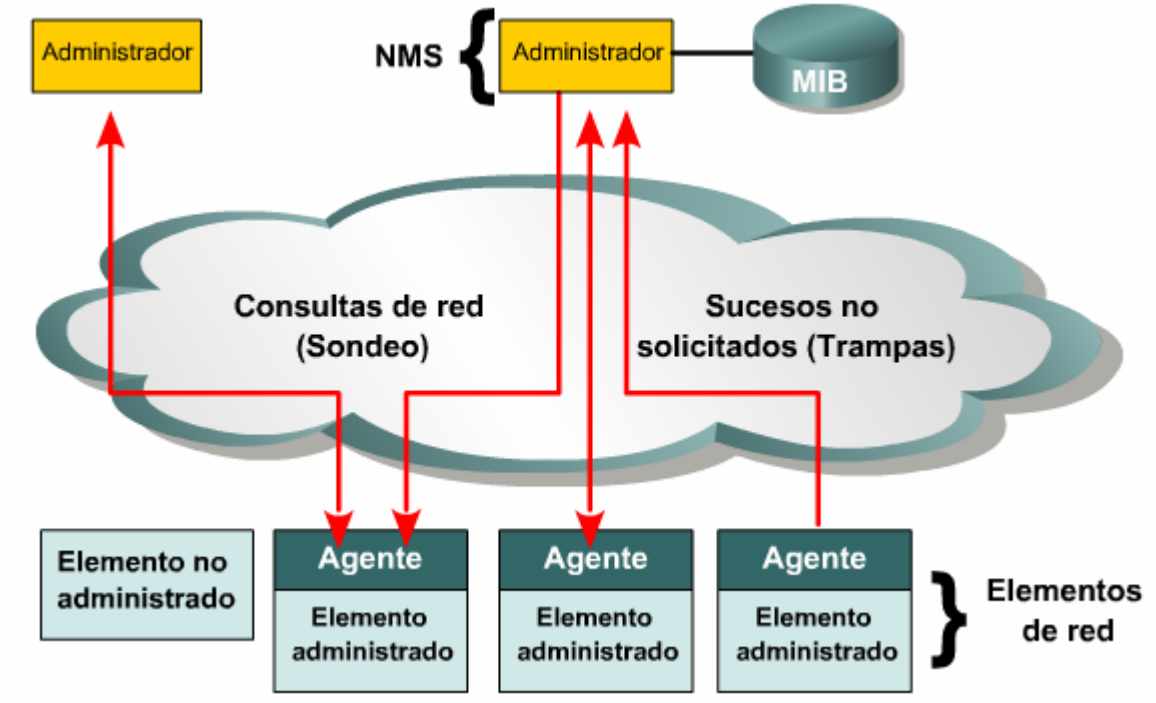


Figura 4.1 Diagrama de bloques de la interacción entre agentes y estación de monitoreo en SNMP [2]

El protocolo se comunica por medio de UDP a través de los puertos 161 y 162, y el agente debe ser configurado en los equipos para que el protocolo pueda empezar a recoger información. Los comandos *get* y *set* usan el puerto 161 y los avisos de trap el puerto 162. El uso de UDP hace que una consulta por SNMP no sea confiable, pero también utiliza mucho menos tráfico por consulta que un paquete TCP.

Cada agente administra una base de información de monitoreo (Management Information Base) que se compone de todas las variables que se pueden monitorear en el equipo. A cada variable se le asigna un identificador de objeto (Object Identifier, OID). Este identificador se escribe en notación punteada, y se puede ver la lista de números y las variables correspondientes a los equipos Cisco en [3] o en internet en [5]. Este protocolo es un estándar internacional y cada fabricante debe publicar sus OID públicamente. El esquema siguiente presenta el camino en el árbol estandarizado para

productos Microsoft. Como ejemplo, el OID para el objeto sysUpTime se representa como .1.3.6.1.2.1.1.3. El informe de la primer fase de la herramienta de monitoreo del Banco Popular tiene una explicación más concisa de estos conceptos básicos.

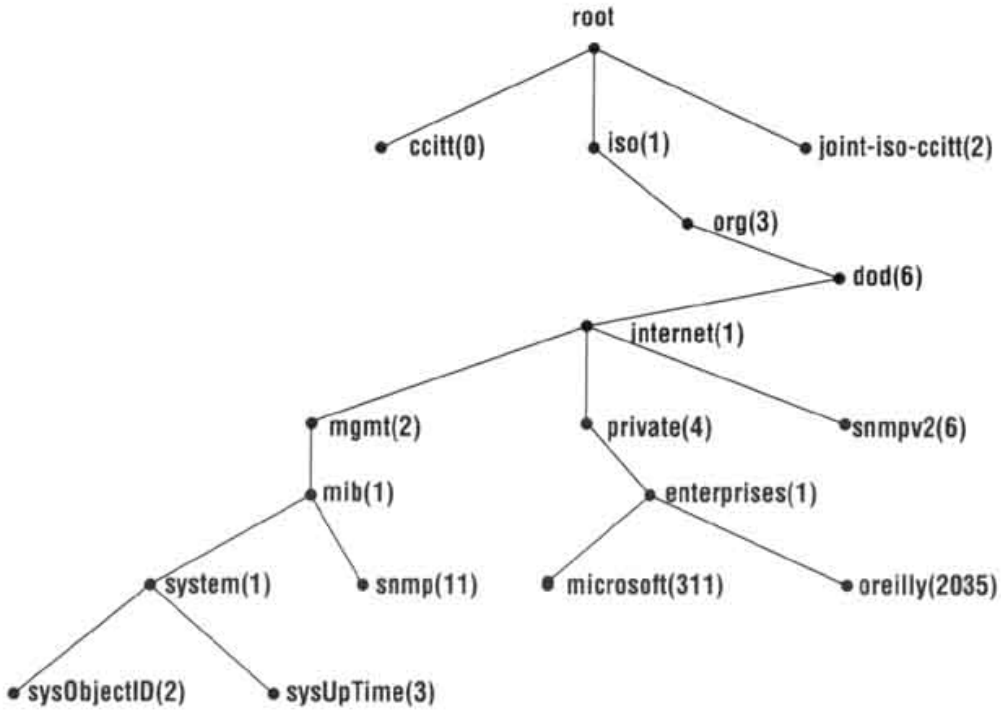


Figura 4. 2 Mapa de distribución de OID estandarizado [12]

3.3.3 Reemplazo de bibliotecas Internet Direct (Indy) por biblioteca Ararat Synapse como conector SNMP para Delphi

La biblioteca IdSNMP de Indy se usó con éxito en la primera fase de la herramienta de monitoreo. Sin embargo, no soporta el nuevo estándar, SNMPv3. Al preguntar por correo electrónico sobre esta nueva funcionalidad, sus desarrolladores declararon no estar interesados en soportarlo. Para resolver esta situación se utilizó la librería Ararat Synapse, gratuita y de código abierto, que soporta autenticación por MD5 y SHA en SNMPv3.

3.3.4 Tipos de bases de datos

El uso de bases de datos se aplica principalmente cuando hay una cantidad considerable de datos que almacenar y estos datos deben ser compartidos entre varios usuarios. Los motores de bases de datos se encargan de proveer una estructura para los datos y controlar el acceso a los mismos.

Los servidores de bases de datos relacionales varían en su funcionamiento y en el modo que permiten a los usuarios acceder a los datos. Hay dos tipos de servidores, remotos y locales.

En los servidores de base de datos remotos la información se guarda en una computadora diferente a la que accede a la información; los datos pueden inclusive estar distribuidos a través de una nube de servidores y en diferentes arquitecturas. Los servidores remotos presentan al cliente una interfase lógica común; la norma actual es el lenguaje SQL (Structured Query Language). Aunque SQL es un estándar desarrollado por ANSI (American Nacional Standards Institute) e ISO (Internacional Organization for Standardization), algunas compañías incorporan pequeños cambios en su sintaxis, como es el caso de Oracle ®, Interbase ® y Microsoft ® SQL Server, entre otros.

Los servidores locales residen en la misma máquina de la aplicación. El ejemplo más común es Microsoft ® Access ® y Paradox ®. Los servidores locales comparten el sistema de archivos con su cliente, mientras que en los servidores remotos el cliente y el servidor pueden usar diferentes sistemas de archivos.

Para escoger correctamente cual tipo de base de datos se debe implementar, se considera cuántos usuarios accederán los datos simultáneamente. Las bases de datos remotas están diseñadas para servir a varios usuarios al

mismo tiempo, manejar múltiples conexiones simultáneas, y proveen varios niveles de seguridad y acceso según el usuario que las consulta. También se necesita considerar la cantidad de datos y la velocidad de respuesta del servidor: las bases de datos locales son, en general, más rápidas, pero tienen menor capacidad y escalabilidad.

3.3.5 Integración, optimización, funcionabilidad.

Es de vital importancia el uso de hilos de procesamiento para que las aplicaciones que deben trabajar simultáneamente no se interrumpan entre sí y la aplicación sea de rápida ejecución a vista del usuario. Los hilos de procesamiento son la habilidad del sistema operativo de asignar tiempos de ejecución a varios procesos que desean efectuar operaciones en el CPU, de manera que cada uno lo consigue por corto tiempo; las diferentes funciones dan la impresión al usuario de ejecución simultánea debido a que las operaciones de las computadoras son mucho más rápidas que la percepción humana.

Se trabajará de cerca con el usuario final para crear un ambiente gráfico informativo, cómodo y de uso intuitivo. Cuando se diseñan interfaces se debe buscar que la información disponible sea estrictamente la necesaria, y si se requiere más información, sea fácil ubicarla e interpretarla. La herramienta debe ser capaz de recolectar información variada y específica, pero dar informes concisos y fáciles de entender. De esta manera, el administrador está conciente cuando hay un problema, y sabe dónde buscar los detalles que llevarán a su resolución.

3.3.6 Programación de aplicaciones con sockets

Por lo general, cuando se comunican equipos a través de IP se establece una comunicación de tipo cliente-servidor. Un socket es un punto de conexión lógico entre la aplicación y el protocolo IP con el cual se desea establecer comunicación.

Existen dos técnicas de programación de sockets, síncrona y asíncrona. El método asíncrono fue la norma en ambientes win16, debido a que no existía la capacidad multi-hilos. Por ello, al programador se le daba la tarea de manejar la comunicación y liberar el programa mientras espera la respuesta remota, sin posibilidad de ejecutar otra acción en toda la PC hasta tener éxito o declarar un error.

Con la llegada de win32 se hizo posible a los programadores usar sockets síncronos, pues win32 no pierde el control de la máquina mientras un programa espera una respuesta, sino que permite a varias aplicaciones correr en diferentes planos. Sin embargo, los programadores del Windows Sockets Standard rápidamente se dieron cuenta de que usando un hilo interno por cada conexión podían permitir al usuario del programa realizar otras acciones en su propio programa mientras se espera una respuesta o un tiempo de espera agotado. El método de tener un hilo principal para la interacción con el usuario pero crear hilos para conexiones por IP se convirtió en un standard recomendado de la programación orientada a internet.

Capítulo 4: Procedimiento Metodológico

En este capítulo se expone el proceso de diseño utilizado para llegar a la solución del problema; se explica, en forma breve, las consideraciones, ideas y limitaciones que llevaron a escoger la solución planteada.

4.1 Reconocimiento y definición del problema

Para definir los nuevos requerimientos de la herramienta de monitoreo se efectuaron entrevistas con el Coordinador del SAOR del BPDC, el Ing. Rodrigo Vargas Vásquez, y con el Ing. Alfonso Quesada Fernández, quien trabajó en la primera fase de la herramienta. La importancia del problema fue expuesta por ellos; qué funcionalidades se deseaban implementar, qué limitaciones tenía la solución anterior, qué avances se habían hecho desde la entrega del proyecto anterior.

Al entrar a trabajar en la empresa se tuvo siempre buena comunicación para entender limitaciones, esperanzas de funcionamiento y revisar detalles a medida que surgían. Se tuvo contacto con el resto del Subproceso y experiencia como otro funcionario de ella, y esto ayudó a pensar en las necesidades más concretas del departamento e incorporarlas a la herramienta.

4.2 Obtención y análisis de información

Al trabajar dentro del BPDC en el SAOR se tuvo acceso a los siguientes documentos:

- Diagramas de la red, tanto de oficinas remotas como de centrales.
- Acceso con contraseña a todos los equipos como parte de la subred de administración.

- Acceso ilimitado a internet, siempre observando las políticas de uso del BPDC.
- Computadora propia, que tomaría el lugar de NMS al terminar el proyecto.

Para tener una referencia del lenguaje Pascal, usado por Delphi, se usaron libros electrónicos y diversos sitios de internet. Esta elección se fundamentó en la primera fase; ofrecía facilidades para trabajar con diversas bases de datos y mucho material de apoyo. Además, existe una necesidad de continuidad entre fases.

La investigación más profunda sobre el protocolo SNMP se dio explorando la solución de la primera fase. En el plano teórico, con el currículo del programa CCNA4 de Cisco Learning Academy y documentos específicos elaborados por Cisco ®, y con investigación a través de buscadores de Internet en sitios independientes de vendedor. SNMPv3 fue el principal tema de estudio, pues era la innovación en esta fase. Luego, al descubrir que la biblioteca IdSNMP de Indy era insuficiente, se buscó una solución que incorporara SNMPv3 en ambientes Pascal. A pesar de que un ejemplo para SNMPv3 no había sido implementado en Ararat Synapse ®, se pudo contactar al autor y conjuntamente lograr un ejemplo específico a equipo Cisco ®.

En el proceso de selección de una base de datos se usó material encontrado en Internet, consejos del Ing. Alfonso Quesada y expertos en sistemas del Subproceso de Soporte Técnico del BPDC, y la ayuda de Delphi. La discusión de los puntos débiles de Ms Access ® fue la que guió la búsqueda de un motor que usara SQL. En la instalación y uso posterior, se utilizó la excelente documentación de MySQL y ejemplos en internet, junto con las listas de correo, para resolver dudas y generar mejoras. Para los problemas difíciles de resolver, la suscripción a una lista de correos de usuarios de MySQL mostró ser una herramienta mucho más eficaz que las búsquedas y artículos encontrados.

La lectura casual de la revista Cisco Packet llevó a descubrir un artículo [6] que hablaba de los retos que suponía diseñar una interfase para software de monitoreo; estas opiniones fueron discutidas con los usuarios finales y personal con ingeniería en sistemas. También con este personal se discutió la implementación de hilos; se investigó en internet y finalmente se concluyó que el uso de hilos de la primera fase estaba bien logrado, por lo tanto su forma de implementación en esta segunda fase se mantendría y expandiría.

Sobre los posibles problemas de resolución que se manejaban al principio, se notó al empezar a trabajar que existía una incongruencia con los datos dados en las primeras conversaciones con gente del SAOR. La pantalla de 42 pulgadas no era un televisor, como se pensaba, sino un monitor; por ende, no se necesitó una tarjeta sintonizadora de TV, como se había contemplado. El monitor presenta nativamente todas las resoluciones que le da la tarjeta de video de una computadora normal.

Se usó la experiencia de soporte del departamento y lo aprendido en cursos de Cisco por parte del practicante para poder señalar e incluir en la herramienta de monitoreo diferentes tipos de avisos y alarmas a los que ofrecía la primera versión. Por ejemplo, ahora la aplicación sabe que un enlace con problemas de saturación en horas pico, que por calidad de servicio (QoS) ocasiona la pérdida de paquetes ICMP, es una alarma leve de una condición transitoria que se debe analizar posteriormente. Un reporte SNMP que indica que una oficina ha perdido la comunicación a nivel de protocolo es una emergencia que requiere actos inmediatos por parte del administrador. Los distintos tipos de alarma y sus formas de avisar al administrador se discutieron con el SAOR.

4.3 Evaluación de las soluciones alternativas

Disponiendo de alternativas, es importante discriminar y fundamentar el camino elegido:

- Existen 2 protocolos ampliamente aceptados par el monitoreo de redes. Sin embargo, SNMP tiene mayor aceptación de la industria, apoyo de los equipos Cisco, mayor bibliografía disponible en varios niveles de especialización y aplicación desde un programa de alto nivel comprobada.
- Para las opciones del lenguaje de programación, cualquier programa de alto nivel que permitiera el uso de una biblioteca SNMP era factible, como es el caso de Visual Studio .net ® y C++. Sin embargo, el trabajo ya realizado anteriormente junto con la ventaja de que el trabajo nuevo será fácilmente asimilado por el departamento debido a su experiencia en este lenguaje dejan claro que Delphi es lo más conveniente. Es un ambiente acostumbrado a manejar bases de datos y no presentó problemas serios en adaptarse a una solución con MySQL y SNMPv3.
- La biblioteca IdICMP de Indy se utilizó pues no presentó ningún problema en adaptarse a la nueva fase. Sin embargo, IdSNMP si tuvo que ser reemplazada por Ararat Synapse para poder implementar SNMPv3. Esta librería fue escogida partiendo de que el software de desarrollo era Delphi, pues existen más librerías, pero para otros programas de desarrollo.
- Delphi, a través del sistema dbExpress, permite conectarse a varias bases de datos, como son Oracle, Ms SqlServer, Sybase, etc. La base de datos utilizada en la fase 2 debe ser un servidor de fácil mantenimiento, de soporte fácil y operación confiable. La instalación de MySQL es tan sencilla como descomprimir los archivos en una carpeta; la inicialización y terminación, por línea de comando. Al ser una aplicación de código abierto, soporte, ejemplos y actualizaciones son gratuitas y de fácil acceso.

- La etapa de conexión al TV y la compensación de cambios de despliegue al pasar de monitor a TV se disipó al notar que el TV, era en efecto, un monitor de pantalla plana. Lo que se tuvo que adaptar fue encontrar una resolución que permitiera varios elementos en pantalla, pero que diera legibilidad a una distancia de aproximadamente 2 metros de la misma. Además, asegurarse que los gráficos generados para la aplicación tuvieran el tamaño apropiado para su mejor visibilidad y que no aparecieran borrosos por mala ampliación.
- El diseño de la nueva interfaz obedeció a las sugerencias de los usuarios, combinado por el objetivo de hacer que la interfaz fuera muy intuitiva y sencilla de descifrar a primera vista. La nueva interfaz facilita toda la información disponible de los equipos al usuario que quiera explorar, pero en su pantalla inicial muestra sólo la información relevante para la operativa de la oficina.

4.4 Implementación de la solución

El procedimiento utilizado para implementar la solución se puede resumir en los siguientes pasos:

1 Primero, se estudió la información que entregó el BPDC al concretarse el acuerdo entre BPDC y la Escuela de Ingeniería Electrónica: su topología de red, su distribución de oficinas, sus documentos de control de equipo. Se comprobó que la red estaba bien documentada en archivos Visio y Excel, y se analizó la operativa normal del SAOR.

2 Se dialogó con el creador de la primera fase sobre los puntos fuertes y débiles de la misma. Se concedieron los códigos fuente y se procedió a estudiarlos, y a disipar dudas de sus funciones.

3 Se discutió con más detalle la visión del Subproceso sobre las nuevas características de monitoreo y de flexibilidad de la herramienta.

4 Se procedió a desarrollar aplicaciones sencillas que permitieran medir el dominio sobre las nuevas herramientas y protocolos necesarios.

5 Al dominar el uso de las librerías IdSNMP e IdICMP, se procedió a hacer una aplicación que hiciera el equivalente a la primera versión, y a partir de ella se empezó a experimentar cómo incluir las funciones deseadas. Se probó una primera versión del programa que usaba una hoja de cálculo para generar dinámicamente las oficinas, en vez de incluir su información en el código fuente.

6 Se trabajó en incluir funciones como telnet y pruebas de ping (ICMP manejado desde Windows) desde la aplicación, así como la habilidad de reubicar oficinas con la aplicación corriendo. Se hizo una presentación, lo que permitió observar reacciones del SAOR a una interfaz que dividía las oficinas por su ubicación según las provincias de Costa Rica.

7 Se hizo una lista de las funcionalidades logradas y las esperadas para la elaboración del segundo prototipo, que ya debía incluir funciones como la recopilación y almacenaje de datos por SNMP en una base de datos y monitoreo continuo de paquetes ICMP.

8 Verificada la funcionalidad básica de las herramientas conocidas, se investigó el motor de base de datos a usar y la forma de conectarse a ella a través de Delphi. Una vez lograda la comunicación, se hicieron exámenes de estabilidad, velocidad y consumo por registro.

9 Se procedió a diseñar un programa que usara al máximo la base de datos y que lograra la mínima cantidad de opciones definidas por código, para que lograra ser muy versátil y escalable.

10 Se definió la necesidad de hacer una aplicación para manejo de la base de datos para el administrador del sistema, de manera que pueda definir las opciones de monitoreo de cada equipo.

11 Se procedió a hacer una aplicación que, a partir de los datos de red encontrados en tablas de configuración, preparara las tablas necesarias y ejecute sólo el monitoreo pedido.

12 Se implementó un recolector de datos con el SNMP usando múltiples hilos, y un monitoreo ICMP simultáneo inteligente, con control sobre los intervalos de monitoreo. Ahora el sistema puede dar más información sobre el estado real de una oficina.

13 Confirmado el funcionamiento del recolector de datos y su estabilidad, se procedió a desarrollar la interfaz que permitiera desplegar los datos y tomar acciones pro-activas ante problemas.

14 Se probaron varios diseños de interfaz hasta que se logró llegar a un consenso con el SAOR. Con este diseño, se procedió a crear una interfaz que utilice la información de la base de datos para dibujar los enlaces remotos, y la información recolectada por SNMP e ICMP para enseñar el estado de la red.

15 Se implementó la opción de cambiar colores y opciones de aviso para que el usuario pueda cambiar la aplicación a su mejor gusto.

16 Se implementó un sistema de bitácora con alarma audible y email (configurables también) y la opción de llenar la información de la línea al hacer un reporte de fallo desde la aplicación.

17 Se implementó un sistema para exportar las bases de datos mensuales a un formato de uso generalizado, mantenimiento de las tablas viejas y avisar cuando el espacio de disco duro se acerca a niveles críticos.

18 Implementar los cambios en el servidor MySQL para tener dos interfaces gráficas: una para la pantalla y otra como herramienta LAN para cada miembro de SAOR, con opciones individuales, contraseñas y niveles de acceso.

19 Creación de dos manuales de usuario, uno para el administrador (y encargado) de la aplicación, y otro para el usuario normal del SAOR.

20 Entrega de la aplicación; exposición y capacitación sobre sus características y modo de empleo, y monitoreo del desempeño de la misma, tomando en cuenta los comentarios de los usuarios.

4.5 Re-evaluación y re-diseño

Como en todo proyecto, una vez concluido, se piensa que si se diera la oportunidad de desarrollarlo nuevamente, se podría hacer algo mejor. He aquí un comentario breve sobre los puntos generales del diseño que se piensa no fueron los óptimos:

1 La aplicación recolectora y la interfaz del usuario terminaron siendo aplicaciones distintas y separadas, pero esto no se evidenció desde el diseño, sino que se dio en pleno desarrollo de la herramienta. Esto debería tomarse en cuenta desde el principio para decidir que es lo óptimo para cada aplicación, pues pueden probarse varias combinaciones para obtener mejores resultados. Por ejemplo, el servidor central puede ser una máquina linux, muy segura, corriendo un script de SNMP e ICMP en ANSI C; en verdad no había un criterio preponderante para efectuarlo en Delphi, a exceptuar el conocimiento del lenguaje por el encargado de la herramienta. La interfaz en Delphi despliega los datos en la pantalla de monitoreo, pero esto tal vez sólo es necesario en el caso de la aplicación que irá a la pantalla gigante. Al usuario normal de SAOR, que no necesita ver la aplicación corriendo durante el transcurso del día, sino sólo cuando hay problemas, se le puede activar una interfaz vía Web para acceder a la información más importante.

2 La base de datos es la parte más sensible de la aplicación y la que más beneficia al sistema en general cuando se hacen optimizaciones. En este diseño se usaron muchas llaves basadas en texto, que son las mas ineficientes; se debieron haber hecho identificadores con números y que cada número estuviera vinculado a una oficina o equipo en otra tabla.

3 Hay muchas opciones para configurar MySQL de manera óptima para la aplicación, pero por ignorancia y falta de tiempo se utilizó una configuración estándar.

4 Usando adecuadamente los lineamientos de la programación orientada a objetos, se hubiera logrado crear una interfaz final más eficiente; esto es una observación de los ingenieros de sistemas del BPDC.

5 Este diseño empezó centrado en una tabla con una fila por equipo. Cada equipo tiene una o más interfaces, y más de un equipo puede ser de una oficina remota. Si el diseño hubiera empezado como una fila por interfaz, donde una interfaz pertenece a un equipo, la tabla sería más larga pero más eficiente; el diseño actual tiende a dejar espacios en blanco pues no todos los equipos tiene más de una interfaz.

6 No se contempló que el cuello de botella más grande de la aplicación sería la conexión entre Delphi y MySQL. La solución ofrecida por Borland carece de buen soporte; los desarrolladores no están interesados en lograr un buen producto final para MySQL, por lo que la base de usuarios no es tan extendida. Esto ha ocasionado que los mejores conectores hayan sido desarrollado comercialmente. Debido a problemas encontradas en el BPDC para adquirir estas soluciones, se optó por mantener una solución no ideal pero que cumple con los objetivos, sacrificando en áreas de eficiencia y estabilidad entre versiones. En las últimas etapas de desarrollo, se conocieron otras opciones, de código abierto, pero era muy tarde para incorporarlas en el código.

7 A la interfaz se le asignaron ciertas funciones que perfectamente se pudieron haber logrado en la aplicación recolectora; es probable que este cambio pueda ayudar a la estabilidad y rapidez de la herramienta.

Capítulo 5: Descripción detallada de la solución.

Este capítulo se centra en los detalles de la solución implementada. Primero se exponen los diseños opcionales para la aplicación, y luego se describe por qué los requerimientos llevaron al desarrollo de la solución final.

5.1 Análisis de soluciones y selección final

Las tres aplicaciones vigentes de la primera fase de la herramienta de monitoreo se exponen a continuación:

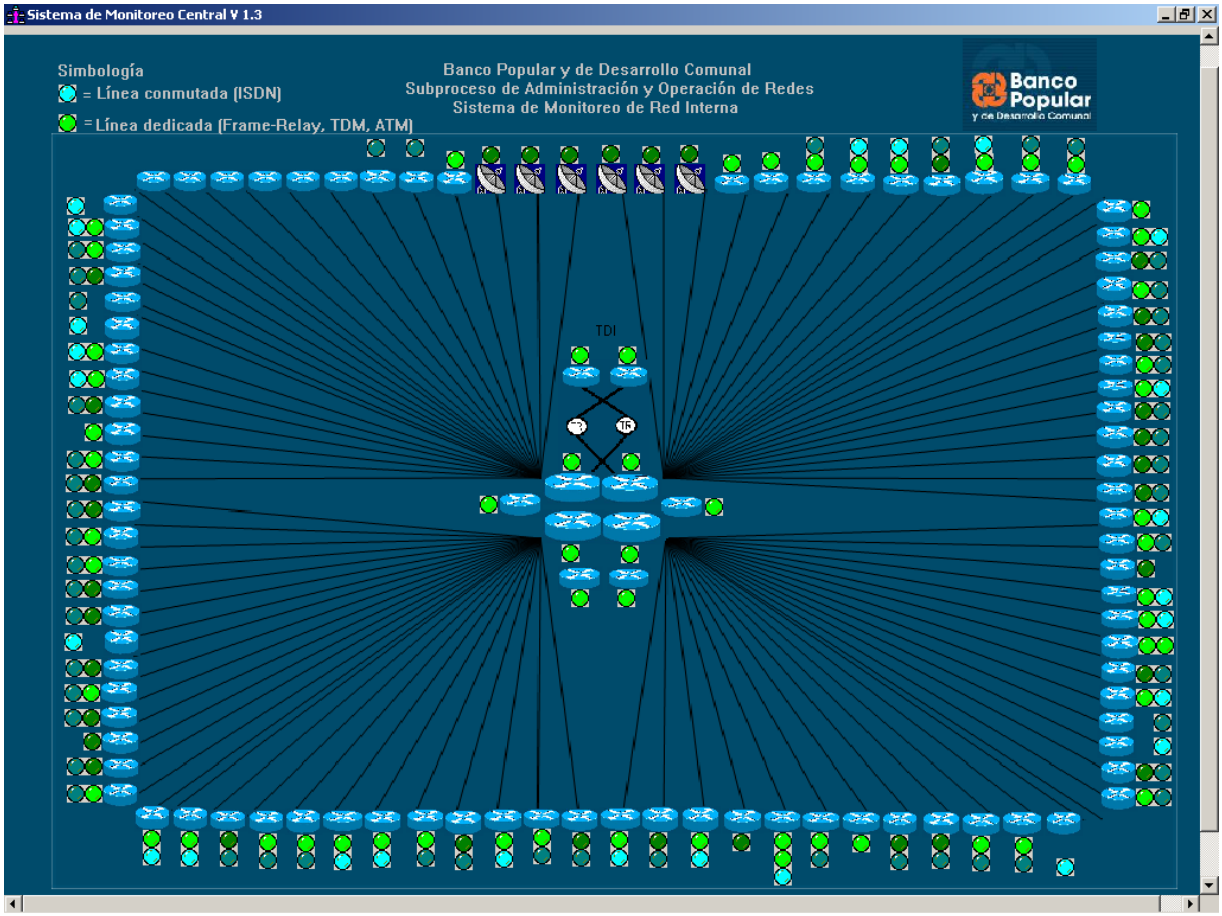


Figura 5. 1 Interfaz principal de la herramienta de monitoreo del BPDC, v1.3

La herramienta de monitoreo cuya interfaz se presenta en la figura 5.1 corre en una computadora separada de los cubículos del personal del SAOR. La computadora que corre esta herramienta está en un lugar visible, usando como monitor una pantalla gigante. La herramienta de monitoreo del SAOR tiene internamente en su código un listado de las direcciones IP de las interfaces conectadas al edificio central de Informática del BPDC. En su interfaz gráfica, tiene una luz indicadora para cada interfaz activa. Al arrancar, empieza un temporizador a ejecutar *echo requests* a cada dirección IP por medio de un hilo de procesamiento que no interfiere con el hilo principal de la interfaz. Estos *echo requests* han sido configurados con el máximo tiempo de espera para permitir una respuesta lenta de oficinas con problemas de enlaces saturados. El periodo de recolección de datos de esta aplicación es de aproximadamente 2:20 minutos.

Para enlaces seriales, utiliza color verde; si el enlace es ISDN de respaldo, usa color aqua. Cuando un enlace tiene un tiempo de espera agotado, la aplicación colorea a la luz indicadora en amarillo. Si un enlace tiene 3 tiempos de espera agotados seguidos, la aplicación le pone color rojo. Esto significa que, al perderse la comunicación de protocolo en un enlace, la aplicación dura siete minutos para confirmar esta información al usuario.

La razón por la que se tiene esta precaución es debido a que, por configuración, el QoS configurado en los equipos de enrutamiento del BPDC descarta *echo requests* cuando el enlace tiene saturado el ancho de banda del enlace. Un *echo request* rechazado no es sinónimo de una falla de enlace; puede ser un enlace saturado o puede ser que un equipo no responde por una falla del enlace. Esto obliga a los ingenieros de soporte a investigar por otro método el estado del enlace, convirtiendo a la primera fase de la herramienta en un sistema de detección de *posibles* problemas.

Cuando se desea ver cual enlace tiene problemas, se le posiciona el ratón encima del dibujo del enrutador, lo que hace que una ventanilla informativa con el nombre de la oficina se presente. Al no tener los nombres visibles todo el tiempo, obliga al usuario a acudir hasta el NMS para obtener esta información. No tiene otra forma de aviso que la visual; si nadie nota un cambio en la pantalla, pasa desapercibido.

Los problemas de saturación se dan debido a que los servicios del ICE y RACSA no han podido dar opciones de diferentes anchos de banda para áreas específicas, por lo que se deben manejar oficinas que saturan el enlace a ciertas horas. Sin embargo, es conveniente que la aplicación sepa dar prioridad a los diferentes tipos de fallos.

Fortalezas

- Despliegue claro de información de estado de todas las oficinas del BPDC.
- Interfaz de fácil manejo.
- Permite visualizar la activación de enlaces de respaldo.
- Da el máximo tiempo de espera en *echo request* para permitir que equipos lentos contesten.
- Código fuente sencillo de mantener.
- Buen aprovechamiento de la pantalla.

Debilidades

- No muestra el nombre de la oficina hasta que se posiciona el ratón sobre ella.
- Las oficinas no están ordenadas de alguna forma que facilite su ubicación.
- Podría desplegar más información útil, por ejemplo, el número de línea, que se usa para reportar enlaces con problemas a los proveedores.
- Al permitir el máximo tiempo de espera, el ritmo de refrescamiento es lento.
- No cambia su despliegue si el cable de red es desconectado (descubierto por accidente).

- No tiene otro método de aviso que el visual, por lo que una falla puede pasar desapercibida si no se está atendiendo el monitor

Continuando con los avances logrados desde la entrega de la primera fase, se consolidaron en una sola aplicación tres aplicaciones que habían sido creadas por aparte para la fase anterior: un graficador de ancho de banda, un confeccionador de reportes de uso de CPU y RAM y un display de valores de temperatura en los routers centrales.

Los datos de CPU, RAM y temperatura son instantáneos; esto es, cuando se activa un botón, los programas ejecutan un ciclo y devuelven un muestreo de los datos actuales. No se puede ver un historial de estos datos, pues estas nuevas aplicaciones corren sin usar una base de datos. En su funcionamiento utilizan la memoria RAM del programa por el tiempo en que se ejecuten. Únicamente el graficador de ancho de banda continúa un muestreo desde el momento en que se ejecuta por primera vez.

Debido a la forma en que se organizó la base de datos en Ms Access ®, se llegaba en pocos días al tamaño límite de archivo y colapsaba la aplicación. Esto debido a que el tamaño límite de una tabla en Access 2000 es 1 GB y el diseño sólo usaba una tabla, sin exportación de datos para solventar esta limitación.

Cuando se deseaba usar el graficador de ancho de banda, se debían alterar los datos del programa desde el código fuente para que coincidieran con los del equipo. Las aplicaciones que efectúan reportes de CPU / RAM y temperatura tiene las direcciones IP de los equipos dentro del código, por lo que cualquier cambio en direccionamiento necesita de interacción del programador.

Fortalezas

- Permite ver gráficos de ancho de banda de cualquier oficina desde un tiempo determinado en adelante. Ideal para monitoreos donde se desea comprobar el efecto de una cambio en la red.
- Permite ver en una sola pantalla los valores actuales de CPU y RAM de los equipos del BPDC.
- Permite monitorear la temperatura de operación de los enrutadores centrales del BPDC.

Debilidades

- No se pueden ver datos que han ocurrido antes de iniciada la aplicación.
- Las direcciones IP e información usada por SNMP están imbuidas en el código; necesita mantenimiento del programador para acoplarse a cambios.
- La única forma de conservar los datos obtenidos es tomando imágenes de la pantalla.
- No se puede ver el comportamiento histórico del uso de CPU, RAM y temperatura de los equipos.

Considerando los objetivos específicos planteados por el SAOR para este proyecto, en resumen se necesita en la segunda fase:

1. Implementar una base de datos que guarde los datos recogidos por SNMP, como son uso de CPU, RAM, ancho de banda y temperatura. La idea es que se puedan incluir más variables, como el estado administrativo de la interfaz, estado del protocolo, cantidad de errores en la interfaz.
2. Permitir al administrador ver la información de la base de datos con gráficos y manipular la información para crear informes estadísticos en la manera en que SAOR crea más conveniente.

3. Permitir que el administrador final, que no es la misma persona que el programador, pueda añadir o eliminar variables de monitoreo de manera externa al código de la aplicación.
4. Reunir las aplicaciones pasadas para que las diferentes funciones se encuentren disponibles desde una sola interfaz de usuario, que reúna la información importante para el monitoreo de red.
5. Permitir al administrador un control sobre el monitoreo para optimizar el uso de recursos disponibles.
6. Permitir el uso de telnet desde la aplicación.
7. Corregir problemas de seguridad de SNMPv1.

A continuación se explican las opciones consideradas como soluciones viables y la opción que predominó para el diseño, con su fundamento:

- *Implementar una base de datos (punto 1*): las opciones son variadas; a pesar de que Ms Access ® puede soportar varias tablas de 1 GB cada una, es preferible usar un motor de bases de datos que esté diseñado para volúmenes grandes para no tener problemas a futuro.

  Para el SAOR es más conveniente usar un servidor que no necesite licenciamiento ni mantenimiento de parte de otros subprocesos, sino que pueda administrarse localmente, para evitar burocracia interna. Se notó que entre las opciones de código abierto respetables, destaca MySQL por estabilidad, licenciamiento, satisfacción de usuario, disponibilidades de conexión con lenguajes de programación y documentación. Descartados Oracle y MS SQL Server, principales motores comerciales, por su alto costo. Además, MySQL es una opción más viable que PostGreSQL ® y TinySQL ®, otras opciones populares de código abierto, por tener más documentación y usuarios, lo que garantiza que el código se mantiene vigente y con soporte.

En las pruebas preliminares se realizó un prototipo que usaba un archivo Excel para guardar las opciones de configuración; tenía la ventaja de que Excel es un formato conocido y se puede proteger con contraseña, lo que facilitaría al usuario final la actualización de datos, pues es un ambiente conocido. Sin embargo, es una solución que recarga la velocidad de la herramienta y obliga a que la computadora lo tenga instalado. Su desempeño general no es el óptimo para manejar grandes volúmenes de datos, si se compara al rendimiento de un motor de base de datos. Finalmente se descartó cualquier uso de Excel por la sencillez y rapidez que mostró la conexión Mysql y Delphi; descartar su uso ahorra una licencia de Ms Office al BPDC y abre más posibilidades a la herramienta, sobre todo si se decide mejorar la misma.

Al escoger MySQL, se abre una gama de posibilidades que se extienden más allá de los lineamientos del proyecto. Este motor tiene versiones en muchos sistemas operativos, y puede usarse localmente o como servidor de una red, donde transfiere información por el puerto 3306. Esto posibilita la separación, no sólo lógica, sino también física, de la interfaz gráfica de la herramienta, lo que permitirá que la aplicación tenga más opciones de presentación; por ejemplo, consultas de la red vía Web, que pueden algún día pasar de la LAN.

- *Permitir el monitoreo de varias variables por SNMP, y configuración de la cantidad de las mismas (puntos 1 y 3):* Los OID que se usan en SNMP son cadenas de números que no presentan problema para ser guardadas en una base de datos. Lo más complicado de este requerimiento es pensar cómo diseñar las tablas donde la información monitoreada de cada oficina va a ser guardada, si existe la posibilidad de que cambien las columnas, según la cantidad de interfaces de cada equipo.

  Por ejemplo, un administrador puede decidir no monitorear los errores de salida en una interfaz; pero después de una semana, cambia de opinión y

decide que si se va a incluir dicho OID en el monitoreo. Si la columna no estaba creada en una tabla, debe crearla, con lo que potencialmente se obtienen varias tablas no uniformes. Esto es un problema: como asegurarse de que el código fuente sepa encontrar toda la información en tablas que no han sido creadas uniformemente. También está el caso de un OID que ya no se piensa monitorear; ¿se debe eliminar la columna anterior, perdiendo datos de monitoreo?

Para prever esta posibilidad se implementó que el código asuma que todas las variables posibles serán monitoreadas en alguna ocasión. Primero se definió que hay dos tipos de OIDs: algunos son variables con el tiempo, y otros son mucho menos variables. Por ejemplo, el ancho de banda que consume una interfaz en un período de tiempo tiende a no ser constante si el periodo va aumentando, y aunque se pueda tener una idea de su variación promedio, su valor instantáneo depende de muchos factores. En cambio, el nombre de un equipo o la cantidad de memoria Flash instalada son cambios deliberados de la administración cuyo valor permanece igual por largos periodos de tiempo.

Con esta observación, se preguntó a los encargados del SAOR qué variables les interesaba más monitorear de sus equipos. A partir de esta información, se recopiló una selección de OIDs, expuestos en las tablas 5.1 y 5.2, que resultan útiles a la hora de inspeccionar el comportamiento diario de un equipo, y que conforman la base de datos desde la cual se fundamenta el diseño del programa:

Tabla 5. 1 Tabla de OIDs de *monitoreo* (su valor es dinámico)

Nombre_oficial	Descripción	OID
cpmCPUTotal1minRev	CPU USO 1 MINUTO Promedio de 1 minuto de uso de CPU	1.3.6.1.4.1.9.9.109.1.1.1.1.7.1
freeMem	MEMORIA RAM LIBRE Memoria RAM libre (show processes memory)	1.3.6.1.4.1.9.2.1.8.0
ifAdminStatus	ESTADO LINEA ADMINISTRATIVO Estado administrativo de la interfase x.	1.3.6.1.2.1.2.2.1.7.x

	1=up 2=down 3=testing	
ifOperStatus	ESTADO LINEA OPERATIVO line protocol up - down 1 2 3 = ifAdminStatus 4=unknown 5=dormant 6=notPresent	1.3.6.1.2.1.2.2.1.8.x
locIfInBitsSec	INTERFAZ ANCHO DE BANDA ENTRANTE Cantidad de Bytes/s entrantes a la interfase x	1.3.6.1.4.1.9.2.2.1.1.6.x
ifInErrors	INTERFAZ ERRORES ENTRANTES Total de errores entrantes en la interfase x	1.3.6.1.2.1.2.2.1.14.x
locIfOutBitsSec	INTERFAZ ANCHO DE BANDA SALIENTE Cantidad de Bytes/s salientes por la interfaz x	1.3.6.1.4.1.9.2.2.1.1.8.x
ifOutErrors	INTERFAZ ERRORES SALIENTES Total de errores salientes en la interfase x	1.3.6.1.2.1.2.2.1.20.x
ciscoEnvMonTemperature StatusValue	TEMPERATURA Medición de temperatura en grados centígrados	1.3.6.1.4.1.9.9.13.1.3.1.3.x
ciscoEnvMonTemperature State	TEMPERATURA Estado del termómetro 1: normal 2: peligro 3: critico 4: apagando 5: no presente 6: no funciona	1.3.6.1.4.1.9.9.13.1.3.1.6.x
ciscoEnvMonVoltageStatu sValue	VOLTAJE Valor actual del voltaje de la fuente interna x	1.3.6.1.4.1.9.9.13.1.2.1.3.x
ciscoEnvMonVoltageState	VOLTAJE Estado de los voltímetros 1: normal 2: peligro 3: critico 4: apagando 5: no presente 6: no funciona	1.3.6.1.4.1.9.9.13.1.2.1.7.x
ciscoEnvMonSupplyState	FUENTE DE PODER Estado: 1: normal 2: peligro 3: critico 4: apagando 5: no presente 6: no funciona	1.3.6.1.4.1.9.9.13.1.5.1.3.x
ciscoEnvMonTemperature StatusDescr	TEMPERATURA Descripción del punto de medición de temperatura en los routers capaces (tarjeta EnvMon)	1.3.6.1.4.1.9.9.13.1.3.1.2.x
ciscoEnvMonTemperature Threshold	TEMPERATURA Valor mas alto de temperatura que puede registrar el equipo antes de apagarse automáticamente	1.3.6.1.4.1.9.9.13.1.3.1.4.x
ciscoEnvMonVoltageStatu sDescr	VOLTAJE Descripción del punto de voltaje medido x	1.3.6.1.4.1.9.9.13.1.2.1.2.x
ciscoEnvMonVoltageThres holdLow	VOLTAJE Valor mínimo de voltaje en la fuente interna antes de que el equipo se apague automáticamente	1.3.6.1.4.1.9.9.13.1.2.1.4.x
ciscoEnvMonVoltageThres holdHigh	VOLTAJE Valor máximo de voltaje en la fuente interna antes de que el equipo se apague automáticamente	1.3.6.1.4.1.9.9.13.1.2.1.5.x
ciscoEnvMonVoltageLastS hutdown	VOLTAJE Valor guardado en NVRAM al apagarse el equipo, aun en apagados de emergencia.	1.3.6.1.4.1.9.9.13.1.2.1.6.x
ciscoEnvMonSupplyStatus Descr	FUENTE DE PODER Descripción de la fuente externa x	1.3.6.1.4.1.9.9.13.1.5.1.2.x

Tabla 5. 2 Tabla OIDs de *información* (valores estáticos)

Nombre_oficial	Descripcion	OID
SysLocation	EQUIPO UBICACION Ubicación del equipo (configurada previamente)	1.3.6.1.2.1.1.6.0
SysDcr	EQUIPO DESCRIPCION Descripción del	1.3.6.1.2.1.1.1.0

	equipo. Similar a (show version)	
whyReload	REINICIO CAUSA Permite saber la causa de reinicio	1.3.6.1.4.1.9.2.1.2.0
ciscoImageString	IOS NOMBRE Nombre común de la imagen del IOS	1.3.6.1.4.1.9.9.25.1.1.1.2.2
no especificado	EQUIPO MODELO Familia Cisco del Equipo	1.3.6.1.4.1.9.9.25.1.1.1.2.3
no especificado	CAPACIDADES IOS Características sobresalientes del IOS	1.3.6.1.4.1.9.9.25.1.1.1.2.4
no especificado	IOS VERSION Versión exacta del IOS en ejecución	1.3.6.1.4.1.9.9.25.1.1.1.2.5
ciscoFlashDeviceSize	MEMORIA FLASH TAMAÑO Tamaño total de la memoria FLASH instalada en bytes	1.3.6.1.4.1.9.9.10.1.1.2.1.2.1
ciscoFlashDeviceDesc	MEMORIA FLASH TIPO Tipo de memoria FLASH instalada o removible	1.3.6.1.4.1.9.9.10.1.1.2.1.8.1
ifNumber	INTERFAZ INDICES Cantidad de interfaces vistas por SNMP en el equipo	1.3.6.1.2.1.2.1.0
sysObjectID	EQUIPO Regresa un valor que permite saber exactamente que equipo es.	1.3.6.1.2.1.1.2.0
ifDescr	INTERFAZ DESCRIPCION Descripción de cada interfaz del equipo. La x se substituye en la ejecución.	1.3.6.1.2.1.2.2.1.2.x

Es una particularidad de SNMP el que varios OID dependen del número SNMP de interfaz que se desea monitorear en el equipo; estos números de interfaz asignados por SNMP son diferentes para cada configuración. En los casos en que un OID debe completarse con esta información, se decidió terminar con una “x” los OIDs incompletos.

Por ejemplo, si estamos buscando cual es el número SNMP para una interfaz Fa0/0 en un equipo dado, se empieza a preguntar el OID *ifDescr* desde el número x = 1 y se incrementa hasta que la respuesta, que es una descripción en palabras, sea exactamente Fa0/0.

La tabla 5.3 es un ejemplo de los números SNMP para un enrutador 2600 Cisco que tiene conectados a si cajeros y una línea de respaldo:

Tabla 5. 3 Ejemplo de números SNMP para un router c2600

Número SNMP	ifDescr
1	BRI0/0
2	Ethernet0/0
3	TokenRing0/0
4	BRI0/0:1

El número puede seguir incrementando y con esto se pueden observar todas las interfaces disponibles del equipo, incluso las interfaces lógicas como Null0 y sub-interfaces seriales.

Siguiendo con el diseño que contempla columnas que pueden cambiar, una vez definida la tabla de OIDs de monitoreo, se puede crear una estructura de la tabla de almacenamiento. Los criterios para el diseño de esta tabla de almacenamiento fueron usar una tabla por equipo monitoreado y que la vida útil de esa tabla fuera de un mes. Después de este periodo, sería exportada a un formato conveniente y se reemplazaría la tabla en la base de datos con una nueva tabla.

La elección de un mes, y una tabla por equipo, responden a que la mayoría de la información que precisa al SAOR ha ocurrido recientemente; normalmente, se buscan datos de eventos que han pasado en la última semana. Sin embargo, para las funciones de comunicación de resultados a niveles de gerencia, normalmente se dan reportes en términos de meses: reportes mensuales, bi-mestrales, tri-mestrales, anuales. Una cantidad de 12 reportes por año, por equipo, es manejable y cómoda de usar, en contraste con tablas que duren una semana o 3 meses.

Los puntos en contra de tablas muy grandes que concentran información de muchos equipos son que se vuelven ineficientes en tareas de escritura (que es el caso) y que en el caso de una falla y corrupción de datos, se pierde mucha

información en un solo incidente. Además, es inconveniente graficar muchos datos cuando se busca una falla o el comportamiento de un día; claramente, para la elaboración de gráficas se debe poder acotar el intervalo.

Para poder dar la flexibilidad al administrador de poder añadir variables a su antojo, se ha decidido que se elaborarán tablas individuales que permitan insertar todas las respuestas a OIDs que se encuentren en la tabla de configuración *oids_monitoreo*. Esto significa crear una columna para cada OID en esta tabla que no contenga x, y una columna para cada interfaz del router que use en su monitoreo el número SNMP de una interfaz. Por ejemplo, *freeMem* usa una columna, mientras que *ifOperStatus* usará cuántas interfaces diferentes tenga el enrutador a monitorear.

Se investigó que las interfaces que interesan al SAOR son las interfaces WAN: seriales y RDSI. Las oficinas más exigentes tienen a lo más 3 interfaces, por lo que se hizo un formato estándar que crea 3 columnas por OID con "x". Para nombrar cada columna, se creó otra columna en la tabla de oids_monitoreo. La columna de la tabla 5.4 llamada *Nombre_en_columna_monitoreo* se usa para elaborar las tablas de la herramienta, con la lengitud elegida en *Numero_caracteres_columna*.

Tabla 5. 4 Nombres para columnas generadas automáticamente de OIDs de monitoreo

Nombre_oficial	**Nombre_en_columna_monitoreo**	**Numero_caracteres_columna**
cpmCPUTotal1minRev	USO_CPU_1min	3
freeMem	RAM_LIBRE	20
ifAdminStatus	ESTADO_ADMIN_x	1
ifOperStatus	ESTADO_PROTOCOLO_x	1

Nuevamente, la "x" sirve para especificar al programa que va a generar las tablas, que necesita hacer 3 copias de esa columna, pues hay a lo más tres interfaces en el equipo. Resulta muy fácil a nivel de programador revisar si el último carácter de una palabra es una "x".

Con esto, se puede elaborar una rutina que cree tablas de almacenamiento que obedezcan a los OID disponibles. Esta rutina debe ejecutarse después de preguntarle al administrador si está listo para empezar el monitoreo con las opciones disponibles.

Para que este método funcione, debe encontrarse la información de número SNMP guardada con anterioridad para cada equipo que va a ser monitoreado. De esta manera, se puede recrear el OID necesario para encontrar la información deseada en la interfaz deseada en una consulta SNMP. Por ende, esta lista depende de que exista otra lista con al menos un identificador de enrutador, una dirección IP a la cual dirigir la consulta SNMP, y números SNMP para cada interfaz. Pronto se retomarán los requerimientos de esta nueva tabla de equipos a monitorear.

Para poder monitorear variables como temperatura y voltaje, se necesita que el equipo tenga instalado una tarjeta de monitoreo ambiental (Environmental Monitor Card). Como no todos los equipos la tienen, se debe colocar una columna en el listado de equipos a monitorear que confirme o niegue su existencia. Debido a que la tarjeta tiene 6 puntos de medición de temperatura y 2 de voltaje para cada “x” en sus OIDs, se puede notar que estos equipos tienen tablas con 18 columnas más que los equipos que no las tienen. Normalmente estas tarjetas se instalan sólo en los routers más críticos de la empresa. En el caso del BPDC, son 4 equipos las que tienen esta salvedad, pero de esta manera se permite que se cambie la tarjeta a otro equipo o que equipos nuevos tengan esta función, y se adapten sin problemas a la aplicación.

- *Permitir la visualización gráfica de los datos recolectados y la capacidad de generar informes estadísticos a partir de los datos recogidos (punto 2):* ya en

la primera fase se había permitido la graficación del ancho de banda desde Delphi. Para la segunda fase, se permite la graficación de cualquier dato que se encuentre en la tabla de datos de almacenamiento desde Delphi, dejando que el usuario especifique el intervalo de tiempo deseado. No se cambió la forma de hacerlo pues la solución desde Delphi, con los componentes nativos, se queda corta de las verdaderas capacidades del control TChart. Sólo se añadió la visualización del valor de los puntos que conforman el gráfico y la capacidad de graficar cualquier valor en la base de datos que venga de un OID dinámico.

En lo que respecta a informes estadísticos se dialogó con todos los miembros del SAOR para encontrar un formato de reporte que los permitiera obtener la información que necesitaban. Finalmente se llegó a dos tipos de reporte: una exportación de cada tabla mensual a un archivo CSV, que toma menos espacio y es más rápido de crear que un XLS; y una aplicación generadora de reportes que toma datos de una base de datos actual o un CSV de respaldo, y crea un XLS por demanda, con las estadísticas más importantes para el SAOR. Esto es, una tabla con varios parámetros de monitoreo y valores porcentuales promedio y pico; hora en que ocurrió el valor pico, y según el valor pico, el estado de la oficina según parámetros recomendados; esto, para cualquier intervalo de tiempo y nombre de archivo. En el caso de querer reportes de más de un mes, el interesado debe unir los datos en un sólo archivo antes de usar la aplicación.

La ventaja de este método es que se no se limita al usuario a un tiempo o gráfico; tiene la opción de crear sus propios gráficos, operaciones estadísticas o intervalos de observación. Se había manejado la idea de hacer reportes diarios, semanales, mensuales, trimestrales, anuales en Excel; pero el volumen de información requería más espacio y mantenimiento que la base de datos propiamente, y la complejidad de programación y procesamiento

durante la elaboración de informes no coincidía con el beneficio esperado de los mismos.

La solución con CSV se prefiere porque hay rutinas de importación/exportación directa entre MySQL y este formato, por lo que se pueden recargar las tareas de procesamiento al motor de base de datos con comandos SQL. Esto logra que se hagan informes bajo demanda sólo de los equipos e intervalos de interés; evita desperdicios que roben espacio de disco a la base de datos, lo que conlleva a menos mantenimiento de parte del administrador. Además, el formato CSV se usa en más aplicaciones que Ms Excel, inclusive en ambientes Linux, lo que lo hace más exportable.

- *Reunir las aplicaciones separadas en una sola interfaz gráfica multifuncional (puntos 4 y 6):* En la primera fase del proyecto cada aplicación requería que el usuario indicara el equipo en el cual estaba interesado, por aparte. La meta en esta fase es que al escoger un equipo, sólo una vez, se pueda acceder a toda su información de monitoreo fácilmente.

  Esta solución debía reunir ciertos atributos: debe ser efectiva reuniendo toda la información de un equipo u oficina cuando se espera que lo haga. Debe ser intuitiva y fácil de usar; no se puede esperar que el usuario, por ejemplo, digite el nombre del equipo o que seleccione uno de entre una lista con cientos de equipos. Además, debe cumplir los objetivos de la interfaz en que debe mostrar sólo la información necesaria en el formato más adecuado para cada requerimiento del usuario.

  Esto se logró con el uso de componentes en la interfaz que simulan el comportamiento de links Web; cada botón se crea reflejado en un equipo, oficina o interfaz; al hacer clic, el programa reconoce que botón le ha hecho un evento, y procede a llenar un cascarón multiuso con la información

correspondiente. Una vez dentro de ese cascarón, se pueden elegir que información se desea ver con más detalle: gráficos varios, uso actual de CPU, RAM, estado de los enlaces, o revisión de la información contenida en la base de datos. Asimismo, funcionalidades como el acceso directo a telnet y la capacidad de utilizar el ping de Windows se han incorporado dentro del cascarón; al pulsar el botón, se recoge desde la base de datos toda la información del equipo en cuestión y se crea un centro de monitoreo especializado en una pantalla aparte, todo a un clic de la interfaz principal.

- *Permitir variar los tiempos de intervalos de monitoreo (punto 5):* para que el administrador verdaderamente pueda configurar y adaptar la herramienta a sus necesidades de monitoreo, debe ser capaz de definir con exactitud y para cada enlace, cuanto tiempo ha de esperar un tiempo de espera agotado de ICMP y de SNMP. Por ello, se guarda en la base de datos un valor en milisegundos de tiempo de espera agotado máximo para cada enlace y para una consulta SNMP; las consultas SNMP se pueden hacer a cualquier dirección IP de un equipo, pero por razones de confiabilidad lo recomendable es hacerlo a una dirección de Loopback.

  Cambiar los tiempos de espera permite al administrador evitar que un enlace que tradicionalmente es lento esté generando alertas innecesarias, pero que si avise de incrementos en latencias en enlaces de alta capacidad que no deberían tener problemas. Al configurar correctamente los tiempos de espera, la aplicación hace los ciclos de monitoreo con los tiempo óptimos para obtener los resultados que el administrador desea.

  Esto permite al administrador flexibilidad en su estrategia de monitoreo: la primera fase asumía que la mejor estrategia era dar un tiempo de espera máximo. En verdad, es mejor definir un tiempo de espera individual que refleje la realidad cotidiana del enlace, pero monitorearlo más seguido; si el enlace

está saturado, por la configuración de QoS igual se va a perder la respuesta ICMP; pero si está disponible, contestará rápidamente. Con este método se logra hacer un monitoreo ICMP completo de todas las oficinas en mucho menos tiempo que con el método del máximo tiempo de espera y la herramienta percibe más rápidamente los problemas en cualquier oficina.

La ventaja de tener un ciclo de monitoreo corto es que se puede controlar el tiempo muerto entre ciclos para lograr el muestreo deseado. Por ejemplo, si se quiere monitorear un equipo cada 60 segundos, y se sabe que en general un monitoreo dura 10 segundos, se configura un tiempo muerto de 50 segundos. Con ciclos largos, es inconveniente tener tiempos muertos, debido a que el tiempo de monitoreo conveniente en verdad es menor a lo que dura un ciclo.

Este principio se aplica de la misma manera para el monitoreo SNMP; sin embargo, si se toma en cuenta que hay un promedio de cuatro *echo requests* efectuados por oficina, pero 16 consultas SNMP, se puede notar que por lo general el monitoreo SNMP es más lento. Por ello, se ha colocado un control de tiempos muertos por tipo de oficina: ciertos tipos de oficina son prioridad para la operativa del BPDC. Esto permite, por ejemplo, que los Centros de Servicios Financieros, que son los que manejan más volumen de transacciones y tienen mejores enlaces, tengan monitoreos muy continuos; mientras que los enlaces de Ventanillas, que tienen características muy variables y normalmente no tienen alta prioridad antes otras fallas por su bajo volumen de transacciones, pueden tener intervalos más espaciados. En la tabla 5.5 se pueden observar cuantas oficinas de cada tipo posee el BPDC.

Tabla 5. 5 Cantidad de oficinas por tipo del BPDC

Tipo	**Cantidad**
Centros de Servicios Financieros (CSFs)	11
Sucursales	18
Periféricas	37

Ventanillas	18

Es importante destacar que el uso de hilos separados de procesamiento es absolutamente necesario para que una sola aplicación pueda monitorear por ICMP y SNMP al mismo tiempo. La posibilidad de que el mismo programa tenga información simultánea de los dos protocolos permite saber con certeza cuando un enlace de un equipo está caído, sólo saturado o el equipo en sí está totalmente incomunicable, lo que supone una gran diferencia con respecto a la primera fase.

- *Consideraciones de seguridad (punto 7):* El uso de SNMPv1 permite a un intruso con un sniffer básico capturar la comunidad SNMP de un ente administrador de red. Por ello, se recomienda sólo usar la opción read-only en SNMPv1, pues una intercepción de una comunidad con permisos de escritura facilita a un usuario no autorizado esquivar las protecciones AAA de un equipo Cisco y efectuar todo tipo de cambios no autorizados en la configuración. Por ello SNMPv1 ha sido duramente criticado. Asimismo, Telnet no es una forma segura de acceder a un equipo pues transmite toda la información en texto claro.

  Para solventar estos huecos de seguridad se ha hecho un esfuerzo por usar SNMPv3 y SSH en los equipos del BPDC. SNMPv3 se activa en una casilla de la información de los equipos; el uso de Putty, un cliente SSH que permite empezar conexiones desde la línea de comando, se puede configurar en las opciones del programa.

  Es de lamentar que Ararat Synapse no soporta nativamente las características de encripción de datos que se han definido como opciones de SNMPv3 en el estándar. Soporta el uso de autenticación, ejecutando un hash MD5 o SHA de la contraseña del usuario, pero el resto de la información es visible a un

sniffer; sólo la contraseña está oculta. Conversando con el SAOR, se concluyó que esta característica no es prioridad para ellos, por lo que con las características de hashing de la contraseña se consideran satisfechos.

La recomendación que se hace en este caso es implementar, por aparte, las librerías de encriptación disponibles para Delphi. Sin embargo, como esta opción no tiene apoyo de quien controla las configuraciones de los equipos, no tiene sentido gastar recursos en algo que no se piensa implementar. Asimismo, no todos los equipos soportan SSH, por lo que es necesario dejar telnet como una opción.

También se pueden usar otras librerías que incorporan la funcionalidad de encriptación nativamente, pero para otros lenguajes: particularmente para Perl, Java y C hay varias disponibles. Elaborar esta herramienta en un lenguaje como Java permitiría ejecutarlo en cualquier plataforma (Windows, Linux, Unix, Solaris, BSD, etc.) con lo que se lograría una solución más completa. Sin embargo, esto involucra un esfuerzo extra de quien administra la herramienta, y se quiere que la transición sea lo más sutil posible.

Es importante mencionar que el sistema es una herramienta de monitoreo de equipo de red; éste equipo está ya instalado y configurado, y no es necesario instalar un módulo físico para lograr el monitoreo, sino que se aprovechará por software un protocolo estandarizado. Por ello, este trabajo no necesita una etapa de hardware creada por el estudiante.

5.2 Descripción del software

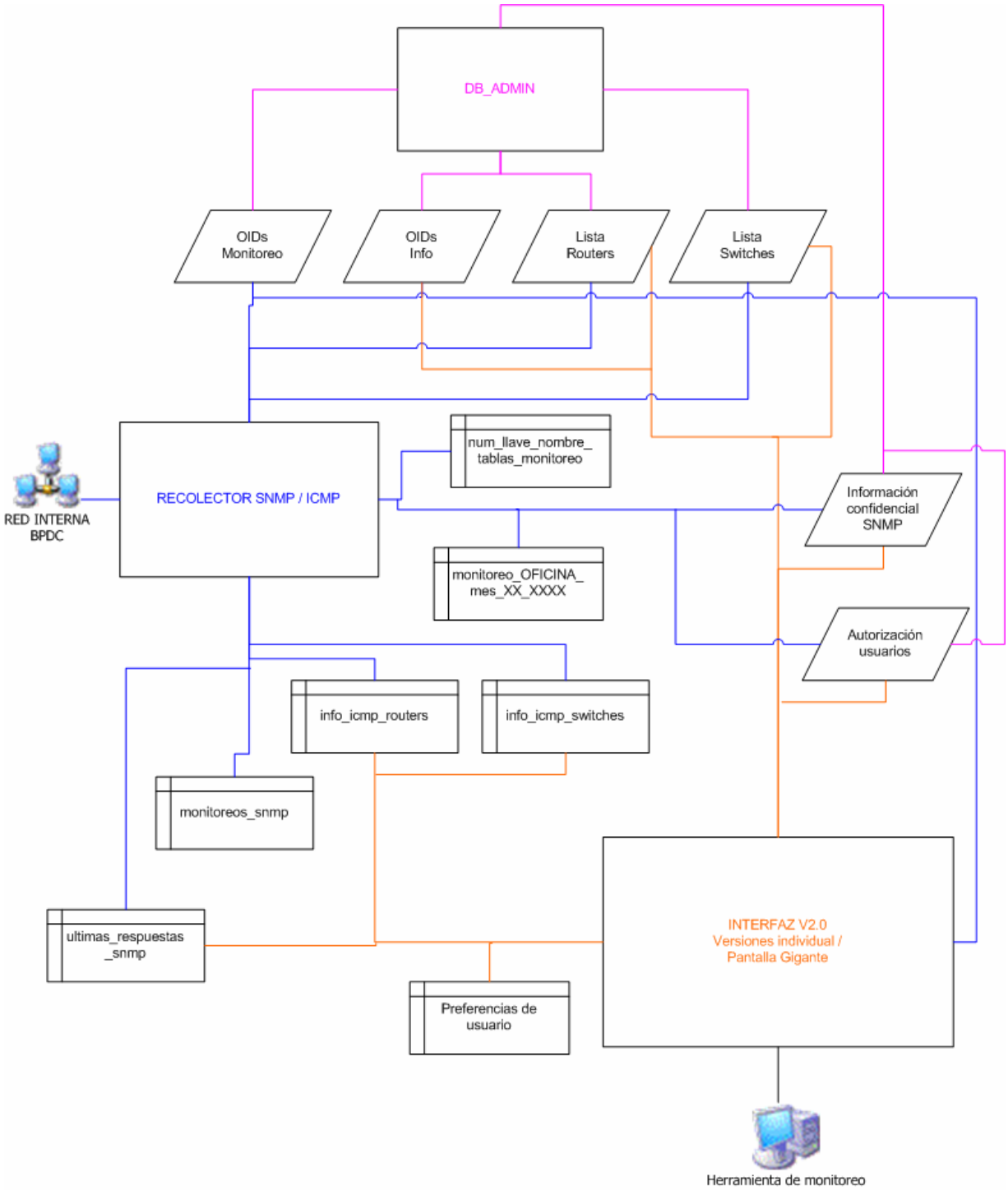


Figura 5. 2 Relación entre tablas de datos y aplicaciones que conforman la fase II de la herramienta de monitoreo de redes del BPDC

El algoritmo del programa parte de la existencia de 6 tablas maestras, donde se guarda toda la información necesaria para generar un monitoreo de la red del BPDC. Estas tablas se muestran con rombos en la figura 5.2.

- OIDs_monitoreo
- OIDs_info
- Lista_routers
- Lista_switches
- Contraseñas_SNMP
- Tablas de autorización de usuarios de MySQL. Estas tablas son parte del funcionamiento interno del servidor.

Ya se ha explicado la estructura de OIDs_monitoreo y OID_info en las tablas 5.1 y 5.2. La información contenida en las tablas lista_routers se muestra en la tabla 5.6, con la información de un equipo como ejemplo:

Tabla 5. 6 Información de un enrutador en Cañas; tabla lista_routers.

nombre_DNS	canas	**proveedor_enlace_1**	ICE	**numero_serie**	JMX0853L104
nombre_oficial	RA025P1_01	**dir_ip_enlace_2**	10.0.7.161	**codigo_barras**	48726
familia_cisco	c2600	**interfaz_2_SNMP**	4	**timeout_recoleccion_SNMP**	1000
region	Guanacaste	**timeout_max_normal_2**	200	**Codigo_consultas_activas**	S11011111100000
oficina	Sucursal Canas	**tecnologia_enlace_2**	RDSI	**Memoria_proceso**	221327648
piso	1	**numero_linea_enlace_2**	669-9010	**ancho_de_banda_enlace_1**	65536
dir_Lo0	10.56.127.6	**proveedor_enlace_2**	ICE	**ancho_de_banda_enlace_2**	65536
RAM_instalada_MB	128	**dir_ip_enlace_3**	10.0.7.161	**ancho_de_banda_enlace_3**	65536
FLASH_instalada_MB	48	**interfaz_3_SNMP**	5	**estado_interfaz1_SNMP**	
dir_ip_enlace_1	10.56.127.2	**timeout_max_normal_3**	200	**estado_interfaz2_SNMP**	
interfaz_1_SNMP	2	**tecnologia_enlace_3**	RDSI_doble	**estado_interfaz3_SNMP**	
timeout_max_normal_1	200	**numero_linea_enlace_3**	669-9010	**Tarjeta_EnvMon**	0
tecnologia_enlace_1	TDM	**proveedor_enlace_3**	ICE	**diagrama_visio**	\\\\ltin-fps02\\subproceso

					aor\\Diagramas de red\\Sucursales\\DG025P1-01.vsd
numero_linea_enlace_1	195-2883	**placa**	74923	**IOS_actual**	c2600-ik9s-mz.122-15.T14.bin

Esta información es confidencial y no se pretende incluir en el informe entregado a la biblioteca.

En total, para cada enrutador se ocupan 42 columnas de información. Es debido a la gran cantidad de información que se debe manejar por equipo que no se expone toda la tabla en este informe. Los datos más importantes a resaltar son:

- Información de Identificación del BPDC

  Esta categoría incluye: el nombre usado en el servidor DNS para acceder a dicho equipo, su nombre oficial dentro del Banco Popular, la región a la que pertenece, la oficina y el piso de la misma en que está ubicado el equipo, el número de serie, número de código de barras aplicado al equipo y el link al diagrama Visio del SAOR de esta oficina.

- Información de configuración de equipo

  Dirección IP de Loopback, IOS actual (sistema operativo de equipos Cisco), memoria RAM y Flash instalada, la memoria disponible para procesos (usada en el cálculo del porcentaje de uso de RAM del equipo), familia Cisco del equipo y tiempo de espera agotado típico para una consulta SNMP.

- Información de las líneas WAN

  Para cada enlace WAN, se sabe su dirección IP remota, número SNMP de dicha interfaz, timeout_max_normal (ICMP), tecnología del enlace, número de línea y proveedor. Se almacena el ancho de banda alquilado para poder presentar los gráficos de forma porcentual, y la columna estado_interfaz_SNMP es una salvedad que se debe hacer cuando hay sub-interfaces en enlaces canalizados o de frame relay, pues no toda la información del enlace queda en un sólo número SNMP.

- Información especial

  La existencia o no de la tarjeta EnvMon en este enlace y el código de configuración del equipo.

Esta información se define en DB_admin; se crean las tablas de recolección en el bloque Recolector SNMP/ICMP, y finalmente se despliegan en la interfaz v2.0. A continuación se explica en detalle cada bloque.

En términos de programas entregados, se crearon tres aplicaciones:

- DB_Admin
- Recolector SNMP/ICMP
- Interfaz v2.0, versiones para pantalla gigante y usuario del SAOR

5.2.1 DB_Admin

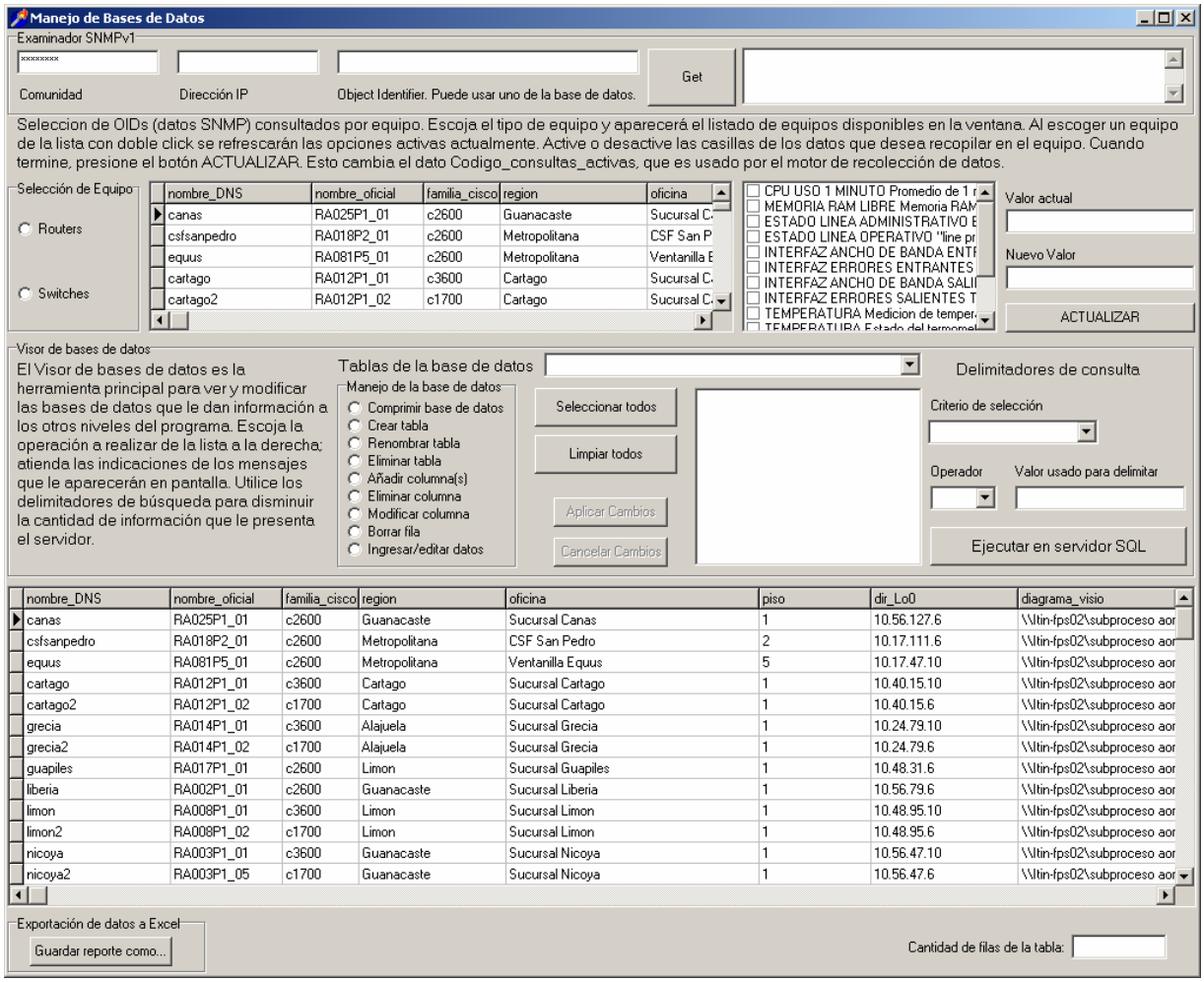


Figura 5. 3 Captura de pantalla de inicio de DB_Admin

La interfaz de la aplicación DB_admin se presenta en la figura 5.3. Sus funciones son:

- Dar al administrador de la herramienta un cliente SNMP básico para consultas aisladas.
- Permitir al administrador ejecutar y visualizar cambios en la base de datos.
- Ser el editor del hilo de configuración que permite especificar el monitoreo individual de cada equipo.
- Proveer una herramienta de creación de reportes desde CSV

En esta aplicación se crean y actualizan las tablas más importantes de la aplicación: oids_monitoreo, oids_info, lista_routers, lista_switches. También en esta aplicación se define para cada equipo cuáles OIDs de monitoreo se van a recoger por medio de un código de monitoreo incluido dentro de la información de cada equipo; es la forma de que el administrador configure el monitoreo específico a cada equipo. En esta aplicación se modifican todas las tablas maestras que generan la información necesaria para que el siguiente programa genere el monitoreo deseado.

Incluye un agente SNMP, un visor de los contenidos de todas las tablas disponibles y permite empezar el generador de archivos XLS desde CSV. Esta tabla usa el usuario MySQL de más alto rango, administrador, para poder editar los contenidos incluso de la tabla de contraseñas SNMP, que las otras aplicaciones sólo pueden leer.

DB_admin sólo debe existir en la computadora del administrador. Para asegurar esto, MySQL permite asegurar el acceso a la base de datos con un usuario, contraseña y además una dirección IP de origen. Sin embargo, para administrar las contraseñas del grupo y propias y tener permiso de borrar las tablas maestras, el administrador debe ir a la máquina que corre el servidor MySQL y usar la contraseña configurada. Esto imposibilita que un usuario que se apodere de la información del administrador provoque daños irrecuperables a la aplicación.

5.2.2 Recolector SNMP/ICMP

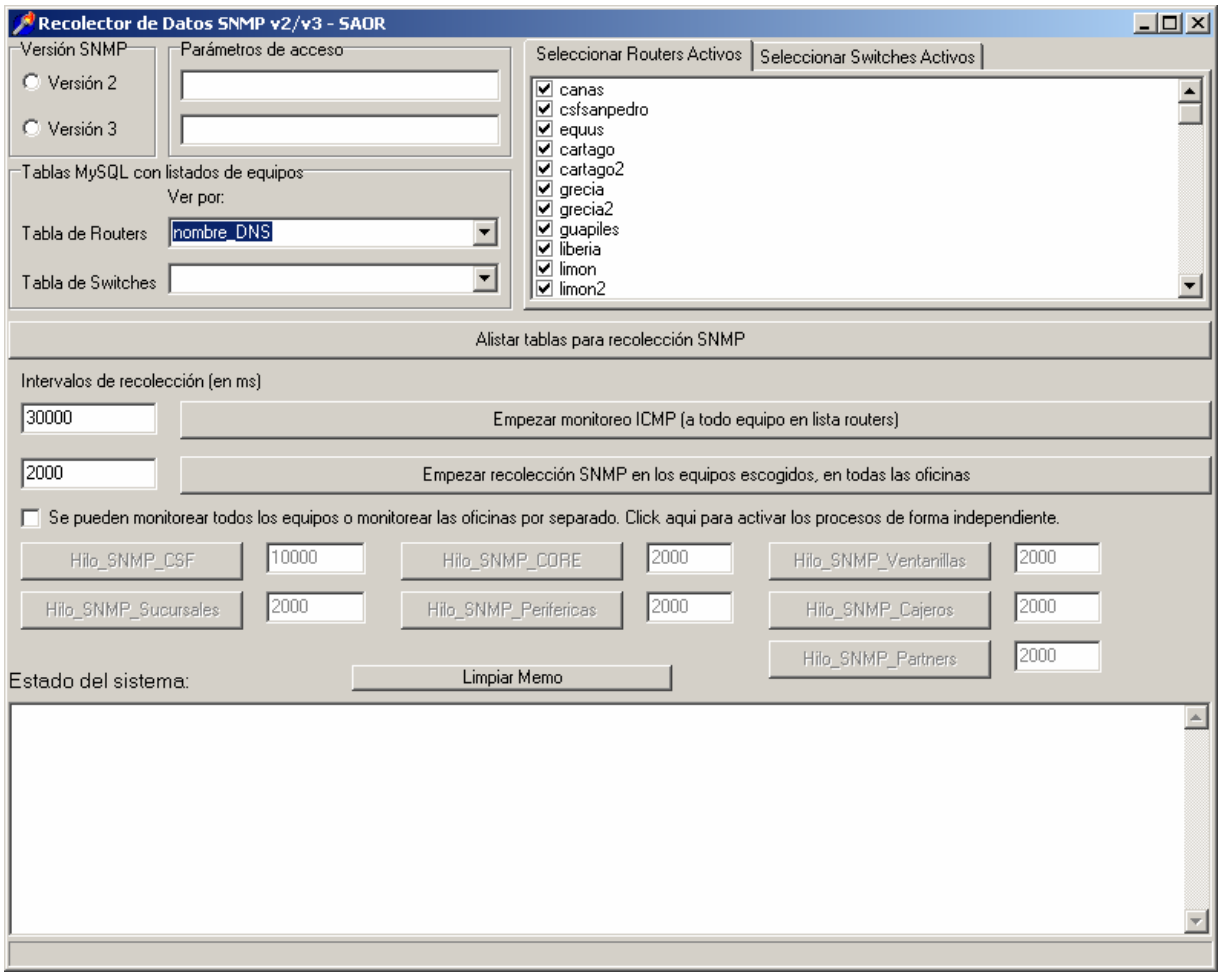


Figura 5. 4 Captura de pantalla de inicio de Recolector SNMP/ICMP

La figura 5.4 muestra la interfaz de la aplicación Recolector SNMP/ICMP. Sus funciones son:

- Crear las tablas necesarias para el funcionamiento de la aplicación.
- Controlar a nivel macro el monitoreo de cada equipo.
- Ejecutar el monitoreo ICMP / SNMP.
- Guardar los datos recolectados en las bases de datos respectivas.
- Presentar al administrador información que le permita saber el funcionamiento de la aplicación.

Cuando el administrador ha definido sus opciones de monitoreo, activa la aplicación que genera las tablas según la información encontrada en las tablas madre. Las tablas de almacenamiento no se regeneran excepto en cambios de mes; las tablas con la información de los monitoreos ICMP y SNMP activos se regeneran en cada reinicio de esta aplicación.

La aplicación permite asignar tiempos muertos entre ciclos de monitoreo SNMP e ICMP. Asimismo, permite asignar esos ciclos según prioridad de oficina.

La principal función de este programa es juntar la voluntad del administrador con el funcionamiento real de la herramienta, y permitirle confirmar que la recopilación de datos se está logrando por medio de una venta de estado.

Las tablas más importantes que se generan en esta aplicación son *info_icmp_routers* e *info_icmp_switches*, que ejecutan un monitoreo ICMP de manera independiente al monitoreo SNMP; si hay información SNMP, se usa para elaborar los informes de estado, pero si no se tiene información SNMP siempre hay un monitoreo ICMP activo que permite al administrador tener información de enlaces con tiempos de espera agotados y enlaces que responden dentro del tiempo de espera definido para ellos.

Es importante declara que para esta etapa el SAOR se contenta con tener sólo un monitoreo ICMP de las interfaces Loopback de los conmutadores, puesto que se principal labor es el monitoreo de enrutadores. Por ello, la aplicación sólo crea tres tablas más:

num_llave_nombre_tablas_monitoreo: esta tabla contiene la información de los nombres de tablas generados según el mes y los equipos a monitorear.
monitoreos_snmp_activos: almacena los OIDs ya armados con los números correctos de interfaz SNMP para cada equipo que será monitoreado.

ultimas_respuestas_snmp: contiene la última respuesta SNMP para cada equipo; se utiliza para que los datos que necesita la interfaz de usuario estén agrupados en un sólo lugar.

5.2.3 Interfaz v2.0 – Para pantalla gigante y para uso personal

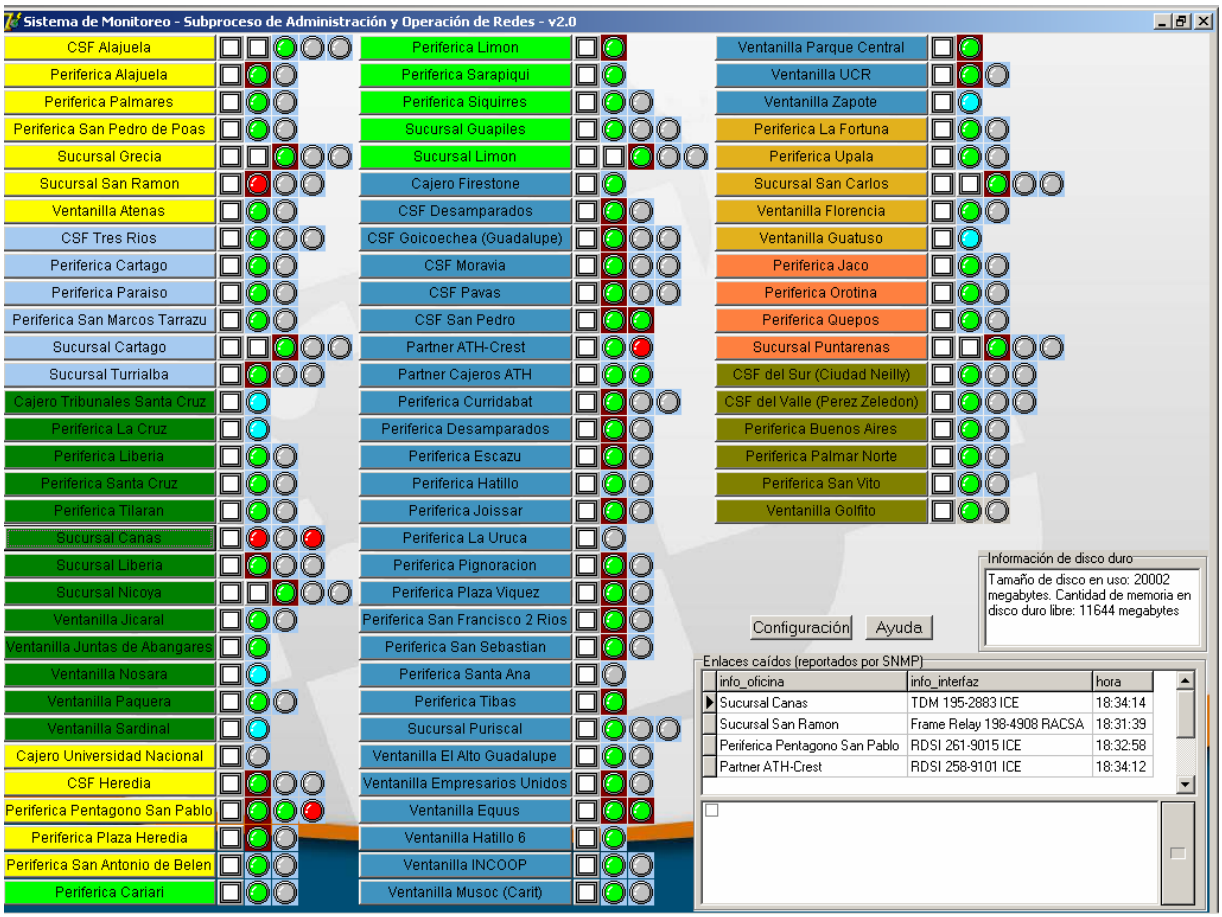


Figura 5. 5 Captura de pantalla de inicio de Interfaz v2.0 – Versión Pantalla Grande

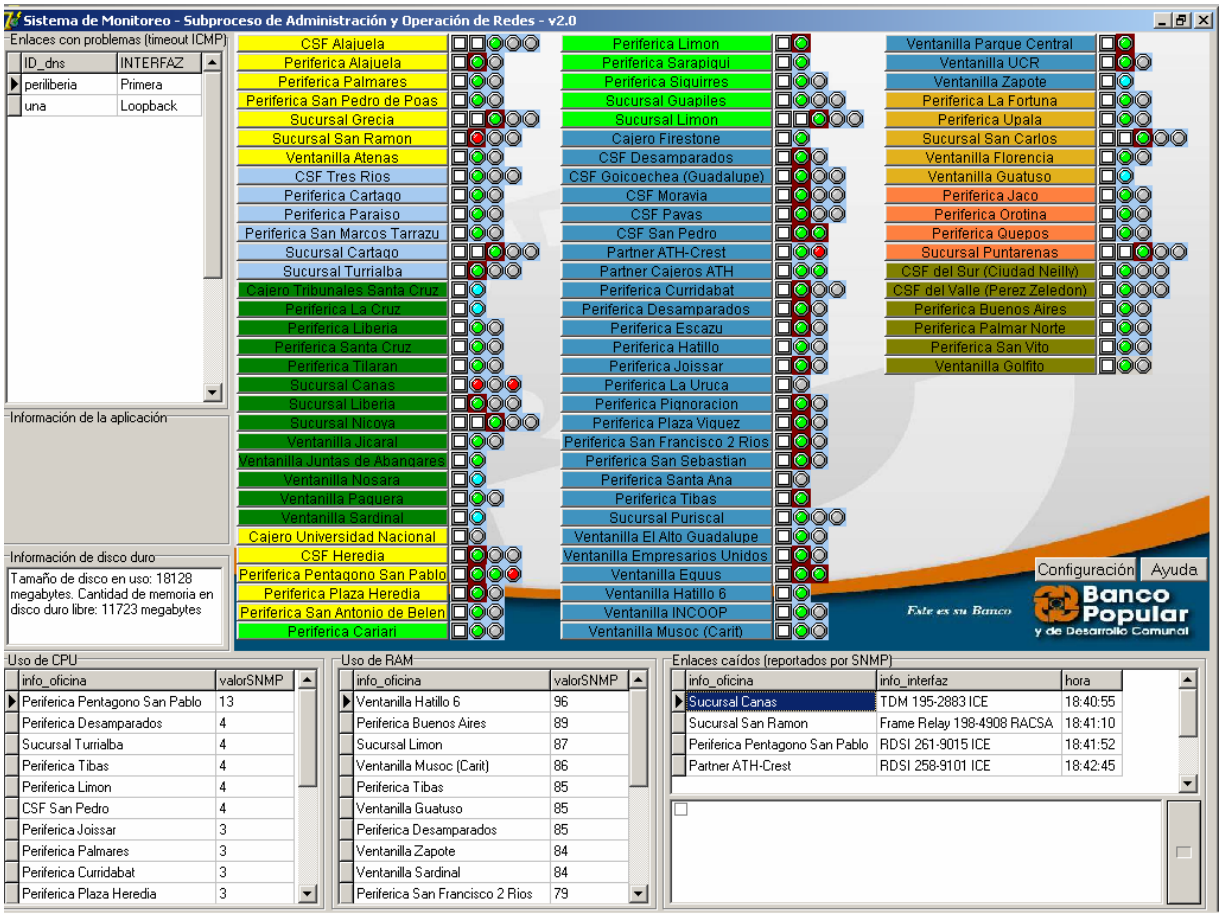


Figura 5. 6 Captura de pantalla de inicio de Interfaz v2.0 – versión usuario SAOR

Las dos versiones de Interfaz v2.0 se muestran en las figuras 5.5 (versión pantalla) y 5.6 (versión usuario de SAOR). Sus funciones son:

- Indicar gráficamente el estado de todas las oficinas del BPDC según lo recogido por Recolector SNMP/ICMP.
- Ser el punto de convergencia de la información disponible en las demás tablas y presentar dicha información con una interfaz intuitiva y útil.
- Servir de herramienta de diagnóstico de problemas y administración para el personal del SAOR.
- Integrar los recursos disponibles actualmente de SAOR para automatizar varios procesos.

La interfaz para pantalla gigante se diferencia de la pantalla para el usuario individual del SAOR en la cantidad de información presentada a primera vista. Son el mismo programa internamente, pero para mejorar la visibilidad a distancias lejanas a la pantalla, se han incrementado el tamaño de las luces indicadoras y sólo han permanecido: enlaces caídos reportados por SNMP, la bitácora de eventos, que es la que determina cuando suena una alarma audible y se manda un correo al grupo con los datos de dicho evento; el indicador de espacio en disco duro y las ventanas de configuración y Ayuda.

La pantalla para el usuario del SAOR incluye información de enlaces que están experimentando tiempos de espera agotados en ICMP, los equipos que están usando más CPU y RAM, más la información que se ve en la versión de pantalla grande. La aplicación puede ser configurada para que reporte valores de uso de CPU y RAM a partir de cierto porcentaje; si hay más de 10 datos disponibles, presenta los 10 más críticos. Asimismo, permite en sus dos versiones cambiar los colores de las luces indicadoras según varios escenarios de posibilidades de estado en los protocolos SNMP e ICMP.

Ambas pantallas presentan la información completa de una oficina al hacer clic en el botón con su nombre. Esto abre un cascarón, como se muestra en la figura 5.7, y permite al usuario seleccionar un equipo de la oficina para visualizar la información recopilada y encontrada en las tablas madre.

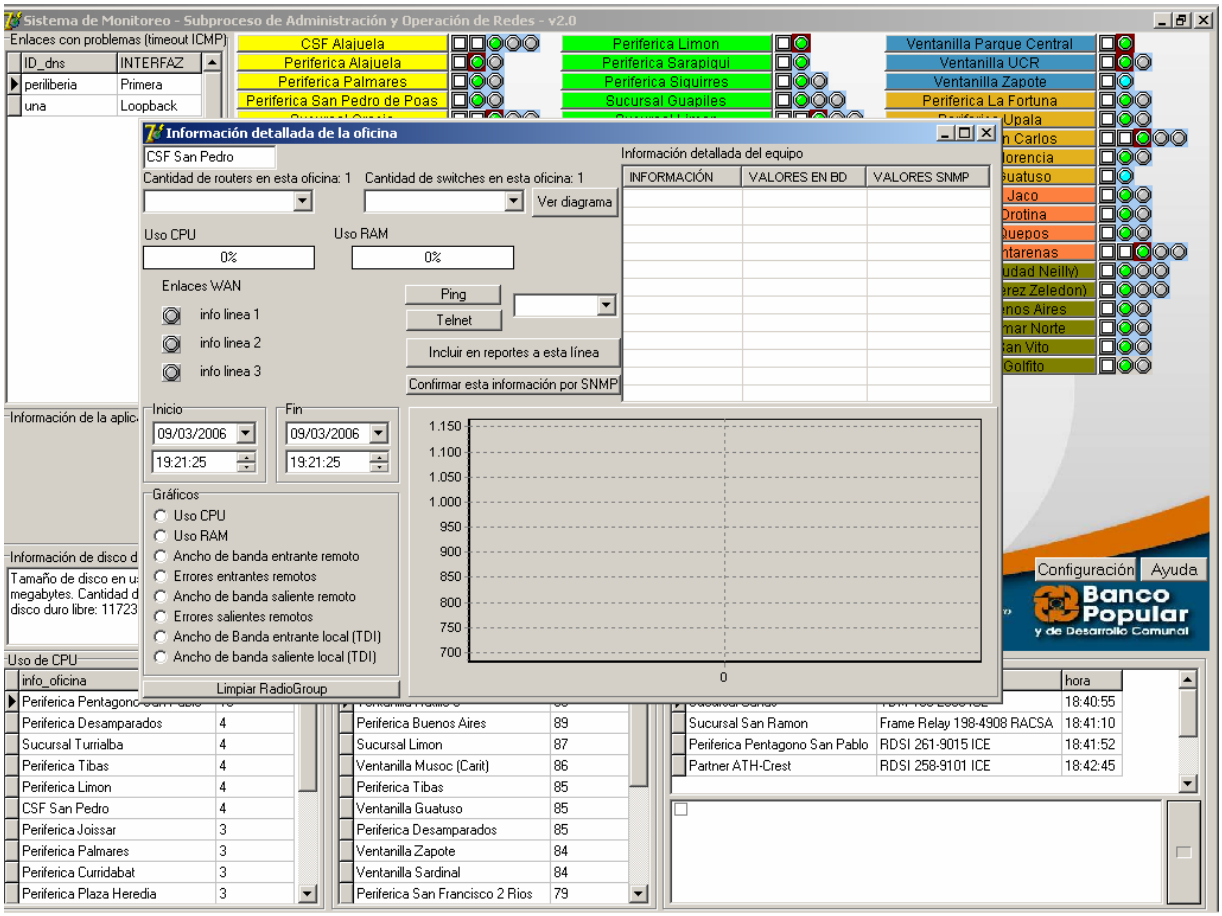


Figura 5. 7 Captura de pantalla de interfaz v2.0 al pulsar el botón de una oficina

Capítulo 6: Análisis de Resultados

En este capítulo se exponen los resultados concretos del proyecto y se analiza si cumplen los objetivos propuestos al inicio del mismo.

6.1 Resultados Experimentales

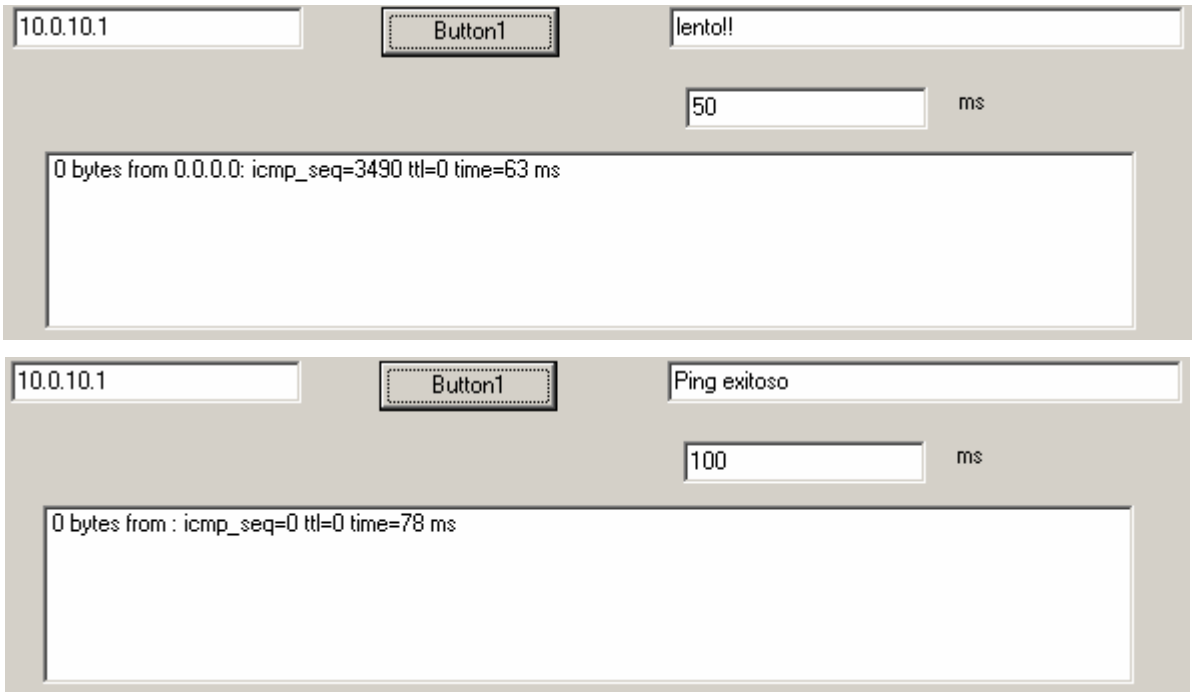


Figura 6. 1 Captura de pantalla de pruebas de tiempos de espera agotados en IdICMP

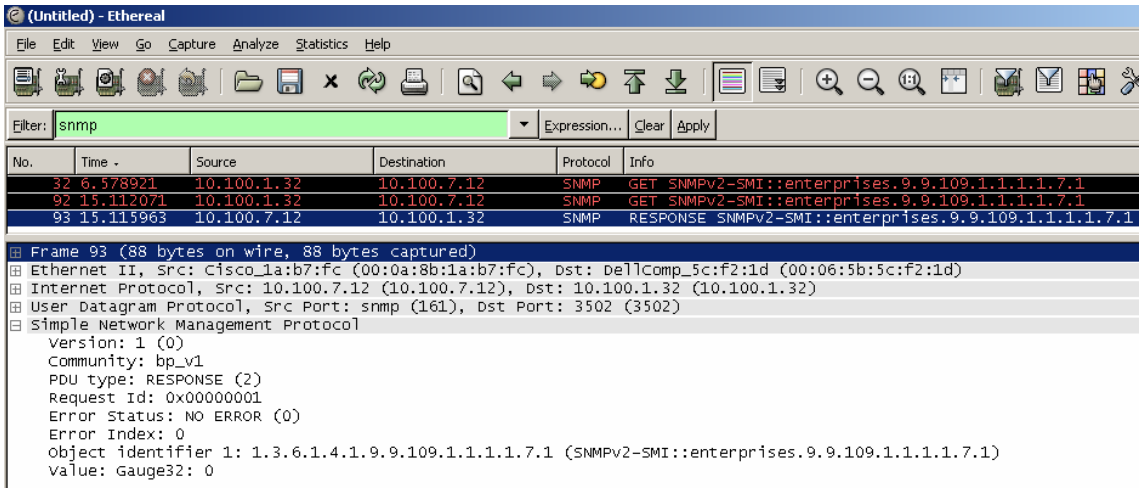


Figura 6. 2 Captura de pantalla que evidencia que la contraseña SNMPv1 (bp_v1) es interceptable

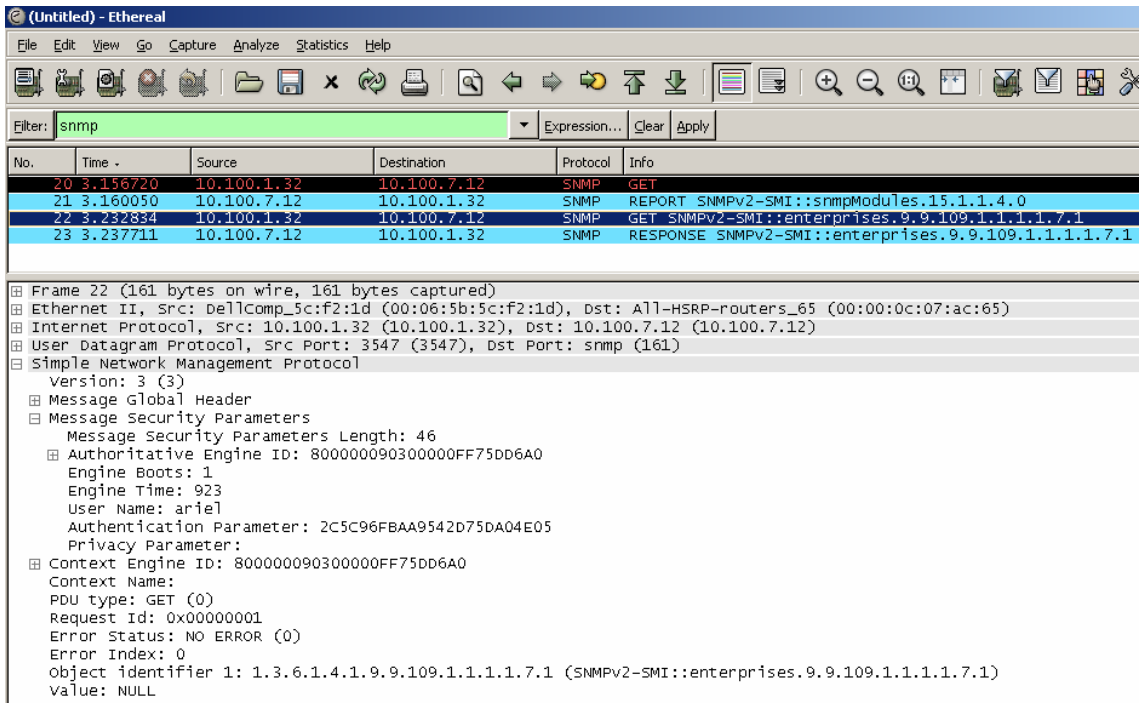


Figura 6. 3 Captura de pantalla que muestra datos hexadecimales donde debería ir la contraseña de un paquete SNMPv3

Figura 6. 4 Mapa vectorizado de Costa Rica para implementar en interfaz

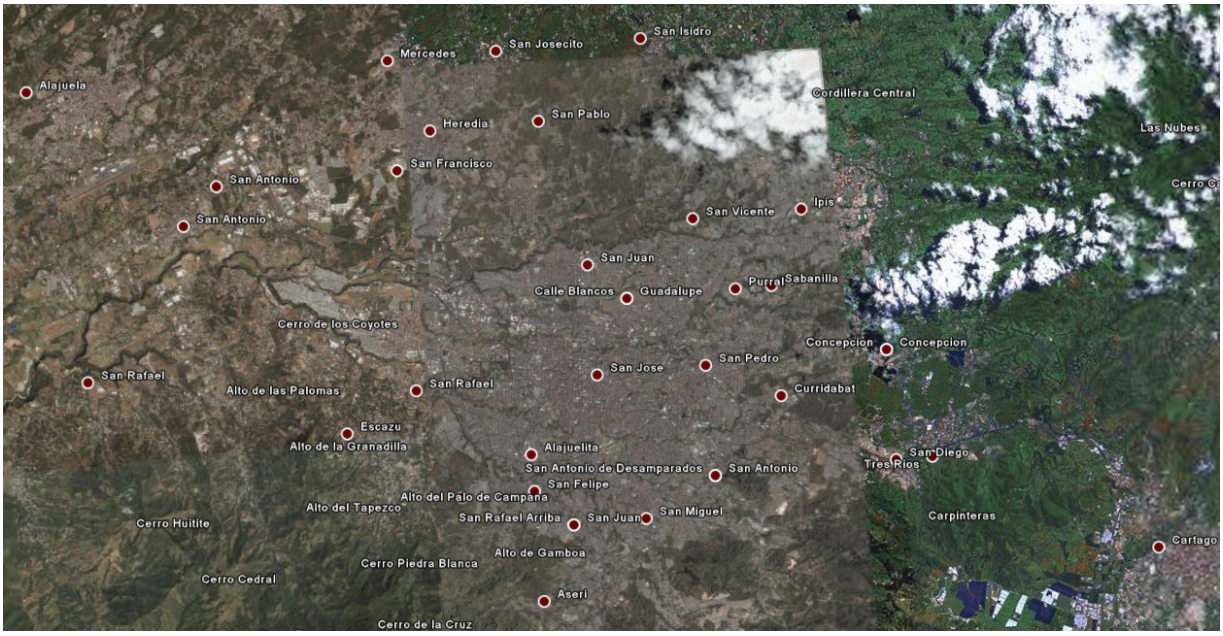


Figura 6. 5 Mapa aéreo de San José

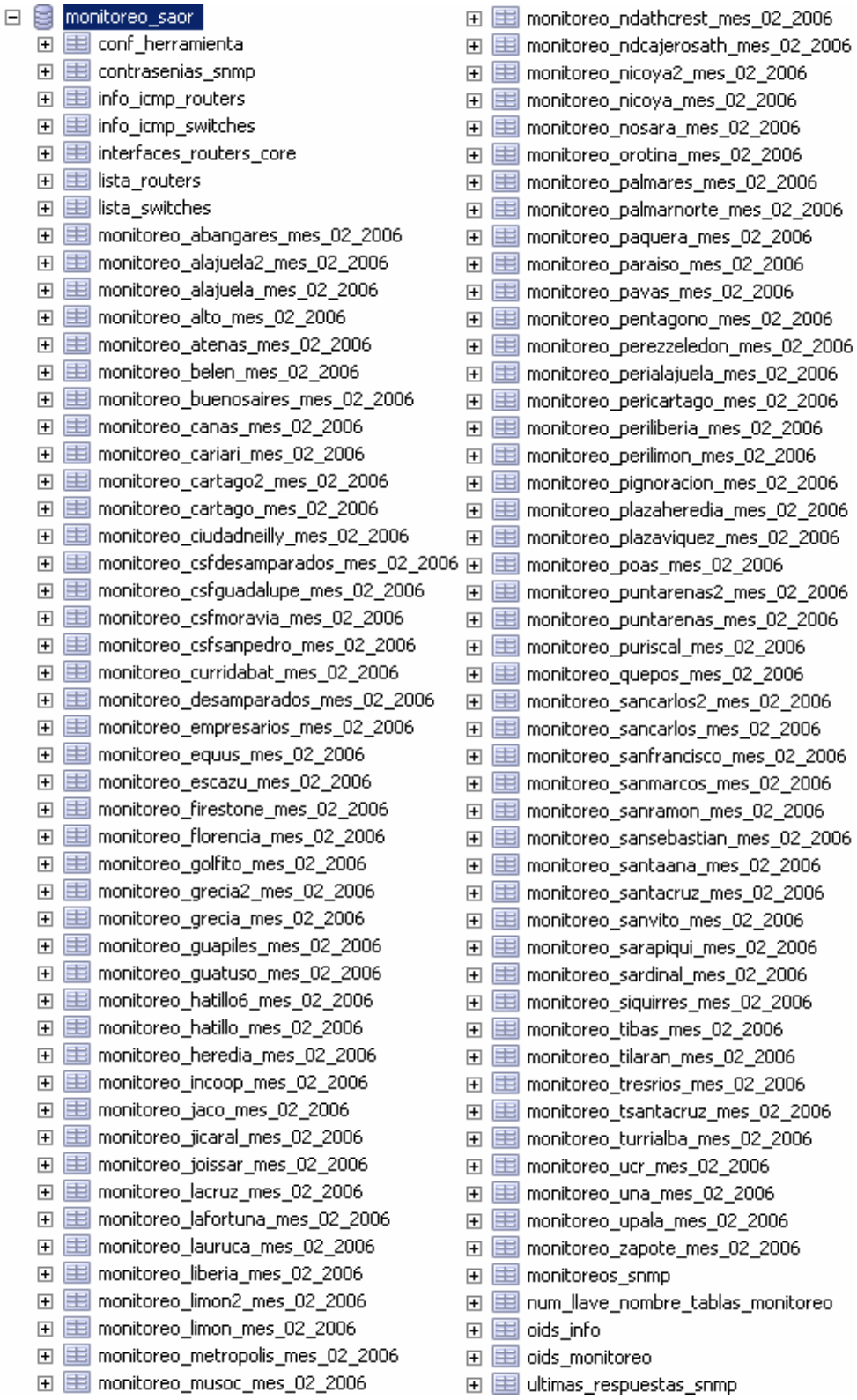


Figura 6. 6 Tablas creadas cuando la aplicación está ejecutando el monitoreo

Tabla 6. 1 Sentencias SQL reales generadas por Recolector SNMP / ICMP en su funcionamiento

Tipo de respuesta	Sentencia SQL generada por Recolector SNMP / ICMP
SNMP	insert into monitoreo_canas_mes_03_2006 (fecha,hora,USO_CPU_1min,RAM_LIBRE,ESTADO_PROTOCOLO_1,ESTADO_PROTOCOLO_2 ,ESTADO_PROTOCOLO_3,BW_ENTRADA_1,BW_ENTRADA_2,BW_ENTRADA_3,ERRORES_E NTRADA_1,ERRORES_ENTRADA_2,ERRORES_ENTRADA_3,BW_SALIDA_1,BW_SALIDA_2,B W_SALIDA_3,ERRORES_SALIDA_1,ERRORES_SALIDA_2,ERRORES_SALIDA_3) values (null,CURRENT_TIME(),"2","10","2","5","1","0","0","2000","1391","0","0","0","0","0","0","0","0"); Guardado en su tabla a las 18:40:56
ICMP	UPDATE INFO_ICMP_ROUTERS SET DELAY_ACTUAL="31", TIPO_RESPUESTA="Ping exitoso" WHERE ID_dns ="canas" AND INTERFAZ="Loopback";

Tabla 6. 2 Tiempos de operación de Recolector SNMP / ICMP

PRUEBA	TIEMPO INICIO	TIEMPO FINAL	DIFERENCIA
creación de tablas iniciales	12:15:56	12:16:11	00:00:15
un recorrido SNMP general, con ciertos errores	12:07:52	12:10:04	00:02:12
un recorrido ICMP	12:16:53	12:17:00	00:00:07
un recorrido SNMP_CSF	12:17:37	12:17:45	00:00:08
un recorrido SNMP Sucursales	12:18:08	12:18:23	00:00:15
un recorrido SNMP Perifericas	12:18:47	12:20:32	00:01:45
un recorrido SNMP Ventanillas	12:21:01	12:21:23	00:00:22
un recorrido SNMP Cajeros	12:21:46	12:22:01	00:00:15

Tabla 6. 3 Permisos para usuarios finales de Interfaz v2.0

Usuario	Tablas afuera de monitoreo_saor	Tablas de monitoreo_saor	Permitido lectura	Permitido Escritura	Permitido Iniciar y Apagar servidor
root (administrador local)	todas	todas	SI	SI	SI
administrador_SAOR (remoto)	no	todas	SI	SI	NO
SAOR_user	no	todas	SI	NO	NO

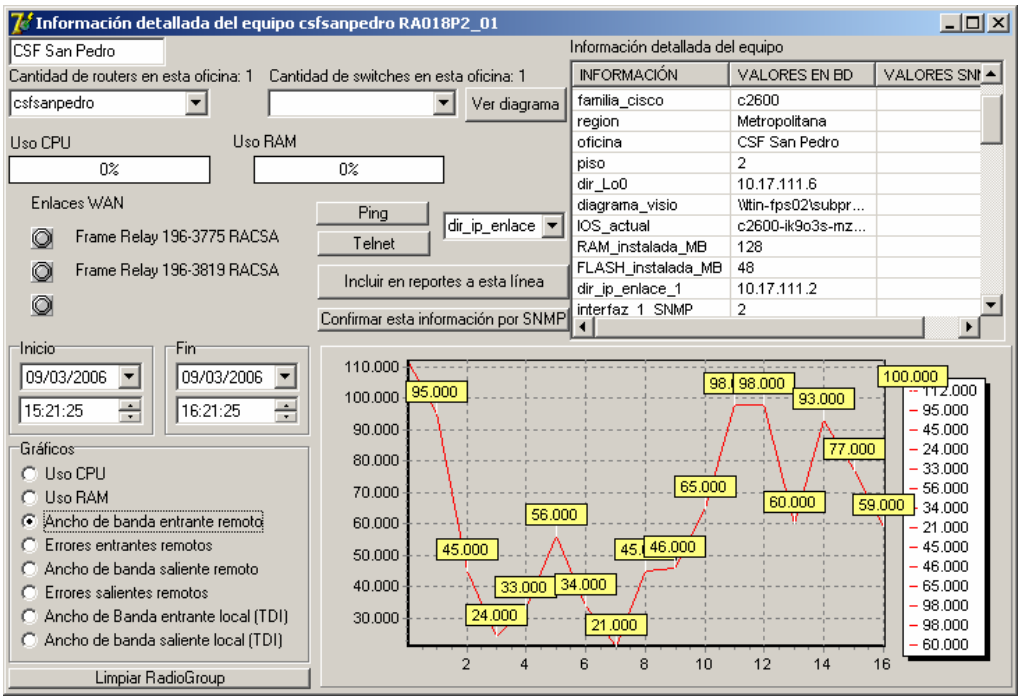


Figura 6. 7 Gráfico de Ancho de Banda entrante en una interfaz serial del CSF San Pedro

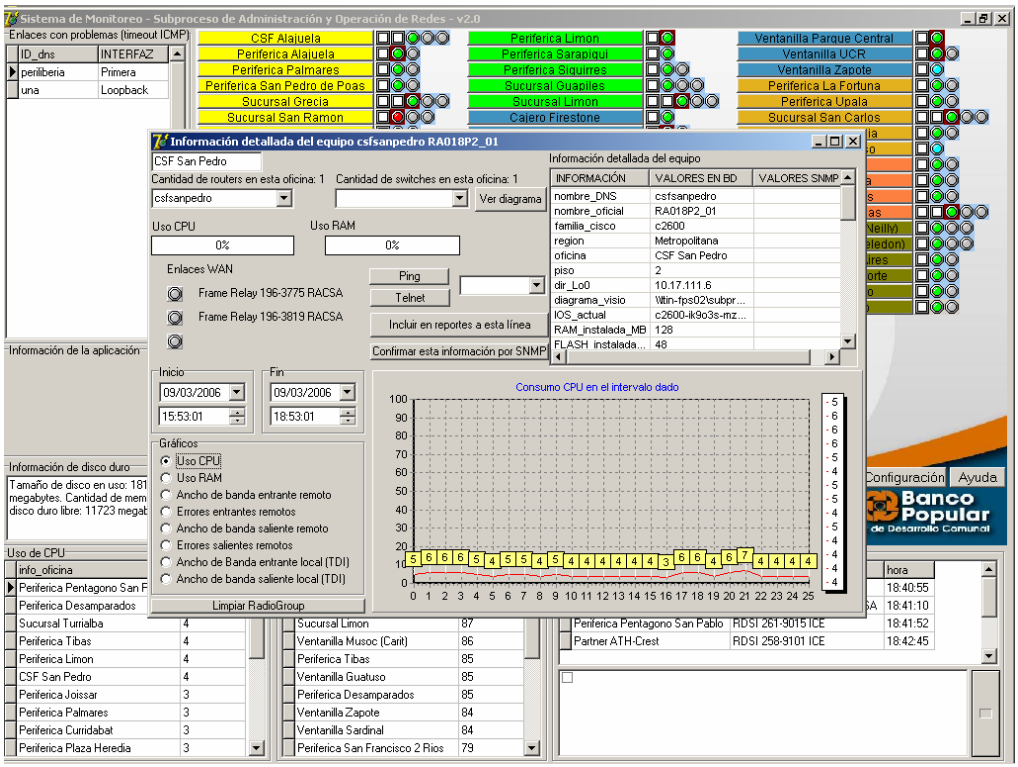


Figura 6. 8 Herramienta de monitoreo v2.0 en uso; en primer plano, un gráfico de consumo CPU

Figura 6. 9 Captura de pantalla de Email recibido desde la herramienta

6.2 Análisis de Resultados

Primero se hicieron pruebas de desempeño de los componentes utilizados en la primera fase, con ánimo de buscar mejores formas de implementación. Revisando el código fuente se comprendió la arquitectura interna de la herramienta de monitoreo y se procedió a elaborar ejemplos que usaran los mismos principios y a explorar las capacidades de las bibliotecas IdSNMP e IdICMP, ésta última es la que facilita la generación de *echo requests* desde Delphi. Se muestra un ejemplo de experimentos con IdICMP para determinar programáticamente cómo determinar un tiempo de espera agotado en un *echo request* en la figura 6.1. En el se verifica que un *echo reply* recibido en más de 50 ms puede ser correctamente identificado como un error de tiempo de espera agotado, pero ampliando dicho tiempo de espera a 100 ms en el mismo experimento, no hay tal error.

Para las pruebas de seguridad en SNMP, se muestran en las figuras 6.2 y 6.3 capturas en Ethereal mostrando una vulnerabilidad en la comunidad (contraseña) en SNMPv1 y un hash de la contraseña en SNMPv3. En la figura 6.2 se puede ver claramente con este sniffer que la comunidad SNMPv1, bp_v1, se observa como parte del paquete. En la figura 6.3 se comprueba que es visible el nombre de usuario (ariel) pero la contraseña está representada por números hexadecimales.

Una de las primeras sugerencias para la nueva interfaz fue colocar las oficinas en un mapa de Costa Rica; en la figura 6.4 se observa un mapa elaborado para tal fin. La intención era ampliar la zona metropolitana, que tiene una gran densidad de oficinas del BPDC, al cuadro azul oscuro. Sin embargo, como se puede ver en la figura 6.5, la zona metropolitana no es un área cómoda para dicha operación. A ello se suma que el BPDC tiene 5 oficinas sólo en San José centro y alrededores. Este diseño se desechó pues aunque se pudiera lograr una distribución aproximada de las oficinas del BPDC, sería menos clara y fácil de usar que un listado con rótulos legibles y grandes luces indicadoras.

En la figura 6.6 se pueden observar las tablas que se crean dinámicamente además de las tablas madres de la base de datos de monitoreo_saor. Los nombres de las tablas de almacenamiento son generados automáticamente por Recopilador SNMP / ICMP.

En la tabla 6.1 se muestra la aplicación Recolector SNMP/ICMP cuando ya ha recogido datos y se dispone a guardarlos en la base de datos respectiva, para SNMP e ICMP. Se puede notar que la cantidad de datos que recolectar y guardar para cada protocolo son diferentes: mientras que hay un solo *echo request* por interfaz activa, hay 6 consultas para cada interfaz SNMP. Esta diferencia afecta los tiempos de recopilación de cada proceso, lo que se refleja en la tabla 6.2. En este ejemplo, se monitorearon todas las variables posibles en SNMP e ICMP. En SNMP, se necesitaron hacer 1513 consultas; por ICMP, 168, para cubrir un total de 89 oficinas, cajeros y conexiones a socios financieros.

La ventaja de usar hilos es que se pueden monitorear simultáneamente diferentes tipos de oficinas. Como se puede ver el cuello de botella es el monitoreo de oficinas periféricas; esto se debe a que MySQL debe ordenar los datos en memoria antes de insertar el primer dato. En este caso, se podrían hacer tablas separadas para cada tipo de oficina, en vez de una sola tabla con todos las consultas SNMP que deba ser reordenada para hacer consultas diferenciadas.

Problemas de optimización de velocidad como este contribuyeron a entender las diferencias que hay que tomar en cuenta en diferentes opciones de conexión y al cuidado que hay que prestar al diseño de una base de datos que usa varias tablas. Aunque existe una serie de reglas para el correcto diseño de una base de datos, no son todas aplicables a SQL, por lo que se implementaron aquellas recomendadas para mejorar la eficiencia de las operaciones. En general, las operaciones de escritura que deben discriminar entre varias variables son las que más tiempo consumen, mientras que lecturas sucesivas se hacen con mucha rapidez

La solución sugerida para este problema por expertos fue utilizar índices; en efecto, las pruebas desde el cliente nativo de MySQL usando índices en las columnas más importantes y usadas permitió mejorías de hasta el 450%. Sin embargo, el conector utilizado entre Delphi y mySQL (dbExpress) no soportaba índices. Se recurrió entonces a mejorar la forma en que se insertaban y actualizaban datos para bajar el tiempo inicial de 2:10 al valor actual de 1:45.

En la tabla 6.3 se puede notar la distribución de permisos que se implementó para las aplicaciones; como todas necesitan recoger información desde la base de datos, deben tener acceso de lectura. Sin embargo, sólo DB_Admin y Recolector SNMP/ICMP tienen necesidad de escribir en la base de datos; Interfaz v2.0 está lógicamente separada y no es más que un medio de despliegue.

En la figura 6.7 se muestra un gráfico del ancho de banda para un periodo de una hora en la sección de información de oficina de la aplicación Interfaz v2.0, en sus dos presentaciones. Gracias a que todos los datos están disponibles en la base de datos, se pudo lograr una gran flexibilidad en la aplicación con relativamente poca complejidad pero gran eficiencia y satisfacción al usuario final. La figura 6.8 es una captura de toda la pantalla mientras la aplicación está en uso.

Aparte de las posibilidades de la aplicación en si, se le solicitó al SAOR configurar prioridad al tráfico SNMP y reservar un 5% del ancho de banda disponible, pues los paquetes SNMP son UDP y ligeros en cuanto a ancho de banda consumido. Con esto se desea que la aplicación siempre tenga datos precisos del estado de la red y no sufra de incertidumbres por tiempos de espera agotados, lo que si puede pasar a nivel de ICMP sin engañar a la herramienta.

La aplicación implementó dos tipos de alarmas cuando hay un enlace caído, sonora y por email. En la figura 6.9 se muestra una captura de un correo recibido tras una

falla. Esto permite a los encargados del SAOR darse cuenta de una falla aunque no hayan estado presentes en el momento del evento. El Subproceso tiene un correo grupal, que es el usado en la práctica para enviar el aviso.

Capítulo 7: Conclusiones y Recomendaciones

1. Se implementó satisfactoriamente un motor de base de datos de mayor capacidad para la segunda fase.

2. La implementación del motor de base de datos se puede mejorar cambiando la interfaz entre Delphi y MySQL para que permita el uso de índices.

3. Se desarrolló una aplicación que permite usar una gran cantidad de objetos administrables definidos en SNMP sin cambios en el código fuente de dicha aplicación.

4. Se mejoró la seguridad de la herramienta al actualizar la versión de SNMP a la más vigente, versión tres. Para ello, se cambió el conector empacado con Delphi por uno de desarrollo libre llamado Ararat Synapse.

5. El uso de una base de datos permite generar informes cronológicos al usuario final.

6. La interfaz de la herramienta se ha diseñado e implementado de una forma que permite al usuario final encontrar toda la información que puede necesitar en un solo lugar y por medio de ayudas gráficas intuitivas.

7. La herramienta de monitoreo permite al administrador configurar con gran detalle el monitoreo que desea implementar.

8. Se han entregado versiones optimizadas para adaptarse a un monitor grande y a un usuario final.

9. Se han incluido opciones que permiten a la herramienta ser un despliegue de información y un facilitador de las tareas de configuración del personal del SAOR.

10. Se han incorporado los conmutadores en el monitoreo ICMP.

A manera de resumen, se adjuntan las características finales de la segunda fase de la herramienta de monitoreo. Se logró implementar en la nueva fase:

- Monitoreo basado principalmente en SNMP.
- Reservación de un porcentaje de ancho de banda en el QoS desde diseño para asegurar la confiabilidad de la herramienta.
- Permitir al administrador definir el intervalo de monitoreo para cada tipo de oficina según prioridad de negocio.
- Generación de *echo requests* con tiempos de espera especificados individualmente (más eficiente).
- Exactitud en un solo ciclo para saber si un enlace está caído.
- Mostrar una ventana con la información importante de cada enlace caído, alarma audible configurable además de la visible y email al grupo con la información del evento.
- Colores diferentes para un enlace caído, tiempos de espera agotado icmp, según tecnología y proveedor, definibles por el usuario.
- A pesar de que el monitoreo principal es en SNMP, siempre hay disponible Información directa de la capacidad de comunicación de una oficina por monitoreo con ICMP a todas sus interfaces.
- Monitoreo de ancho de banda entrante y saliente, errores en interfaz, uso CPU y uso RAM, con opción de añadir cuantas más variables de tipo dinámico se desee.
- Opción de SNMPv1 o SNMPv3 por oficina.

- Opción de tarjeta EnvMon.
- Comprobación de datos estáticos en las tablas madre de los equipos por SNMP.
- Graficado histórico por mes de todas las variables monitoreadas.
- Exportación de tablas enteras a formato CSV.
- Mantenimiento mensual y automático con aviso de capacidad de la base de datos.
- Independencia de cantidad de datos mientras se respeten ciertos parámetros.
- Interfaz gráfica independiente del módulo recolector, lo que lo hace adaptable a nuevas soluciones o usos.
- Ordenamiento de oficinas automático por provincia, diferenciada por colores elegibles por el usuario.
- Botones de ayuda dentro de la aplicación.
- Monitoreo de Loopbacks de conmutadores.
- Acceso desde la aplicación a documentos del Subproceso.
- Configuración de niveles de acceso por usuario por tabla por MySQL.
- Tablas de configuración locales por usuario.
- Dos interfaces visuales disponibles según uso que se le prefiera dar a la herramienta: alarma o herramienta de trabajo.

Recomendaciones:

1. A pesar de que se ha dicho que los equipos normalmente no tienen más de 3 interfaces, hay muchos equipos que sólo tienen una o dos. Esto significa que la tabla de almacenamiento termina, por lo general, con algunas columnas vacías, que a pesar de tomar el menor espacio posible, ayudan a hacer más ineficiente la aplicación. Si a la hora de crear las tablas de almacenamiento se considera cuántas interfaces tiene cada equipo, se puede reducir este desperdicio (recomendación de re-diseño), pero esto cambia la estructura que

se usa después para presentar la información. La solución más eficiente sería elaborar una tabla por interfaz con los OID disponibles, pues aunque un administrador puede decidir que en una interfaz no será monitoreado el ancho de banda, es menos desperdicio una sola columna vacía por OID que tres.

2. Es imperativo buscar un conector más eficiente entre Delphi y MySQL. Incluso es preferible usar uno de código abierto que dbExpress, por lo menos para Delphi 7.

3. A pesar de que el monitoreo SNMP de conmutadores no fue contemplado por parte del SAOR, no se debe descartar la posibilidad de incluirlo en una próxima versión. Un diseño orientado a interfaces puede fácilmente acoplarse a incluir los puertos de un conmutador.

4. Es muy aconsejable migrar de lenguaje de desarrollo para las partes del programa que no son de desarrollo de interfaz. La aplicación Recolector SNMP/ICMP puede sustituirse por un desarrollo en Java, por ejemplo, con el que hay disponibles librerías con más funciones tanto para SNMPv3 como para la comunicación con MySQL. Es recomendable incluso que la interfaz del usuario del SAOR sea via web, pues permitiría más flexibilidad y un alcance de verificación de datos geográfico mucho más amplio.

5. Por la capacidad de manejo de información de los motores de bases de datos y también debido a que cada vez la industria lo demanda con mayor intensidad, los estudiantes de ingeniera electrónica deberían usar motores de bases de datos en sus laboratorios en vez de soluciones que involucren Ms Excel o archivos de texto CSV.

Bibliografía

1. **Borland Software Corporation.** *Delphi Help: Developing Database Applications.* 2002.

2. **Cisco Systems, Inc.** *Cisco Networking Academy Program. Cisco Certified Network Associate 4: Wan Technologies v3.1*. 2003

3. *Cisco Management Information Base (MIB). User Quick Reference.* [en línea] <http://www.cisco.com/univercd/cc/td/doc/product/software/ios11/mbook/mtext.htm> [consulta en agosto del 2005].

4. SNMPv3 (Manual IOS12.0T(3)) Configuration Guide [en línea] < http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/snmp3.htm> [consulta en septiembre 2005}.

5. *Tools & Resources: SNMP Object Navigator*. [en línea] <http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1> [consulta en numerosas ocasiones entre agosto 2005 y febrero 2006].

6. **Chapman, Dave**. "Statistics Versus Dashboards". Packet: Cisco Systems Users Magazine v. 17 (3):15-17,julio-septiembre 2005.

7. **Doughty, Mike**. *Mike's Sketch Pad: Raster and vector graphics.* [en línea] 2005. <http://www.sketchpad.net/basics1.htm> [consulta en agosto del 2005].

8. **Gebauer, Lukas**. *Synapse – Synchronous TCP/IP library for Delphi* [en línea]*, 2005* <http://synapse.ararat.cz/> [consulta en septiembre 2005].

9. **Fujitsu Systems.** Network Monitoring: Fujitsu Thailand**.** [en línea] 2006. <http://www.fujitsu.com/th/th/services/solutions/monitoring/> [consulta en marzo 2005].

10. **Harvey, Martin** *Multithreading – The Delphi Way v1.1a* [en línea]. 2001. <http://www.pergolesi.demon.co.uk/prog/threads/ToC.html> [consultado en noviembre del 2005].

11. **Hower, Chad Z.** *Indy.Sockets*. [en línea] <http://www.indyproject.org/Sockets/ index.iwp> 2005. [consulta en agosto del 2005].

12. **Klein,** Jürgen. SNMP - Netzwerk-Management mit Hilfe von SNMP. [en línea] < http://www.jklein.de/techniker_arbeit/tech_html/teil2.htm> [consultado en agosto 2005].

13. **Quesada Fernández, Alfonso y Vargas Pereira, David.** *Desarrollo de herramienta para monitoreo de red del Banco Popular basada en el Protocolo Simple de Gestión de Red (SNMP).* Proyecto de graduación para optar por licenciatura en ingeniería electrónica. ITCR, Cartago. 2004.

14. **Melton, Jim.** *SQL: The Standard and the language.* [en línea] X/Open Company Limited, 1994. <http://www.opengroup.org/public/tech/datam/ sql.htm> [consulta en agosto del 2005].

15. **MySQL AB.** *MySQL 4.1 Reference Manual*. rev 1530 [en línea] < http://dev.mysql.com/doc/refman/4.1/en/index.html> [consulta en septiembre 2005].

16. **Simpleweb.org.** *The Simpleweb.* [en línea] 2003 < http://www.simpleweb.org/> [consulta en agosto del 2005].

Apéndices

A.1 Glosario

Ancho de banda: capacidad de transmisión de información de un canal o medio físico.

Conmutador (más conocido como switch): dispositivo de red que distribuye datos eficazmente a varios nodos.

CMIP (Common Management Information Protocol): protocolo creado para el monitoreo de redes, segundo en popularidad y aceptación.

CSV (Comma Separated Values file): formato que contiene datos separados con una coma, usado por muchos programas como la forma más simple de intercambiar datos de hojas de cálculo.

CPU (Central Processing Unit): unidad central de procesamiento de un microprocesador electrónico. En este contexto, porcentaje de recursos de procesamiento utilizados por un equipo.

Enrutador (más conocido como router): dispositivo de red que dirige el tráfico IP en una red de computadores.

GUI (Graphical User Interface): parte de un programa que interactúa con el usuario final por medio de una interfaz de orientación gráfica.

ICMP (Internet Control Message Protocol): Protocolo de mensajes de control de Internet. Es una extensión del Protocolo de Internet (IP). Permite generar mensajes de error, paquetes de prueba y mensajes

informativos relacionados con IP. Básicamente, se usa para comprobar la existencia de la máquina consultada.

Intranet: red interna, de uso privado, de una institución.

LAN (Local Area Network): red de área local que cubre un área física y lógica común.

OID (Object Identifier Description): número en formato decimal que identifica una característica de un equipo monitoreada a través del protocolo SNMP.

RAM (Random Access Memory): memoria usada en el funcionamiento de un computador. En este contexto, porcentaje de recursos de memoria utilizados por un equipo.

SNMP (Simple Network Management Protocol): protocolo estandarizado para el monitoreo de redes de computadoras.

SQL (Structured Query Language): lenguaje estandarizado para acceder a bases de datos remotas.

telnet: protocolo estándar de Internet que permite acceso remoto a la consola de otro sistema.

tiempos de espera agotado: condición entre equipos de comunicaciones donde se ha excedido el tiempo en el que se esperaba una respuesta determinada. Cuando esta condición se obtiene por ICMP al ejecutar un *echo request* indica problemas de comunicación.

UDP (User Datagram Protocol): protocolo no orientado a conexión utilizado por SNMP para intercambiar información.

uptime: tiempo en el que un equipo o enlace está activo y permite realizar las operaciones para las cuales está implementado. Un uptime del 100% es deseable pero poco posible. En la práctica 99.999% es la meta.

WAN (Wide Area Network): red que une dos puntos separados geográficamente a través de un enlace serial.

A.2 Información de la institución

A.2.1 Descripción de la empresa

El Banco Popular y de Desarrollo Comunal fue creado mediante la ley No. 5435, el 29 de noviembre de 1973, como un banco que es por su naturaleza propiedad de los trabajadores. Tiene un aproximado de 2500 empleados tomando en cuenta el edificio central en la avenida segunda y todas las oficinas del mismo en el territorio nacional, con oficinas distribuidas desde las principales poblaciones en la zona sur hasta el norte del país.

Cuenta con más de 100 oficinas clasificadas en las siguientes categorías en función de los tipos y cantidad de servicios que ofrecen: Centros de Servicios Financieros, Sucursales, Oficinas Periféricas, Ventanillas de servicio, Cajeros automáticos tipo isla y Socios del Negocio.

Este sistema se desarrolla por iniciativa del Coordinador del Subproceso de Administración y Operación de Redes, con el objetivo de contar con una herramienta de monitoreo hecha a la medida. La primera fase se efectuó en el año 2003, y la segunda fase está a cargo del impulsor inicial del proyecto y uno de los autores de la primera fase, que permaneció laborando en el Banco Popular.

A.2.2 Descripción del departamento en la que se realizó el proyecto

La coordinación del Subproceso está a cargo del Ingeniero Rodrigo Vargas, quien fue nombrado por el Macroproceso de Tecnología de Información en mayo del 2003, para atender los requerimientos de la red de telecomunicaciones del Banco Popular.

Esta dependencia está encargada del mantenimiento de la red del banco así como la administración de la configuración de los dispositivos correspondientes; también realiza el planeamiento y ejecución de proyectos que permitan la constante

actualización y mejora general de la red. Recibe apoyo de otras áreas directamente relacionadas:

- El Proceso de Infraestructura y Proyectos: Responsables del cableado de la red (Backbone, UTP, Fibra Óptica, etc.).
- Subproceso de Administración y Operación de Redes: dividida en dos partes, Taller, que es responsable por la instalación y reparación de equipos de cómputo, tales como PC's, servidores e impresoras, y Comunicaciones, que se encarga de dispositivos de red (Hubs, Swiches, Enrutadores, Módems, ISDN, etc)
- Oficina de Presupuesto: asignan los recursos económicos para la ejecución y desarrollo de nuevos proyectos.
- Oficina de Contratación Administrativa, encargada de hacer las gestiones para comprar los dispositivos y software necesarios para comunicar las diferentes oficinas del Banco Popular.

A.3 Ejemplos de configuración

A.3.1 Configuración del servidor SNMP en equipo cisco

Snmp v1

```
rweb#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rweb(config)#snmp-server com
rweb(config)#snmp-server community bp_v1 RO
rweb(config)#exit
rweb#show snmp
Chassis: JAE0815CYNL (1867014538)
0 SNMP packets input
   0 Bad SNMP version errors
   0 Unknown community name
   0 Illegal operation for community name supplied
   0 Encoding errors
   0 Number of requested variables
   0 Number of altered variables
   0 Get-request PDUs
   0 Get-next PDUs
   0 Set-request PDUs
0 SNMP packets output
   0 Too big errors (Maximum packet size 1500)
   0 No such name errors
   0 Bad values errors
   0 General errors
   0 Response PDUs
   0 Trap PDUs

SNMP logging: disabled
```

SNMP v3

```
rweb#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rweb(config)#snmp-server view vista_snmp_BP internet included
rweb(config)#snmp-server group grupo_BP v3 auth read vista_snmp_BP
rweb(config)#snmp-server user ariel grupo_BP v3 auth md5 proyectoBP

rweb#show snmp group
groupname: ILMI                       security model:v1
readview : *ilmi                      writeview: *ilmi
```

notifyview: <no notifyview specified>
row status: active

groupname: ILMI security model:v2c
readview : *ilmi writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: grupo_BP security model:v3 auth
readview : vista_snmp_BP writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active

A.3 Manuales de Usuario

A.3.1 Manual del usuario administrativo de la herramienta de monitoreo de redes IP del Subproceso de Administración y Operación de Redes, v2.0

Introducción

Para que la herramienta ejecute el monitoreo deseado, se deben seguir los pasos en el orden en que se explican.

Primer paso – MySQL

Instalación
El software del servidor MySQL se encuentra en la carpeta \Instaladores\MySQL del CD de instalación. Descomprima el archivo en una carpeta \mysql del disco duro que desea usar para la herramienta. Es recomendable que este disco tenga más de 8 GB libres de memoria.

Ubique el directorio \data entre los archivos comprimidos. Borre los archivos y subdirectorios encontrados. Desde la misma carpeta del CD de instalación, descomprima el archivo ***configuración_SAOR_2006.zip*** en este directorio. Esto obliga al servidor a usar la contraseña definida en la entrega del proyecto para el servidor MySQL.

Iniciar el servidor de MySQL

Ejecute el script ***mysql_server_saor.vbs*** que se encuentra en el CD de instalación bajo la carpeta \Instaladores\Scripts

Si en la ejecución sucede algún error, copie el archivo a su máquina en un lugar al que solamente usted como administrador tenga acceso. Con click derecho, escoja *Modificar*. Revise que los enlaces entre paréntesis contengan ubicaciones validas en su sistema de archivos.

El servidor le va a pedir una contraseña para iniciar; utilice la que se dio en la entrega del proyecto.

Para iniciar al servidor desde la línea de comando en vez de un script, ejecute el comando

mysqld --console --p

Desde el directorio bin creado en la descompresión del archivo del software del servidor.

Para re-definir una contraseña, ejecute el script ***contraseña_mysql_server.vbs*****.** Este script le pedirá una contraseña y la instalará en la base de datos.

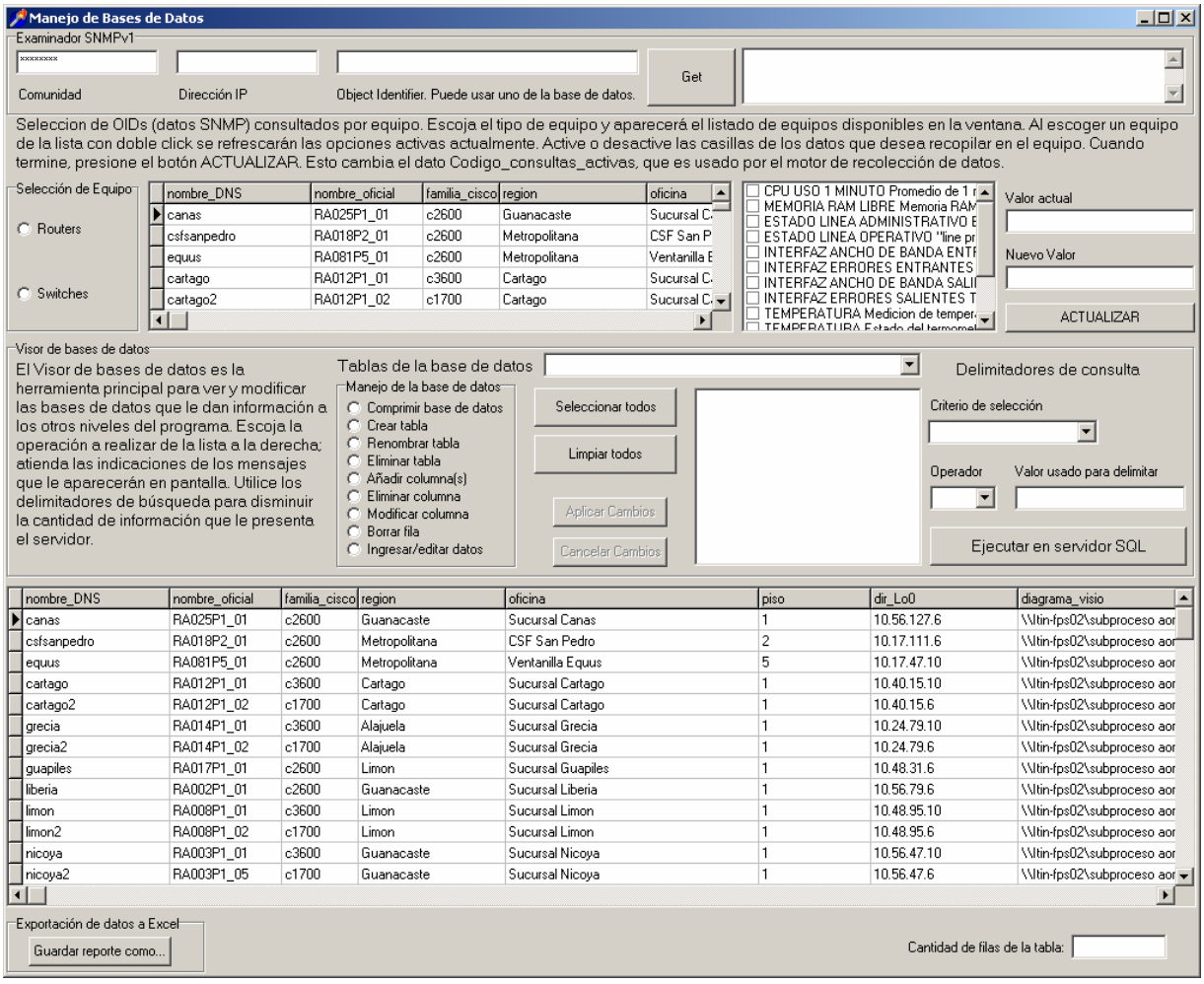
Revisar bases de datos y ejecutar operaciones de mantenimiento

El sistema necesita de las siguientes tablas principales para funcionar correctamente:

OIDs_monitoreo
OIDs_info
lista_routers
lista_switches
contraseñas_SNMP

No se les puede cambiar el nombre ni el orden de sus columnas, pero si se pueden añadir o borrar filas a cada tabla. Copie y ejecute la aplicación DB_admin.exe desde la carpeta \Herramienta de Monitoreo\.

En la sección *Visor de Base de Datos* se puede seleccionar una tabla desde el combobox con la leyenda Tablas de la base de datos. Compruebe la existencia de las tablas arriba mencionadas.



Captura de Pantalla de DB_admin

Verifique que las tablas contienen información actualizada antes de proceder con el monitoreo. Cuando se desee hacer un respaldo de estas tablas actualizadas,

simplemente debe apagarse el servidor como se explica al final de este manual y copiarse las carpetas con los nombres de las tablas principales a la ubicación de respaldo.

Utilice la sección *Selección de Equipo*, pulsando el botón de Routers o Switches, para configurar los OIDs que serán monitoreados para cada equipo, activando o desactivando la casilla que corresponde. Al terminar, pulse el botón ACTUALIZAR.

Con esto se completa la información necesaria para que la herramienta pueda empezar un monitoreo.

Iniciando el monitoreo SNMP/ICMP

Para iniciar el monitoreo SNMP/ICMP, ubique la aplicación Recolector SNMP-ICMP.exe en el directorio \Herramienta de Monitoreo\. Ejecute y seleccione los routers y switches; se desplegará una lista de todos los disponibles, junto con una casilla activada. Si UD desea dejar de monitorear un equipo sin sacarlo de la base de datos, desactive su casilla.

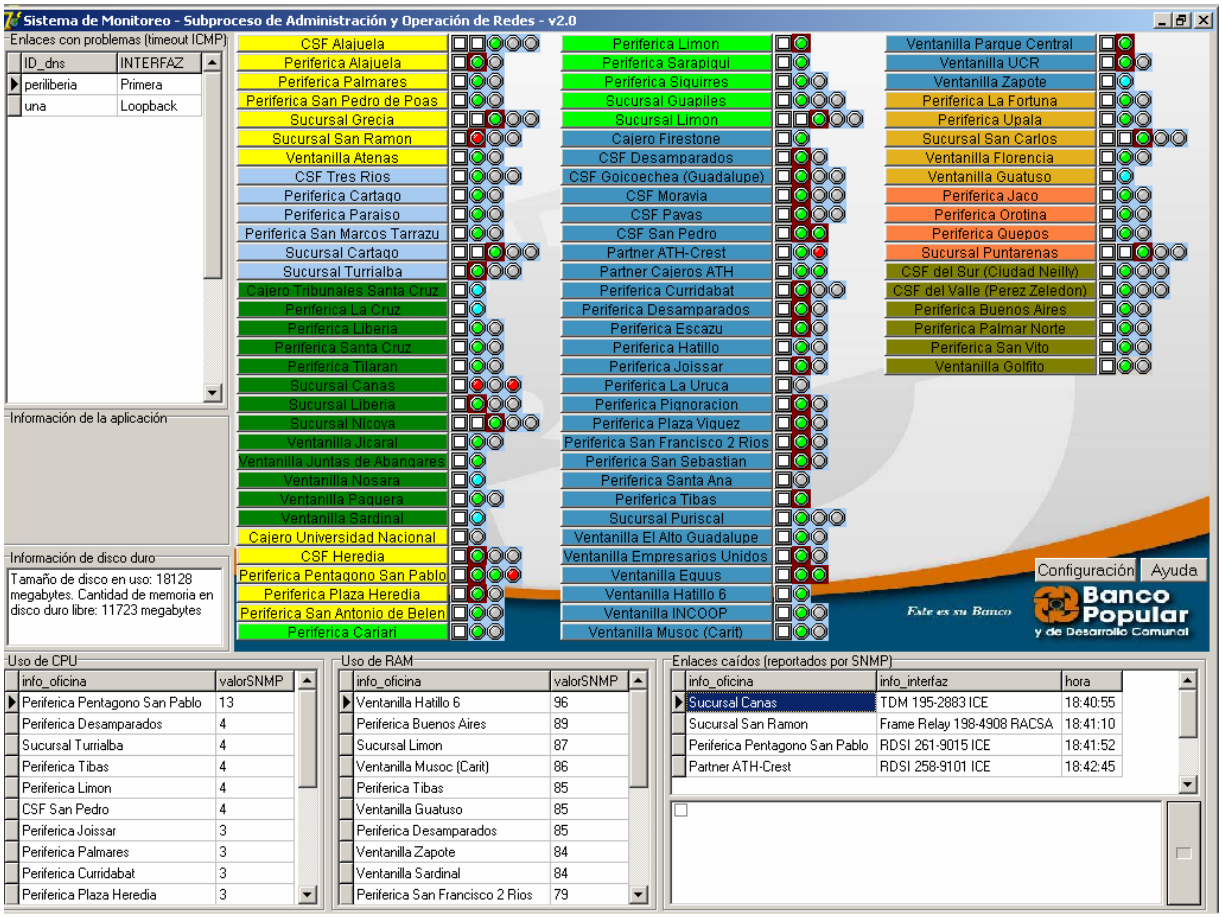
a continuación pulse el botón que dice “Alistar tablas para recolección SNMP”. El sistema le indicará cuando puede proseguir; la demora normalmente no es más de medio minuto.

Cuando se le indique, revise los tiempos de muestreo con que se monitoreará cada tipo de oficina y ajústelos a sus intereses; deben darse en milisegundos. Ejecute la opción de monitoreo automático y compruebe que se ha empezado un monitoreo por los mensajes desplegados en la ventanilla de estado.

Con esto se completa el inicio de la herramienta de monitoreo en la red. Para cambiar un parámetro, se debe detener esta aplicación, volver a DB_admin, ejecutar el cambio, y volver a alistar las tablas para el monitoreo.

A.3.2 Manual de usuario para la herramienta de monitoreo de redes IP del Subproceso de Administración y Operación de Redes, v2.0

1. Verifique que el administrador ha activado el servidor de datos de la herramienta.
2. Ubique la aplicación Interfaz v2.0 – usuario del CD de instalación en la carpeta \Herramienta de Monitoreo\
3. Ejecute la herramienta. Después de unos momentos, verá aparecer una pantalla como esta:



Los enlaces a los lados de los nombres de las oficinas representan la capacidad de comunicación de cada oficina: los colores vienen predeterminados como verde =

bueno y rojo = malo, con amarillo = tmeout ICMP. Esto se puede cambiar en el botón *configuración* encima del logo del Banco Popular a mano derecha.

4. Podrá notar que además de los nombres de las oficinas hay cuadros que se refrescan con información general sobre uso de CPU, RAM, enlaces con tiempos de espera agotados actualmente por medio de ICMP, y una ventana con información de enlaces con protocolo caído. Esta ventana tiene la capacidad de avisar con un sonido configurable cuando hay un cambio en ella; el sonido se apaga con un botón con un cuadro en la esquina inferior derecha.
5. Para visualizar información de una oficina, pulse directamente sobre el nombre de la misma. Esto le permite, en otra ventana, seleccionar el equipo de interés dentro de esa oficina y ver su desempeño.
6. En todas las pantallas puede pulsar el botón de Ayuda para más indicaciones. Mientras el servidor está corriendo, usted va a recibir correos con la información sobre enlaces caídos, por lo que puede cerrar y abrir la aplicación sin afectar su desempeño.