

DESARROLLO DE UN APLICATIVO PARA  
MONITOREO DE RED



JOHN ENRIQUE GUAYAZÁN ORTÍZ  
HENRY ALBERTO MACHADO SÁNCHEZ

UNIVERSIDAD DE SAN BUENAVENTURA  
FACULTAD DE INGENIERÍA  
PROGRAMA DE INGENIERÍA ELECTRÓNICA  
BOGOTÁ D.C.  
2007

DESARROLLO DE UN APLICATIVO PARA  
MONITOREO DE RED



JHON ENRIQUE GUAYAZÁN ORTÍZ  
HENRY ALBERTO MACHADO SÁNCHEZ

Proyecto de grado como requisito  
para optar por el Título de  
Ingenieros Electrónicos

Asesor  
Msc. Ing. HAROLD ALEXANDER PIÑEROS

UNIVERSIDAD DE SAN BUENAVENTURA  
FACULTAD DE INGENIERÍA  
PROGRAMA DE INGENIERÍA ELECTRÓNICA  
BOGOTÁ D.C.  
2007

## **DEDICATORIA**

Jhon Guayazán: dedico especialmente este trabajo a mis padres Blanca Sofia Ortiz y Jorge Enrique Guayazán, por la paciencia y el apoyo incondicional a lo largo de mis años de estudio.

Henry Alberto Machado Sánchez: dedico con mucho cariño este esfuerzo a mi familia, a mis padres y a mis hermanas, sin quienes este trabajo no podría haber sido posible .

## **AGRADECIMIENTO**

Nos gustaría aprovechar este espacio para mostrar nuestro mas profundo agradecimiento a todas aquellas personas e instituciones que de alguna manera, formaron parte importante de este logro tan significativo para nosotros. Consideramos que este proyecto de grado es el fruto de un gran trabajo en equipo y que todas las personas con las que participamos e interactuamos durante estos meses, ayudaron a la culminación y el alcance de nuestras metas propuestas, tanto académicas como de desarrollo personal.

En primer lugar queremos agradecerle especialmente al Msc. Ing. Harold Alexander Piñeros Forero, experto en el área comercial y operativa de telecomunicaciones, tecnologías de la información, y gestión de redes, por su gran apoyo a lo largo de este tiempo, tanto en el ámbito académico como en lo personal. Agradecemos mucho su entusiasmo y la dedicación que siempre mostró durante la realización de este proyecto, pero sobre todo, le damos gracias por su gran calidad humana y por todo el tiempo que dedicó a este proyecto.

Así mismo al ingeniero Julio César Caldas, quien participó en la fase de investigación de este trabajo.

En el plano personal, nos gustaría agradecer a nuestros padres, por su ejemplo y su constante apoyo, y porque estos logros son también fruto de toda su enseñanza.

También nos gustaría expresar nuestro especial agradecimiento al ingeniero Henry Pacheco, Gerente de Operaciones Tecnológicas del BCSC (Banco Caja Social de Ahorros - Colmena), quien de igual manera, colaboró en gran medida en este proyecto, permitiéndonos probar el aplicativo en el BCSC.

**NOTA DE ACEPTACIÓN**

---

---

---

Jurado

---

---

---

Jurado

---

---

---

Presidente del Jurado

Bogotá D.C., noviembre 6 de 2007

## GLOSARIO

*ACSE: (Association Control Service Element)* Se utiliza para establecer y liberar asociaciones entre entidades de aplicación.

**Bases de datos:** Conjunto de datos organizados de una manera estructurada, y los cuales están interrelacionados

**Cisco Works:** Programa de gestión de red desarrollado por CISCO.

**CMIP:** Protocolo de administración de red que define la comunicación entre las aplicaciones de administración de red y la gerencia de los agentes

**CMISE: (Common Management Information Service Element)** Proporciona los servicios básicos de administración confirmados y no confirmados para reportar eventos y manipular datos de administración.

**Enrutadores:** Dispositivos que hacen funciones de la capa 3 del modelo OSI. Direccionan tráfico en una red utilizando direcciones lógicas.

**FCAPS (Fault Management-Gestión de fallas, Configuration Management-Gestión de configuración, Accountant Management-Gestión de Contabilidad, Performance Management-Gestión de Desempeño y Security Management-Gestión de Seguridad).**

**HP Openview:** Programa de gestión de red desarrollado por HP que consta de varios módulos

**ICMP (Internet Control Message Protocol):** Es un programa de verificación para conocer el estado de una conexión TCP/IP. El comando PING trabaja enviando un número determinado de paquetes IP a un destino específico dependiendo de la necesidad del usuario, aunque el valor de paquetes predeterminados es de 4.

**IP (Internet Protocol):** Es un protocolo de máximo esfuerzo de entrega no orientado a conexión, utilizado más que ningún protocolo, actualmente en Internet.

**Latencia:** Es la cantidad de tiempo que demora un paquete en el transito desde su origen hasta su destino.

**MIB (Management Information Base):** Define los objetos que pueden ser gestionados para cada capa en el protocolo TCP/IP.

**MODELO OSI:** Sistema de interconexión abierto. Es un sistema utilizado para el estudio del comportamiento de las redes, que no se utiliza en la práctica y se compone de 7 capas, aplicación, presentación, sesión, transporte, red, enlace de datos y física.

**MODELO TCP/IP:** Sistema de interconexión de redes utilizado en la práctica a diferencia del modelo OSI. Se compone de 4 capas, aplicación, transporte, internet y acceso a la red.

**MRTG (Multi Traffic Grapher):** Programa de gestión de red de licenciamiento gratuito.

**MySQL:** Gestionador de bases de datos de licencia libre para uso personal.

**Navegador WEB:** Un navegador WEB es una aplicación que interpreta código HTML, y otros muchos añadiéndole los Plug-ins correspondientes.

**NMS (Network Management System):** Sistemas de gestión de red.

**Ping:** Programa de verificación para conocer el estado de una conexión TCP/IP. El comando PING trabaja enviando un número determinado de paquetes IP a un destino específico

**Protocolos de RED:** Los protocolos de red son un conjunto de reglas o normas gracias a los cuales es posible que hoy día dos o más hosts a través de una red puedan intercomunicarse,

**PRTG (Paessler Router Traffic Grapher):** Programa de gestión de red gratuito.

**Publik:** Pantalla compuesta de matrices de led, que despliega mensajes de interés común. Puede ser monocromática o contener varios colores.

**ROSE: (Remote Operation Service Element)** Es el equivalente OSI a una llamada de un procedimiento remoto. ROSE permite la invocación de una operación en un sistema remoto.

**SNMP (Simple Network Management Protocol):** Protocolo de capa de aplicación que fue diseñado para facilitar la administración de los dispositivos de una red.

**Tivoli:** Programa de gestión de red desarrollado por IBM.

**TMN (Telecommunications Management Network):** Modelo de red de gestión de telecomunicaciones.

**SLAs (Service Level Agreement SLA):** Acuerdos de Nivel de Servicio pactados por el cliente final con sus proveedores de comunicaciones.

## CONTENIDO

	pág
INTRODUCCIÓN	13
1. PLANTEAMIENTO DEL PROBLEMA	14
1.1 ANTECEDENTES	14
1.2 DESCRIPCIÓN Y FORMULACIÓN DEL PROBLEMA	14
1.3 JUSTIFICACIÓN	15
1.4 OBJETIVOS DE LA INVESTIGACIÓN	16
1.4.1 Objetivo General	16
1.4.2 Objetivos Específicos	16
1.5 ALCANCES Y LIMITACIONES DEL PROYECTO	17
1.5.1. Alcances.	17
1.5.2. Limitaciones.	18
2. MARCO DE REFERENCIA	19
2.1 MARCO TEÓRICO CONCEPTUAL	19
2.1.1 Administración de Redes.	20
2.1.2 SNMP	21
2.1.3 CMIP	25
2.1.4 Bases de datos.	28
2.1.5 MIB.	31
2.1.6 Protocolo IP.	31
2.1.7 Modelos de interconexión de sistemas abiertos.	32
2.1.8 ICMP	33
2.1.9 PING	36
2.1.10 TTL o Tiempo de Vida.	37
2.1.11 Latencia.	37
2.1.12 Navegador Web.	37
2.1.13 Redes De Datos.	38



2.1.14 Protocolos de red.	39
2.2 MARCO LEGAL O NORMATIVO	40
3. METODOLOGÍA	43
3.1 ENFOQUE DE LA INVESTIGACIÓN	43
3.2 LÍNEA DE INVESTIGACIÓN	43
3.3 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN	43
3.4 HIPÓTESIS	43
3.5 VARIABLES	43
3.5.1. Variables Independientes	43
3.5.2. Variables Dependientes	44
4. PRESENTACIÓN Y ANÁLISIS DE RESULTADOS	45
4.1 PÁGINA DE PRESENTACIÓN O INICIO	45
4.2 MONITOREO DE RED	45
4.3 ANÁLISIS DE RED	46
4.4 DISPONIBILIDAD	47
4.5 DESEMPEÑO	47
5. DESARROLLO INGENIERIL	48
5.1 REQUISITOS	48
5.2 ESPECIFICACIÓN	48
5.3 DISEÑO Y ARQUITECTURA	50
5.4 PRUEBAS	52
5.5 MANUAL DEL USUARIO	55
5.5.1 Requerimientos básicos :	55
5.5.2 Instalación del aplicativo.	56
5.5.3 Operación De Funciones Básicas	59
6. CONCLUSIONES	71
7. RECOMENDACIONES	72
BIBLIOGRAFÍA	73
ANEXOS	74

## LISTA DE FIGURAS

	pág
Figura 1. Elementos que componen SNMP	22
Figura 2. Gestión del protocolo SNMP	24
Figura 3. Formato del datagrama utilizado por el protocolo IP	32
Figura 4. Modelos OSI y TCP/IP	32
Figura 5. Ilustración de varias redes LAN interconectadas con salida a Internet	39
Figura 6. Esquema de monitoreo para el aplicativo	49
Figura 7. Diagrama de Flujo del funcionamiento del programa.	51
Figura 8. Monitoreo en tiempo real de la red del BCSC	52
Figura 9. Monitoreo en tiempo real de trafico para un elemento de red de el BCSC	53
Figura 10. Monitoreo en tiempo real del análisis de trafico Detallado para un elemento de red del BCSC	53
Figura 11. Monitoreo en tiempo real del análisis de trafico en Históricos para un elemento de red del BCSC 1	54
Figura 12. Monitoreo en tiempo real del análisis de trafico en Históricos para un elemento de red del BCSC 2	54
Figura 13. Pop-up de aviso critico desplegado a un operador de red del BCSC	55
Figura 14. Pantalla de Monitoreo de red	60
Figura 15. Menú principal	60
Figura 16. Enlaces monitoreados y su información correspondiente	61
Figura 17. Eventos almacenados en una tabla	62
Figura 18. Alerta generada en el publik	62
Figura 19. Dirección del nodo en estado de alerta	63
Figura 20. Menú de la consola de administración del programa	63

Figura 21. Pantalla de inserción de un nuevo elemento o enlace a ser monitoreado	64
Figura 22. Confirmación de inserción y configuración de nuevo elemento a monitorear	64
Figura 23. Pantalla de Modificación información acerca de elementos de red	65
Figura 24. Pantalla de eliminación de un elemento de red o enlace	65
Figura 25. Pantalla de inserción de un elemento de red o enlace para el análisis de tráfico	66
Figura 26. Pantalla de análisis de tráfico	67
Figura 27. Gráfica de análisis de tráfico sobre el nodo elegido por el usuario en la pantalla anterior.	67
Figura 28. Gráfica Detallada de análisis de tráfico sobre el nodo elegido por el usuario.	68
Figura 29. Pantalla principal de disponibilidad de red	69
Figura 30. Grafica de desempeño de un enlace determinado	69
Figura 31. Pantalla principal de disponibilidad de red	70
Figura 32. Gráfica de latencia de un enlace elegido por el usuario	70

## **LISTA DE ANEXOS**

ANEXO A. REPORTE DE VISITA A EMPRESAS

ANEXO B. ESTADO DEL ARTE

ANEXO C. METODOLOGÍA DE DISEÑO

ANEXO D. ESTUDIO DE ALGUNAS DE LAS APLICACIONES DE SOFTWARE DE MONITOREO MAS CONOCIDAS ACTUALMENTE

ANEXO E. LEY 44 DE 1993

ANEXO F. ESTUDIO DE COSTOS

ANEXO G. CHECKLIST

ANEXO F. SUGERENCIAS DEL JURADO

## INTRODUCCIÓN

La gestión de redes unificada es actualmente uno de los mayores requerimientos de las empresas de telecomunicaciones, ya que la administración manual de las mismas y la cantidad innumerable de sistemas de Monitoreo propietario dificultan la administración. Las compañías necesitan de sistemas de gestión de red (Network Management Systems NMS) que reduzcan los costos globales de funcionamiento y que satisfagan todas sus necesidades sin depender de la marca o el tipo de tecnología.

Este proyecto busca desarrollar una aplicación de Monitoreo en software y hardware para enrutadores Cisco y/o Huawei que puedan ser alcanzables mediante IP, monitoreables mediante ping (ICMP Internet Control Message Protocol) y gestionables bajo SNMP (Simple Network Message Protocol) conforme a las necesidades detectadas sobre algunas de las empresas del país con experiencia en el área de las telecomunicaciones y de las tecnologías de información. Por confidencialidad algunas de estas empresas no permiten publicar sus nombres y mucho menos permitir que se conozca cómo realizan el monitoreo, gestión y seguridad de red, aunque para todos es conocido que realizan estas tareas con aplicaciones como HP Openview, Cisco Works, Whatsup, PRTG, MRTG, Netcool o con aplicativos propietarios de las mismas empresas y en el mejor de los casos con Tivoli.

Debido a lo anterior y a los grandes costos que implica adquirir herramientas como Tivoli o Netcool, se propone el desarrollo de un sistema integrado de monitoreo tanto en hardware (Monitoreo en hardware por medio de una pantalla tipo publik en donde se puedan visualizar únicamente los eventos significativos ocurridos sobre los elementos de red) como en software basado en estándares abiertos que permitan a futuro integraciones o ampliaciones de una forma fácil y funcional.

# **1. PLANTEAMIENTO DEL PROBLEMA**

## **1.1 ANTECEDENTES**

En la actualidad existen muchos tipos de monitores y gestores de red, pero cada uno de ellos en su gran mayoría especializados en un reducido número de funciones. Es decir, dichos programas han sido diseñados para tratar un sólo problema o no están orientados a los requerimientos reales del sector de las telecomunicaciones y tecnologías de Información, en aspectos como la gestión de fallos, gestión de configuración, gestión de contabilidad, gestión de desempeño y gestión de seguridad. Entre ellos es de destacar programas como HP Openview, Cisco Works, Whatsup, PRTG, MRTG, Netcool, "P2P Hazard v.14 Beta", que es un programa para bloquear rangos o IPs no deseadas en el ordenador; y "Router IP Console 3.3" que asegura el tráfico de red mediante un administrador de routers, entre otros.

En Colombia, Telmex cuando aún era conocida como AT&T Latinoamérica desarrolló un aplicativo para poder visualizar el tráfico de red así como el monitoreo de los elementos de red vía interface web, permitiendo de esta manera proporcionar al cliente final un estado del ancho de banda consumido en tiempo real y a su vez facilitar la atención oportuna de un evento o falla de red de una manera mucho más ágil. Adicionalmente, es de resaltar que en el entorno de las telecomunicaciones existen empresas como Telefónica Telecom que a la fecha cuentan con software para la gestión de red especializado para cada tipo de fabricante de elementos de red, haciendo que el monitoreo y gestión de red sea una labor de difícil manejo, destacando el hecho que el contar con un diverso número de aplicativos aumenta en gran medida los tiempos de atención y solución de una falla.

## **1.2 DESCRIPCIÓN Y FORMULACIÓN DEL PROBLEMA**

Si bien existe software general que ayuda en la administración de redes, y que a pesar de que existen aplicativos de gestión de red con soluciones completas, algunos de ellos son demasiado costosos (como es el caso de Tivoli), y algunos a pesar de ser razonablemente asequibles en precio no integran todas las funciones especializadas que requiere una empresa de telecomunicaciones o no están acorde al modelo FCAPS (Fault Management-Gestión de fallas, Configuration Management-Gestión de configuración, Accountant Management-Gestión de Contabilidad, Performance Management-Gestión de Desempeño y Security Management-Gestión de Seguridad). Las empresas con una infraestructura de red grande o aquellas proveedoras de servicios de telecomunicaciones normalmente se ayudan de programas generales, robustos, costosos y que finalmente le dejan

al usuario final expectativas sin cumplir, teniendo entonces que adquirir nuevo software o hacer modificaciones a los programas, siendo esto último una tarea difícil que podría incluso requerir permiso expreso del autor del aplicativo. Otra opción a la que se recurre frecuentemente en estas empresas es adquirir más de un software para cumplir las diferentes necesidades, lo cual se traduce en un aumento enorme de los costos de operación debido a que deben contratarse personas especializadas en el manejo de cada nuevo software adquirido. La opción que se maneja en este proyecto es desarrollar un software más especializado en este campo, a la medida de la empresa, en un lenguaje amable y fácil de editar como es el PHP.

Teniendo en cuenta lo anteriormente argumentado, surge la siguiente pregunta:

¿Qué características referentes a monitoreo debe tener el aplicativo a desarrollar para cubrir las necesidades básicas de una empresa de telecomunicaciones, sin que sus costos de operación se incrementen de una forma dramática?

Como respuesta a dicho interrogante se propone y ofrece la solución que se expone en los siguientes apartes de este proyecto de grado.

### **1.3 JUSTIFICACIÓN**

Es importante destacar que a pesar de que un proyecto de este tipo no genera ganancias directas sobre una empresa de Telecomunicaciones o influye directamente en la sociedad Colombiana, el desarrollar estos aplicativos influye a mediano y largo plazo en la agilidad de administración de los recursos de red y por tal motivo reduce los costos implícitos en la gestión, tales como aquellos asociados al mantenimiento preventivo y correctivo de los enlaces, lo que permite proporcionar a los clientes finales mejor atención y por ende un alto grado de satisfacción al usuario.

Si el sector de telecomunicaciones contara con facilidades diseñadas por recurso humano nacional y acorde a los requerimientos propios, evitaría tener que invertir en aplicativos sumamente costosos y no orientados a lo que realmente se necesita.

Adicionalmente, es de resaltar que el proyecto planteado busca incrementar el campo investigativo en el país del área de la gestión de redes, lo que proporcionaría a futuro un mejor nivel socio-económico del mismo dentro de Colombia, beneficiando a gran parte de la sociedad colombiana que hace uso de algún servicio de teleinformática asociado a redes de comunicaciones.

De forma más específica, la acción directa sobre las empresas de telecomunicaciones es poder proporcionar un soporte técnico personalizado y

especializado, pues mediante la aplicación de este proyecto se podrá lograr una mejor relación con el cliente final, proactiva, ágil, precisa y personalizada.

El proyecto es factible debido a que los recursos necesarios para desarrollarlo están al alcance, tanto humanos, como físicos. Existe mucha documentación en Internet y libros acerca del lenguaje PHP, bases de datos de MySQL y Servidores funcionando bajo Apache, lo cual garantiza fuentes de información suficientes para el desarrollo de la aplicación. El proyecto como se mencionó anteriormente, está soportado bajo software de licenciamiento libre, como es el caso del lenguaje de programación PHP, el Apache y MySQL, lo cual garantiza que el costo económico del proyecto sea muy pequeño, reduciéndose prácticamente al costo que implica invertir en la adquisición del computador que esta siendo utilizado, y al costo de la mano de obra.

## **1.4 OBJETIVOS DE LA INVESTIGACIÓN**

### **1.4.1 Objetivo General**

Desarrollar una aplicación en hardware y software para detección de fallas, monitoreo del desempeño de una red, y conteo de bits de entrada y salida en elementos de red.

### **1.4.2 Objetivos Específicos**

- Desarrollar un módulo que permita identificar fallas en una red de datos debido a patrones como retardos excesivos en el intercambio de datos o intermitencia en la comunicación entre dos equipos de red, esto con base en observaciones durante la visita a diferentes empresas del sector de las telecomunicaciones y el estudio de algunas de las aplicaciones de software de monitoreo más conocidas actualmente.
- Desarrollar e implementar el módulo de consola de administración, monitoreo de red, detección de fallas, monitoreo del desempeño de red, y que permita el poblado de tablas en mysql, que faciliten el ordenamiento y manipulación de los registros a utilizar en las diferentes etapas del aplicativo.
- Implementar la solución por medio de hardware (utilizando una pantalla tipo Publik).
- Implementar un módulo de monitoreo de contabilidad, entendiéndose que para llevar a buen término dicho módulo, se utilizará y acoplará la herramienta conocida en el mercado como MRTG “Multi Router Traffic Grapher”, mediante la cual se podrá llevar el conteo de los bits entrantes y salientes de un elemento de red.



- Realizar pruebas de la aplicación desarrollada, de forma tal que la aplicación de la metodología descrita conlleve a la realización de este proyecto.

## **1.5 ALCANCES Y LIMITACIONES DEL PROYECTO**

**1.5.1. Alcances.** Este proyecto culmina con la entrega de una aplicación en hardware y software para monitoreo de fallas, desempeño, y conteo de bits de entrada y salida para enrutadores Cisco y/o Huawei, conforme a las necesidades detectadas sobre algunas de las empresas del país con experiencia en el área de las telecomunicaciones y de las tecnologías de información.

La idea planteada es desarrollar un aplicativo basado en las necesidades de las empresas del sector de telecomunicaciones, y para ello se propone la solución mediante un desarrollo basado en PHP, y poblar bases de datos en MySQL, que se actualizarán mediante scripts en lenguaje batch para aquellos sistemas basados en Windows.

Se pretende cubrir de forma global las necesidades básicas de una empresa de telecomunicaciones o de tecnologías de información para monitoreo de enrutadores Cisco y/o Huawei que puedan ser alcanzables mediante IP, monitoreables mediante ping (ICMP Internet Control Message Protocol) y gestionables bajo SNMP (Simple Network Message Protocol); en cuanto a la capa de gestión de red del modelo de Red de Gestión de Telecomunicaciones TMN (Telecommunications Management Network), se cubrirá únicamente las áreas funcionales de F (Fault Management-Gestión de fallas), A (Accountant Management-Gestión de Contabilidad), y P (Performance Management-Gestión de Desempeño). El producto final debe cumplir todos los requerimientos tecnológicos; teniendo en cuenta que se deben desarrollar las siguientes interfaces:

- a. Monitoreo en hardware, utilizando una pantalla tipo publik en donde se puedan visualizar únicamente los eventos significativos ocurridos sobre los elementos de red.
- b. Monitoreo en software de:
  - Recursos de red
  - Tráfico de entrada y salida de los recursos de red, indicando el consumo diario, semanal y anual.
  - Latencia de red
  - Generación de alertas ante eventos no esperados.
- c. Administración, mediante la cual se podrá configurar la aplicación y agregar, borrar o modificar los elementos a monitorear.

Adicionalmente, el aplicativo a desarrollar contará con las siguientes funcionalidades:

- Generación de alertas mediante mensajes emergentes (Cuadros informativos que desplieguen los cambios de estado de los recursos de red sobre las pantallas de los PC, haciendo uso del aplicativo Net Send de Windows).
- Visualización de los niveles exactos de disponibilidad del servicio prestado al cliente final, permitiendo de esta manera el estricto y real seguimiento al cumplimiento de los SLAs (Service Level Agreement SLA) “Acuerdos de Nivel de Servicio” pactados por el cliente final con sus proveedores de comunicaciones.

**1.5.2. Limitaciones.** Se desarrollará una solución mediante la cual se pueda realizar el monitoreo de enrutadores marca Cisco y/o Huawei que cubra únicamente y parcialmente las áreas funcionales de F (Gestión de Fallas), A (Gestión de Contabilidad) y P (Gestión de Desempeño) de la capa de gestión de red del modelo TMN.

La solución a desarrollar no incluye las áreas funcionales C (Gestión de configuración) y S (Gestión de Seguridad) de la capa de gestión de red del modelo TMN, ya que es muy difícil crear módulos que sean lo suficientemente abiertos para poder configurar y asegurar la totalidad de elementos de diferentes marcas y se incrementaría considerablemente la complejidad del proyecto.

Para las áreas funcionales que si se cubrirán con la solución expuesta en este proyecto de grado, se desarrollará un aplicativo capaz de monitorear enrutadores que sean alcanzables mediante IP, monitoreables mediante ping (ICMP Internet Control Message Protocol) y gestionables bajo SNMP (Simple Network Message Protocol).

Las visitas a las empresas de telecomunicaciones están sujetas a las condiciones expuestas por las mismas, ya que muchas de estas empresas no permiten que se realice dicha acción, por motivos de privacidad y seguridad.

## 2. MARCO DE REFERENCIA

### 2.1 MARCO TEÓRICO CONCEPTUAL

Una red de datos debe contar con un sistema de administración porque hay que asegurar a sus usuarios la operación de los medios que permiten el uso de recursos de red. La monitorización del tráfico y la Calidad de Servicio, QoS, evitan problemas, y son muy importantes para llegar a una solución rápida y eficaz.

La monitorización de redes de cierto tamaño, no puede hacerse a mano. A medida que se hacen más heterogéneas, se requieren herramientas automatizadas de gestión de fallos, de cuentas, de configuración y nombres, de prestaciones y de seguridad, basadas sobre estándares, que funcionen sobre la gran variedad de equipos de diferentes fabricantes, con interfaces de operador únicos, con un conjunto de ordenes que realicen todas las tareas de administración de la red, con un software incorporado en las estaciones de usuario y en los dispositivos de red con capacidad de recoger estadísticas del equipo en que se aloja, responder a las ordenes del centro de control y enviar mensajes bajo condiciones establecidas, y con capacidad de generación de estadísticas, y de informes.<sup>1</sup>

Según las redes crecen y evolucionan, la administración se convierte en el recurso más crítico e importante para una organización.

A medida que una red organizativa crece, la administración de la red se hace cada vez más difícil, por ello se necesita que el administrador o los administradores de red, cuenten con las herramientas pertinentes, para poder diagnosticar fallos, prevenir situaciones que puedan perturbar el correcto funcionamiento de la red, esto obviamente de una forma activa y en tiempo real, con los menores retardos posibles.

Las tareas de un administrador de red, incluyen lo siguiente:

- Monitorear la disponibilidad de la red.
- Mejorar la automatización (por medio de un software como el planteado en este proyecto).
- Monitorear el tiempo de respuesta.
- Establecer, configurar y monitorear políticas de seguridad.

---

<sup>1</sup> CISCO SYSTEM. Guía del primer año CCNA 1 y 2. Madrid. Editorial Pearson, 2004.p.46

- Definir estructuras para garantizar redundancia y rápido restablecimiento de los servicios de red.
- Realizar el registro de usuarios.

La administración de red engloba los siguientes aspectos<sup>2</sup>:

- Controlar los medios corporativos: Sin un control efectivo de los recursos de la red, dichos recursos no ofrecerán el rendimiento preciso.
- Control de la complejidad: Con el importante crecimiento que sufren las redes en el número de componentes, usuarios, interfaces, protocolos, vendedores, la pérdida de control de la misma y de sus recursos es una amenaza para la administración.
- Mejora del servicio: Los usuarios esperan el mismo rendimiento, o incluso mejor, según la red crece y los recursos se distribuyen de una forma mas adecuada.
- Balanceo de diversas necesidades: Los usuarios deben disponer de diferentes aplicaciones para un nivel de soporte dado, con una especial atención a las áreas de rendimiento, disponibilidad y seguridad.
- Reducción de los tiempos muertos: Asegurar una disponibilidad elevada de los recursos gracias al propio diseño redundante.
- Control de costes: monitorizar y controlar la utilización de los recursos para que los usuarios estén satisfechos a un coste razonable.

**2.1.1 Administración de Redes.** Cada día se busca más la centralización de la administración de las redes de datos, para esto se siguen unas tareas como las que se muestran a continuación:<sup>3</sup>

- Control de activos empresariales: Si los recursos de red no se controlan de forma efectiva, no proporcionarán los resultados exigidos por los procesos gerenciales.
- Control de la complejidad: Con el crecimiento masivo del número de componentes, usuarios, interfaces, protocolos y proveedores de equipos, la pérdida de control de la red y de sus recursos, amenaza los procesos gerenciales.
- Mejor nivel de servicio: Los usuarios esperan un nivel de servicio igual o mejor a medida que crece la red y que aumente la distribución de recursos.

---

<sup>2</sup> Ibid., p. 58

<sup>3</sup> CISCO SYSTEM. Op. Cit., p. 20

- Equilibrio de las diversas necesidades: Los usuarios deben poder contar con diversas aplicaciones a un nivel de servicio dado, con requisitos específicos en cuanto a rendimiento, disponibilidad y seguridad.
- Reducción de las interrupciones del servicio: Garantizar una alta disponibilidad de los recursos mediante un adecuado diseño redundante.
- Control de costos: Monitorear y controlar la utilización de los recursos a fin de satisfacer las necesidades del usuario de una forma satisfactoria.

Para permitir la interoperabilidad entre las distintas plataformas de red, los estándares de administración han forzado a los fabricantes a que puedan incorporar todos estos estándares. Estos son los estándares más utilizados :<sup>4</sup>

- SNMP (Simple Network Management Protocol)
- CMIP (Common Management Information Protocol)

**2.1.2 SNMP.** hace referencia a un conjunto de estándares para la administración de red que incluye un protocolo, una especificación de estructura de bases de datos y un conjunto de objetos de datos. En pocas palabras, SMNP es un protocolo de capa de aplicación que fue diseñado para facilitar el intercambio de información entre los dispositivos de una red. Usando SNMP y gracias al número de paquetes de datos por segundo enviados a una interfaz o conexión TCP abierta, los administradores de la red pueden controlar fácilmente su rendimiento y resolver los problemas que pueden aparecer<sup>5</sup>.

SNMP es el protocolo más popular en estos momentos para el control de internetwork comerciales universitarias y de investigación. La actividad de normalización continua en cuanto a que los fabricantes desarrollan nuevas tecnologías y aplicaciones de administración basadas en SNMP de avanzada tecnología. SNMP es un protocolo relativamente simple, pero su conjunto de funciones es lo suficientemente potente como para manipular la gran variedad de problemas que se presentan en la administración de los diferentes tipos de redes que existen.

El modelo organizativo para la administración de redes basadas en SNMP está compuesto por 4 elementos:

- Administración de estación.
- Administración de agente.

---

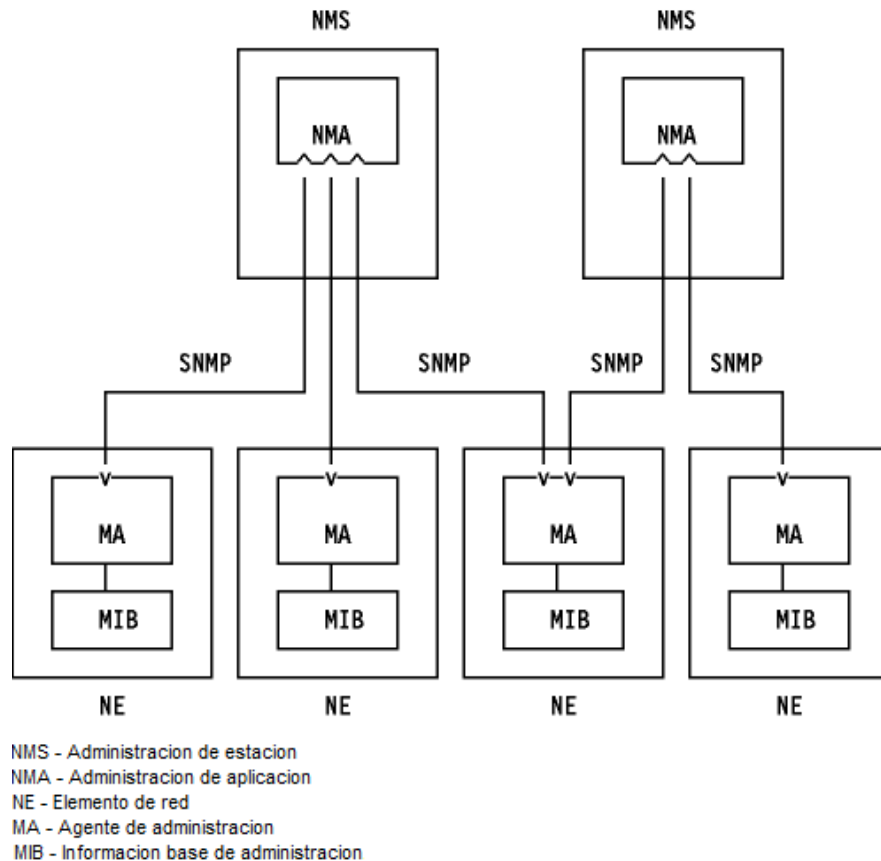
<sup>4</sup> CISCO SYSTEM. Op. Cit., p. 23

<sup>5</sup> [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/snmp.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm)

- MIB (Management Information Base; en español, Información base de administración).
- Protocolo de administración de red.

La siguiente figura ilustra estos 4 elementos de forma jerárquica:

Figura 1. Elementos que componen SNMP



Fuente: <http://ditec.um.es/laso/docs/tut-tcpip/3376c414.html#snmp>

### – Administración de estación

Entidad gestora: Es una aplicación con control humano que se ejecuta en una estación centralizada (Network Operations Center; en español, centro de operaciones de la red). Se encarga de controlar la recolección, procesamiento, análisis y visualización de la información de gestión. También es donde se inician las acciones que controlan el comportamiento de la red, y donde el administrador de la red interactúa con los dispositivos de la red.

Dispositivos gestionados: Es una componente de la red, incluye al equipo de comunicaciones y al software.

En el equipo hay diversos objetos gestionados (por ejemplo una tarjeta, un protocolo de enrutamiento, etc ) y contiene lo siguiente:

- Un agente (es un proceso que se ejecuta en cada dispositivo residente y se encarga de comunicar con la entidad gestora y actualizar la MIB)
- Una base de datos de gestión (MIB).

Protocolos de Gestión: Permite a la entidad gestora comunicarse con los agentes

- Permite al gestor comunicarse con el agente para conocer el estado de los dispositivos (consultar la MIB).
- Los agentes pueden informar al gestor de situaciones "anómalas" en los dispositivos.
- El protocolo no controla por si mismo, sino que proporciona una herramienta con la que el administrador de red puede gestionar la red (supervisar, comprobar, sondear, configurar, analizar, evaluar, controlar, etc).

El protocolo por si solo puede generar unas alertas o Traps que comunicarán sucesos o acciones inusuales, sin que estos hayan sido solicitados por la unidad gestora o NMS. Cuando se solicita información del agente (proceso llamado `snmpd` que permite la comunicación con la NMS, mediante el protocolo UDP User Datagram Protocol), se solicita mediante un mecanismo denominado *get-response* (petición de consulta) y recibe la respuesta mediante su homólogo *get-request* (petición de respuesta).

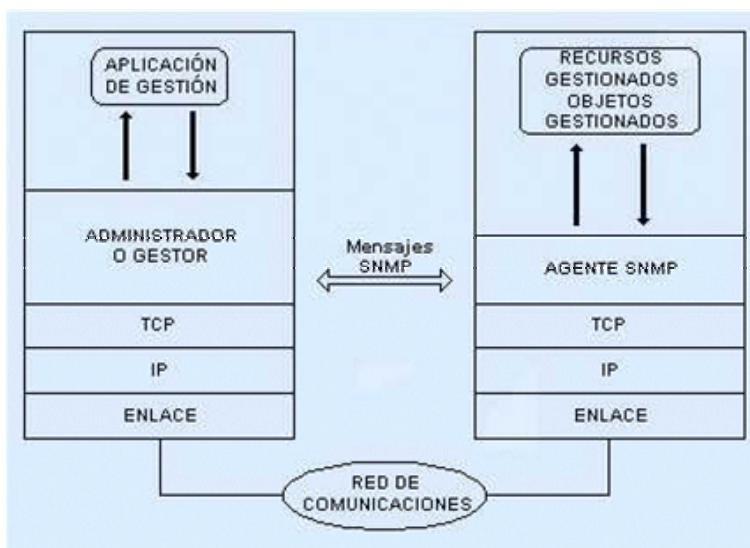
Toda la información del agente se guarda en la MIB (la cual será descrita con mas detalle mas adelante), formando una estructura de árbol y presentada en forma de objetos.

Se debe tener un control sobre quien puede y quien no puede ver/realizar cambios en Base de datos MIB. Básicamente el método de autenticación se basa en `community strings` (cadenas de comunidad; dichas cadenas actúan como contraseñas que delimitan el entorno en donde trabajará SNMP). Los `community strings` son una especie de claves sin nombre de usuarios que se asignan según la operación que se desea realizar, que puede ser leer o escribir en la base de datos.

Los controles de acceso varían de acuerdo a la versión de SNMP que se este manejando. En la versión SNMPv1 por ejemplo, una vez conocido el valor del

community string, se tiene acceso total a la base de datos, pudiendo leer de la misma o modificarla, según sea el caso. Es interesante hacer notar que el manager envía la clave al agente sin encriptar, en código ASCII, con el riesgo que eso conlleva. Los community strings por defecto son "public" y "private".

Figura 2. Gestión del protocolo SNMP



Fuente: [http://www.btwsa.com.ar/Grafs/\\_snmp1gif.gif](http://www.btwsa.com.ar/Grafs/_snmp1gif.gif)

En la versión SNMPv2 se plantearon varios modelos de autenticación, empezando con uno basado en listas de control de acceso, en el cual los derechos que tiene cada manager sobre el agente se basan en su dirección ip, en diversas claves de autenticación, en la acción solicitada por el manager (get o set), etc. Actualmente se ha pasado a otro modelo denominado USEC, *User based Security Model*, mejorando considerablemente la autenticación, control de acceso y privacidad de todo el sistema.

Los programas de gestión de red son desarrollados bajo SNMP (Protocolo Simple de Administración de Redes) e ICMP (Internet Control Message Protocol). Dichos protocolos contemplan la ejecución de ciertas aplicaciones desde un servidor, la cual es una estación de trabajo más robusta que utiliza un software especial de interconexión con la red.

El administrar una red requiere tener en cuenta varios aspectos importantes como lo son controlar los elementos involucrados en la red, que corresponde a ejercer un control eficaz sobre los recursos de la red que no ofrezcan el rendimiento preciso. También es importante para el administrador de la red, ejercer un control de complejidad que le permita tener bajo su poder el crecimiento de la red,



mediante lo cual es posible mantener conocimiento continuo y verídico del número de componentes, usuarios, interfaces, protocolos y vendedores. El correcto control de dichas variables, permite poner a disposición del usuario mejoras en el servicio y áreas de rendimiento, disponibilidad y seguridad mayores.

**2.1.3 CMIP** El Protocolo de administración de información común (CMIP) es un protocolo de administración de red que define la comunicación entre las aplicaciones de administración de red y la gerencia de los agentes. CMIP se basa en el modelo OSI (*Open Systems Interconnection*) y es definido por la serie de recomendaciones ITU-T X.700<sup>6</sup>.

CMIP define la información de la gerencia en términos de objetos administrados y permite tanto la modificación como las acciones sobre objetos manejados. Se describen usando GDMO y los objetos son identificados por un nombre distinguido (DN), similar en concepto al directorio X.500.<sup>7</sup>

CMIP también proporciona buena seguridad (autorización de la ayuda, control de acceso y registros de la seguridad) y un reporte flexible de las condiciones inusuales de la red.

CMIP fue diseñado teniendo en cuenta a SNMP solucionando los errores y fallos que tenía SNMP y volviéndose un administrador de red mayor y más detallado. Su diseño es similar a SNMP por lo que se usan PDUs (Protocol Data Unit) como 'variables' para monitorear la red. En CMIP las variables son unas estructuras de datos complejas con muchos atributos, que incluyen:

- Variables de atributos: Representan las características de las variables.
- Variables de comportamiento: Qué acciones puede realizar.
- Notificaciones: La variable genera una indicación de evento cuando ocurre un determinado hecho.

CMIP es un protocolo de administración de red implementado sobre OSI. La administración OSI posibilita monitorizar y controlar los recursos de la red que se conocen como objetos administrados. Para especificar la estandarización de la administración de red se determinan los siguientes modelos:

- Modelo de organización: Describe la forma en que las funciones de administración se pueden distribuir administrativamente. Aparecen los dominios como particiones administrativas de la red.

---

<sup>6</sup> [http://es.wikipedia.org/wiki/Base\\_de\\_datos](http://es.wikipedia.org/wiki/Base_de_datos)

<sup>7</sup> Enciclopedia virtual libre, <http://es.wikipedia.org/wiki/CMIP>., Noviembre 4 de 2007, 11:05 P.M

- Modelo funcional: Describe las funciones de administración (de fallos, de configuración, de contabilidad, de seguridad...) y sus relaciones.
- Modelo de información: Provee las líneas a seguir para describir los objetos administrados y sus informaciones de administración asociadas. Reside en el MIB (Management Information Base).

CMIP define una relación de igual a igual entre el administrador y el agente, incluyendo lo que se refiere al establecimiento y cierre de conexión, y a la dirección de la información de administración.

Las operaciones CMIS (Common Management Information Services) se pueden originar tanto en administradores como en agentes, permitiendo relaciones simétricas o asimétricas entre los procesos de administración. Sin embargo, la mayor parte de los dispositivos contienen las aplicaciones que sólo le permiten hacer de agente.

La serie CMIP está compuesta por 6 protocolos que se esquematizan en la siguiente tabla:

#### Protocolos CMIP

Procesos de Administración de Aplicaciones	
CMISE ISO 9595/9596	
ACSE ISO 8649/8650	ROSE ISO DIS 9072-1/2
ISO Presentación ISO	
ISO Sesión ISO	
ISO Transporte ISO	

Como se puede ver, un sistema CMIP debe implementar una serie de protocolos de los cuales el CMISE (Common Management Information Service Element) es el que trabaja mano a mano con CMIP: todas las operaciones de administración de red que crea CMISE el CMIP las mapea en una operación en el CMIP remoto.

#### – Protocolos de aplicación en CMIP.

Para comunicarse entre sí dos entidades de aplicación pares del administrador y del agente se utilizan APDU's (Application Protocol Data Units). Como se sabe, CMIP está compuesto de los protocolos OSI que siguen:

**a. ACSE (Association Control Service Element):** Se utiliza para establecer y liberar asociaciones entre entidades de aplicación. El establecimiento lo puede

realizar el agente o el administrador, y durante el proceso se intercambian los títulos de la entidad de aplicación para identificarse, y los nombres del contexto de aplicación para establecer un contexto de aplicación.

Servicios que ACSE proporciona a CMISE:

- A-ASSOCIATE, servicio confirmado utilizado para inicializar la asociación entre entidades de aplicación.
- A-RELEASE, servicio confirmado usado para liberar una asociación entre entidades de aplicación sin pérdida de información.
- A-ABORT, servicio no confirmado que causa la liberación anormal de una asociación con una posible pérdida de información.
- A-P-ABORT, servicio iniciado por el proveedor que indica la liberación anormal de la asociación del servicio de presentación con posible pérdida de información.

**b. ROSE (Remote Operation Service Element):** Es el equivalente OSI a una llamada de un procedimiento remoto. ROSE permite la invocación de una operación en un sistema remoto. CMIP usa los servicios orientados a conexión proporcionados por ROSE para todas las peticiones, respuestas y respuestas de error.

Servicios que ROSE proporciona a CMISE:

- RO-INVOKE, servicio no confirmado que es usado por un usuario de ROSE para invocar que una operación sea realizada por un ROSE invocado remoto.
- RO-RESULT, servicio no confirmado que un ROSE invocado usa para contestar a una previa indicación RO-INVOKE en el caso de que se haya realizado con éxito.
- RO-ERROR, servicio no confirmado que es usado por un usuario de ROSE invocado para contestar a una previa indicación RO-INVOKE en el caso de que haya fracasado.
- RO-REJECT, servicio no confirmado utilizado por un usuario de ROSE para rechazar una petición (indicación RO-INVOKE) del otro.

**c. CMISE (Common Management Information Service Element).** Proporciona los servicios básicos de administración confirmados y no confirmados para reportar eventos y manipular datos de administración. CMISE hace uso de los servicios proporcionados por ROSE y ACSE. Servicios de CMISE: se denominan unidades funcionales. El número que sigue a cada unidad funcional está

definido por el CMIP. También se especifica en cada caso si se trata de servicio confirmado o no confirmado.

El principal beneficio que aporta el protocolo CMIP es que no sólo se puede enviar información de administración de o hacia un terminal, sino que es posible desarrollar tareas que serían imposibles bajo SNMP. Por ejemplo, si un terminal no puede encontrar un servidor de ficheros en un tiempo predeterminado, CMIP notifica el evento al personal adecuado. En SNMP el usuario tendría que guardar el número de intentos de acceso al servidor mientras que en CMIP de esto se encarga el propio protocolo.

CMIP soluciona varios de los fallos de SNMP. Por ejemplo, tiene incluidos dispositivos de administración de la seguridad que soportan autorizaciones, control de acceso, contraseñas... Como resultado de la seguridad que de por sí proporciona CMIP no necesita de posteriores actualizaciones.

Otra ventaja de CMIP es que haya sido creado no sólo por gobiernos sino que también por grandes empresas, en los que puede tener en el futuro un mercado fiel.

Pero CMIP cuenta con varias desventajas, como son: CMIP requiere 10 veces más recursos de red que SNMP, o sea muy pocas redes de la actualidad son capaces de soportar una implementación completa de CMIP sin grandes modificaciones en la red (muchísima más memoria y nuevos protocolos de agente). La única solución es disminuir el tamaño de CMIP cambiando sus especificaciones. Así han aparecido varios protocolos que funcionan con la base de CMIP con menos recursos, pero todavía no ha llegado el momento de prescindir del tan extendido SNMP. Otro problema de CMIP es su dificultad de programación: existe tal cantidad de variables que solo programadores muy habilidosos son capaces de sacarles todo su potencial.

**2.1.4 Bases de datos.** Es un conjunto de datos organizados de una manera estructurada, y los cuales están interrelacionados<sup>8</sup>.

Un modelo de datos es básicamente una "descripción" de algo conocido como *contenedor de datos* (contenedor de información) así como de los métodos para almacenar y recuperar información de esos contenedores. Estos son algunos modelos de bases de datos:

**a. Bases de datos jerárquicas.** Éstas son bases de datos que almacenan su información en una estructura jerárquica. En este modelo los datos se organizan en una forma similar a un árbol (visto al revés), en donde un nodo padre de

---

<sup>8</sup> <http://www.mysqlja.com.ar/temarios/descripcion.php?cod=2&punto=1>

información puede tener varios hijos. El nodo que no tiene padres es llamado raíz, y a los nodos que no tienen hijos se los conoce como hojas.

Las bases de datos jerárquicas son especialmente útiles en el caso de aplicaciones que manejan un gran volumen de información y datos muy compartidos permitiendo crear estructuras estables y de gran rendimiento.

Una de las principales limitaciones de este modelo es su incapacidad de representar eficientemente la redundancia de datos.

**b. Base de datos de red.** Éste es un modelo ligeramente distinto del jerárquico; su diferencia fundamental es la modificación del concepto de *nodo*: se permite que un mismo nodo tenga varios padres (posibilidad no permitida en el modelo jerárquico).

Fue una gran mejora con respecto al modelo jerárquico, ya que ofrecía una solución eficiente al problema de redundancia de datos; pero, aun así, la dificultad que significa administrar la información en una base de datos de red ha significado que sea un modelo utilizado en su mayoría por programadores más que por usuarios finales.

**c. Base de datos relacional.** Éste es el modelo más utilizado en la actualidad para modelar problemas reales y administrar datos dinámicamente. La idea fundamental es el uso de "relaciones". Estas relaciones podrían considerarse en forma lógica como conjuntos de datos llamados "tuplas". Cada relación es pensada como si fuese una tabla que está compuesta por *registros* (las filas de una tabla), que representarían las tuplas, y *campos* (las columnas de una tabla).

En este modelo, el lugar y la forma en que se almacenen los datos no tienen relevancia (a diferencia de otros modelos como el jerárquico y el de red). Esto tiene la considerable ventaja de que es más fácil de entender y de utilizar para un usuario ocasional de la base de datos. La información puede ser recuperada o almacenada mediante "consultas" que ofrecen una amplia flexibilidad y poder para administrar la información.

El lenguaje más habitual para construir las consultas a bases de datos relacionales es SQL, *Structured Query Language* o *Lenguaje Estructurado de Consultas*, un estándar implementado por los principales motores o sistemas de gestión de bases de datos relacionales.

Durante su diseño, una base de datos relacional pasa por un proceso al que se le conoce como normalización de una base de datos.

Durante los años '80 (1980-1989) la aparición de dBASE produjo una revolución en los lenguajes de programación y sistemas de administración de datos. Aunque nunca debe olvidarse que dBase no utilizaba SQL como lenguaje base para su gestión.

**d. Bases de datos orientadas a objetos.** Este modelo trata de almacenar en la base de datos los *objetos* completos (estado y comportamiento). Una base de datos orientada a objetos es una base de datos que incorpora todos los conceptos importantes en el tema de objetos:

- Encapsulación : Propiedad que permite ocultar la información al resto de los objetos, impidiendo así accesos incorrectos o conflictos.
- Herencia: Propiedad a través de la cual los objetos heredan comportamiento dentro de una jerarquía de clases.
- Polimorfismo: Propiedad de una operación mediante la cual puede ser aplicada a distintos tipos de objetos.

En bases de datos orientadas a objetos, los usuarios pueden definir operaciones sobre los datos como parte de la definición de la base de datos. Una operación (llamada función) se especifica en dos partes. La interfaz (o *signatura*) de una operación incluye el nombre de la operación y los tipos de datos de sus argumentos (o *parámetros*). La implementación (o *método*) de la operación se especifica separadamente y puede modificarse sin afectar la interfaz. Los programas de aplicación de los usuarios pueden operar sobre los datos invocando a dichas operaciones a través de sus nombres y argumentos, sea cual sea la forma en la que se han implementado. Esto podría denominarse independencia entre programas y operaciones.

**e. Bases de datos documentales** Permiten la indexación a texto completo, y en líneas generales realizar búsquedas más potentes. Taurus es un sistema de índices optimizado para este tipo de bases de datos.

**f. Base de datos deductivas.** Un sistema de base de datos deductivas, es un sistema de base de datos pero con la diferencia de que permite hacer deducciones a través de inferencias. Se basa principalmente en reglas y hechos que son almacenados en la base de datos. También las bases de datos deductivas son llamadas base de datos lógicas, a raíz de que se basan en lógica matemática.

**g. Gestión de bases de datos distribuida.** La base de datos está almacenada en varias computadoras conectadas en red. Surgen debido a la existencia física de organismos descentralizados. Esto les da la capacidad de unir las bases de datos de cada localidad y acceder así a distintas universidades, sucursales de tiendas, etc. Para gestionar estas bases de datos se utiliza software especializado en la

gestión de bases de datos como MaxDB, MyISAM, MySQL (utilizada en el desarrollo de este proyecto), entre otras. SQL, Structure Query Language (Lenguaje de Consulta Estructurado) es un lenguaje de programación para trabajar con base de datos relacionales como MySQL, Oracle, etc. MySQL es un interpretador de SQL, es un servidor de base de datos. MySQL permite crear base de datos y tablas, insertar datos, modificarlos, eliminarlos, ordenarlos, hacer consultas y realizar muchas operaciones, en pocas palabras, administrar bases de datos.

**2.1.5 MIB.** El MIB define los objetos que pueden ser gestionados para cada capa en el protocolo TCP/IP. Hay dos versiones, MIB-I and MIB-II, aunque la RFC-1156 declara el MIB-I como obsoleto. Conjunto de objetos que representan los distintos tipos de información sobre un dispositivo, utilizados por el Protocolo simple de administración de redes (SNMP) para administrar el dispositivo<sup>9</sup>.

Como se utilizan tipos de dispositivos y protocolos diferentes para los distintos servicios de administración de red, cada servicio tiene su propio conjunto de objetos.

El sistema de administración (Host A), envía un datagrama de SNMP al agente (Host B) con el nombre de host del agente y la dirección IP o IPX. El agente SNMP recibe el datagrama y comprueba el nombre de comunidad al que pertenece el sistema de administración.

Si es un nombre de comunidad válido, el agente recupera los datos solicitados del subagente SNMP adecuado. Si el nombre de comunidad no es correcto, el agente envía una captura de "error de autenticación" a los destinos de captura (hosts C y D). El agente SNMP devuelve el datagrama al sistema de administración con la información pedida.

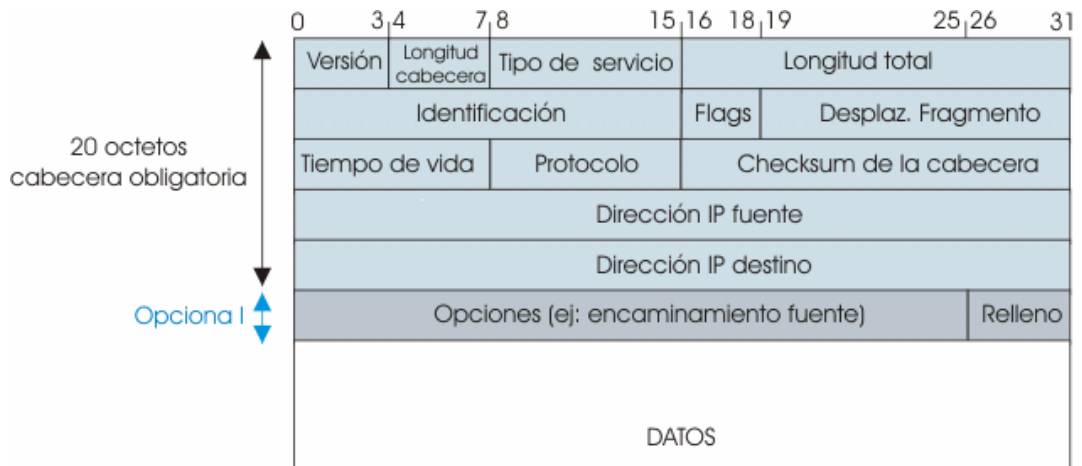
Nombre de comunidad: Nombre utilizado para agrupar hosts SNMP. Este nombre se coloca en los mensajes SNMP enviados entre los dispositivos administrados por SNMP (por ejemplo, entre servidores que ejecutan Windows 2000 Server y estaciones de administración SNMP). Normalmente todos los hosts pertenecen a Public, que es el nombre estándar para una comunidad común de todos los hosts SNMP.

**2.1.6 Protocolo IP.** Es un sistema de máximo esfuerzo de entrega no orientado a conexión, utilizado más que ningún protocolo, actualmente en Internet. El hecho de no estar orientado a conexión lo hace un protocolo relativamente poco fiable para enviar información, debido a que si bien hace el mejor esfuerzo a la hora de enviar el paquete, para que este llegue a su destino, no ofrece garantía alguna de que el datagrama va a llegar como se necesita, a su destino. Se pueden observar el formato del datagrama en la siguiente figura.

---

<sup>9</sup> <http://ditec.um.es/laso/docs/tut-tcpip/3376c414.html#cmot>

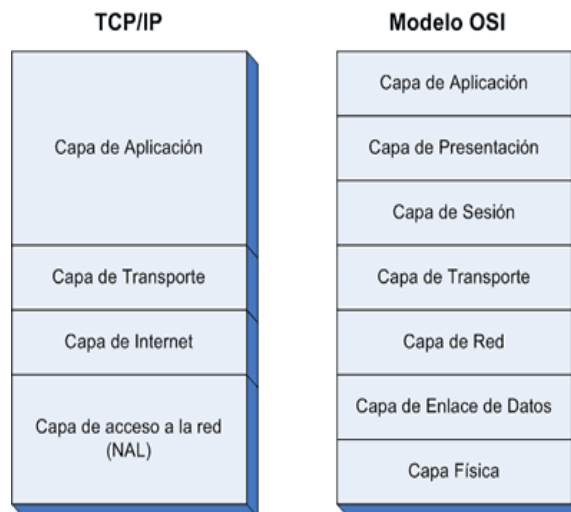
Figura 3. Formato del datagrama utilizado por el protocolo IP



Fuente: [mon.webcindario.com/red/imag/05red05.gif](http://mon.webcindario.com/red/imag/05red05.gif)

**2.1.7 Modelos de interconexión de sistemas abiertos.** TCP/IP es un protocolo que tiene como base varios protocolos que quedan ilustrados en el modelo OSI, en sus 7 capas que muestran el funcionamiento paso a paso de este protocolo, aunque realmente este se rija por el modelo TCP/IP, en la figura 4 se muestran ambos modelos y como se diferencian, siendo OSI un modelo teórico, y TCP/IP un modelo acogido y usado en la práctica.

Figura 4. Modelos OSI y TCP/IP



Fuente: <http://www.textoscientificos.com/imagenes/redes/tcp-ip-osi.gif>



**a. Aplicación:** Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET), HTTP (*Hypertext Transfer Protocol*) y SNMP entre otros.

**b. Transporte:** Para ambos modelos esta capa tiene exactamente las mismas funciones. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos. Obviamente teniendo en cuenta que UDP es un protocolo no orientado a conexión, mientras que TCP es un protocolo orientado a conexión.

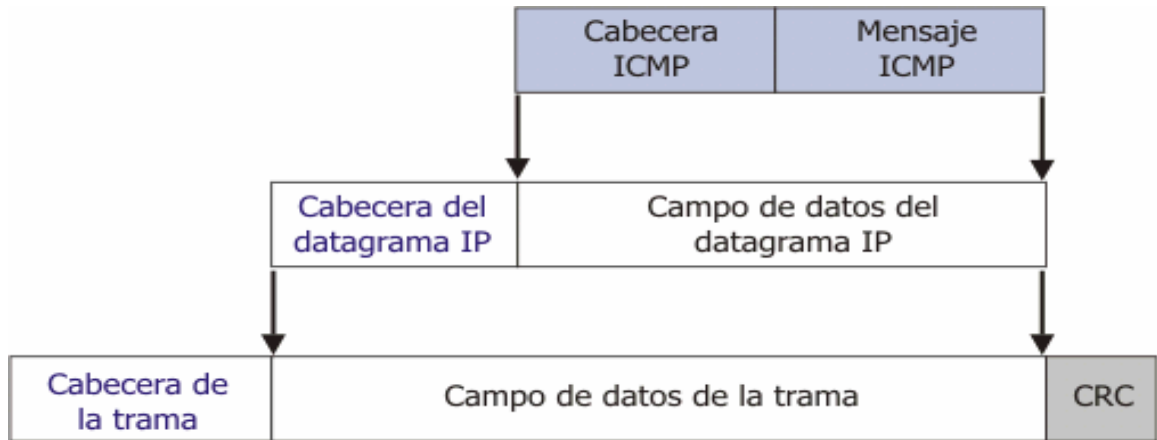
**c. Internet:** Es el equivalente a la capa de red y enlace de datos en el modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes, siendo este un protocolo no orientado a conexión y de máximo esfuerzo.

**d. Físico :** Cumple las mismas funciones tanto en el modelo OSI como en TCP/IP que son la de enviar los datos convertidos en bits después de haberlos recibido de la capa inmediatamente anterior.

**2.1.8 ICMP.** Debido a que el protocolo IP es un protocolo de máximo esfuerzo no orientado a conexión, ICMP (Internet message protocol, protocolo de mensajes de control y error) brinda las herramientas para informar al origen si se ha producido algún error durante la entrega de un mensaje. Por lo tanto ICMP se encarga de transportar varios y diferentes mensajes de control.

ICMP se encarga de notificar aunque no de tomar acciones ante situaciones anormales. Los mensajes ICMP viajan dentro del datagrama de mensajes del protocolo IP tal y como se muestra en el siguiente esquema.

Esquema: Formato del datagrama IP con ICMP incluido



Fuente:[http://mon.frc.utn.edu.ar/sistemas/ingsanchez/Redes/Archivos/Protocolo\\_ICMP.pdf](http://mon.frc.utn.edu.ar/sistemas/ingsanchez/Redes/Archivos/Protocolo_ICMP.pdf)

Los mensajes ICMP se transmiten como datagramas IP normales, con el campo de cabecera "protocolo" con un valor 1, y comienzan con un campo de 8 bits que define el tipo de mensaje.

A continuación viene un campo código, de 0 bits, que a veces ofrece una descripción del error en concreto que se ha producido y después un campo suma de control de 16 bits, que incluye una suma de verificación de errores de transmisión. Tras estos campos viene el cuerpo del mensaje, determinado por el contenido del campo "tipo". Contienen además los 8 primeros bytes del datagrama que ocasionó el error. Los principales tipos de mensaje ICMP son los siguientes:

**a. Mensajes informativos.** Entre estos mensajes hay algunos de suma importancia, como los mensajes de petición de ECO (tipo 8) y los de respuesta de Eco (tipo 0).

Las peticiones y respuestas de eco se usan en redes para comprobar si existe una comunicación entre dos host a nivel de capa de red, por lo que pueden ser útiles para identificar fallos en este nivel, ya que verifican si las capas física, de enlace de datos y red se encuentran en buen estado y configuración. La siguiente tabla ilustra los mensajes informativos del protocolo ICMP:

Código del mensaje	Descripción del mensaje
0	<b>Echo Reply</b> ( <i>Respuesta de Eco</i> )
3	<b>Destination Unreachable</b> ( <i>Destino Inaccesible</i> ) <b>Source Quench</b> ( <i>Disminución del tráfico desde el origen</i> ) <b>Redirect</b> ( <i>Redireccionar - cambio de ruta</i> )
4	
5	
8	
8	<b>Echo</b> ( <i>Solicitud de Echo</i> )
11	<b>Time Exceed</b> ( <i>Tiempo Excedido para un datagrama</i> )
12	<b>Parameter Problem</b> ( <i>problema de parámetros</i> ) <b>Timestamp</b> ( <i>Solicitud de marca de tiempo</i> ) <b>Timestamp Reply</b> ( <i>respuesta de marca de tiempo</i> ) <b>Information Request</b> ( <i>solicitud de información</i> ) - obsoleto- <b>Information Reply</b> ( <i>respuesta de información</i> ) - obsoleto- <b>Addressmask</b> ( <i>solicitud de máscara de dirección</i> ) <b>Addressmask Reply</b> ( <i>respuesta de máscara de dirección</i> )
13	
14	
15	
16	
17	
18	

**b. Mensajes de error.** En el caso de obtener un mensaje ICMP de destino inalcanzable, con campo "tipo" de valor 3, el error concreto que se ha producido vendrá dado por el valor del campo "código", pudiendo presentar los siguientes valores:

Código del mensaje	Descripción del mensaje de error
0	No se pudo alcanzar la red de destino
1	No se puede llegar a la estación de destino
2	El destino no dispone del protocolo solicitado
3	No se puede llegar al puerto destino
4	Se necesita aplicar fragmentación pero la bandera correspondiente indica lo contrario
5	La ruta de origen no es correcta
6	No se conoce la red de destino
7	No se conoce el host de destino
8	El host de origen está aislado
9	La dirección de red es inaccesible por razones administrativas
10	El host es inaccesible por razones administrativas
11	No se puede llegar a la red de destino debido al tipo de servicio
12	No se puede llegar al host de destino debido al tipo de servicio

Este tipo de mensajes se generan cuando el tiempo de vida del datagrama a llegado a cero mientras se encontraba en tránsito hacia el host destino (código=0), o porque, habiendo llegado al destino, el tiempo de reensamblado de los diferentes fragmentos expira antes de que lleguen todos los necesarios (código=1).

Los mensajes ICMP de tipo= 12 (problemas de parámetros) se originan por ejemplo cuando existe información inconsistente en alguno de los campos del datagrama, que hace que sea imposible procesar el mismo correctamente, cuando se envían datagramas de tamaño incorrecto o cuando falta algún campo obligatorio.

Por su parte, los mensajes de tipo=5 (mensajes de redirección) se suelen enviar cuando, existiendo dos o más routers diferentes en la misma red, el paquete se envía al router equivocado. En este caso, el router receptor devuelve el datagrama al host origen junto con un mensaje ICMP de redirección, lo que hará que éste actualice su tabla de enrutamiento y envíe el paquete al siguiente router.

**2.1.9 PING.** Es un programa de verificación para conocer el estado de una conexión TCP/IP. El comando PING trabaja enviando un número determinado de paquetes IP a un destino específico dependiendo de la necesidad del usuario, aunque el valor de paquetes predeterminados es de 4. Cada paquete enviado es una solicitud de respuesta, y cada respuesta contiene datos como el tiempo que tardó en ir y volver el paquete, o si este jamás tuvo respuesta. Gracias a esta información obtenida de una forma fácil y rápida, se puede conocer por el resultado del PING, el estado de una enlace, se puede conocer el tiempo que duró en ir y volver el paquete, o posibles causas por las cuales la petición de ping no fue respondida, emitiendo mensajes distintivos mediante los cuales el usuario puede tener al menos una pequeña pista de que factor esta causando el error. El ping lanza un resultado como el siguiente:

Haciendo ping a 192.168.0.3 con 32 bytes de datos:

Respuesta desde 192.168.0.3: bytes=32 tiempo<1m TTL=128

Respuesta desde 192.168.0.3: bytes=32 tiempo<1m TTL=128

Respuesta desde 192.168.0.3: bytes=32 tiempo<1m TTL=128

Respuesta desde 192.168.0.3: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.1:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0

(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 0ms, Máximo = 0ms, Media = 0ms

Donde se muestran datos importantes y fáciles de identificar como la dirección a la que se le está haciendo la petición de respuesta, si la dirección respondió o no, si lo hizo, cuánto tiempo tardó el paquete en ir y volver al emisor del ping, el número

de paquetes enviados, y cuántos fueron recibidos y cuántos perdidos, y el tiempo total de de envío y recibo de todos los paquetes promediado y totalizado.

Los mensajes que envía ping pueden interpretarse de la siguiente manera:

**a. Respuesta desde:** Tanto el cableado como los protocolos y las direcciones IP estan bien configuradas.

**b. Tiempo de espera agotado:** Problema en el cableado entre dos o mas hosts.

**c. Host de destino inaccesible:** Comprobar las direcciones IP y sus respectivas mascararas de red y subred.

**d. Error:** Pueden estar mal instalados los protocolos TCP/IP del Host de origen.

**2.1.10 TTL o Tiempo de Vida.** Es el máximo tiempo que se permite a un paquete propagarse antes de que lo descarte la red y esta dado en segundos. Después de que este tiempo caduca, el paquete puede ser descartado por cualquier elemento de la red.

Este parámetro viene con un valor numérico por defecto, dependiendo del protocolo que se este utilizando en la red bajo la que se esta trabajando, aunque el usuario puede cambiarlo. El objetivo de este ítem es evitar que un mensaje este dando vueltas por una red, congestionándola indefinidamente.

A medida que el paquete atraviesa cada uno de los Routers, este campo disminuye en 1 unidad, cuando el valor de este campo llega a 0, el mensaje es descartado por completo y se envía un mensaje ICMP tipo 11 (Tiempo excedido) para informar al origen acerca de este suceso.

**2.1.11 Latencia.** Es la cantidad de tiempo que demora un paquete en el transito desde su origen hasta su destino. Varios factores pueden influir en el retardo de un paquete, entre los cuales estarían el tamaño del paquete, la congestión de la red (cantidad de usuarios queriendo transmitir al mismo tiempo), la velocidad del enlace, errores en el enlace que se esta utilizando como medio de transmisión, y el tamaño y formato del paquete que se esta enviando.

**2.1.12 Navegador Web.** Un navegador WEB es una aplicación que interpreta código HTML, uno de los tantos códigos utilizados en el contenido de páginas WEB.

Existen algunos menos utilizados y más complejos, pero gracias a los cuales se pueden obtener contenidos mucho más dinámicos e interactivos, entre estos estarían el XML y el SGML. Entre las aplicaciones más comunes capaces de reproducir este tipo de lenguajes se encuentran el Internet Explorer y el Netscape. Si bien estos exploradores son capaces de interpretar muchos lenguajes de los anteriormente mencionados, hay scripts y ficheros propietarios que únicamente pueden ser interpretados mediante el uso de plug-in, entre los más conocidos están el Flash player, el Acrobat Reader, entre otros.

**2.1.13 Redes De Datos.** Las redes de datos se crearon basadas en la necesidad de las empresas del sector privado y estatal, de transportar información electrónica a largas distancias en poco tiempo.

Anteriormente debía transportarse la información en diskettes de un Host a otro, lo cual en una empresa de más de 100 Hosts era muy difícil lograr que cada usuario tuviera la misma información en un momento dado, y de forma actualizada, pues cada modificación que se hiciera del archivo, debía transportarse manualmente Host por Host, causando que los empleados perdieran mucho tiempo en estos aspectos.

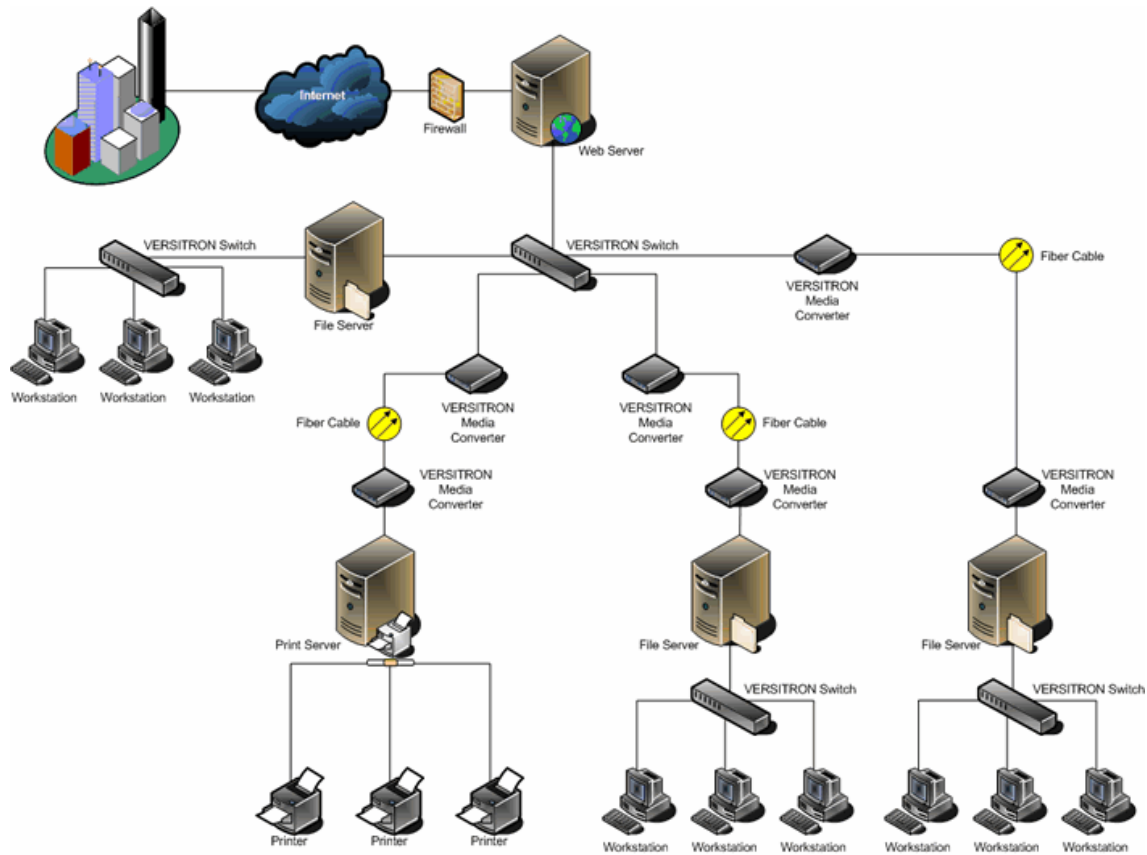
Entonces las empresas necesitaron de medios de comunicación entre Hosts mucho más eficaces, económicos y seguros, centralizando la administración de la red en un sólo punto. La primera solución que vio la luz fue la creación de unos estándares de comunicación llamados LAN (Local Area Network).

Estas redes de área local fueron inicialmente pensadas para ser implementadas y utilizadas a nivel *indoor* en las empresas, para lo cual debían crearse protocolos que estandarizaran la forma en que equipos de diferentes marcas pudieran comunicarse e intercambiar información de una manera eficaz.

Posteriormente se vio la necesidad de mover tráfico ya no sólo de tipo indoor sino también outdoor, es decir, entre empresas, lo cual impulsó la creación de nuevas estandarizaciones como MAN (Metropolitan Area Network) y WAN (Wide Area Network).

Estas dos últimas son interconexiones de varias LAN, es decir interconexiones de varias redes de área local, lo cual actualmente se ha estandarizado para lograr lo que hoy se conoce como INTERNET. En la figura 5 se ilustra una LAN con salida a INTERNET.

Figura. 5. Ilustración de varias redes LAN interconectadas con salida a INTERNET



Fuente: [http://www.versitron.com/images-bb/lan\\_network\\_design\\_2-2.gif](http://www.versitron.com/images-bb/lan_network_design_2-2.gif)

Las LAN pueden estar configuradas de varias formas (Token Ring, Ethernet, FDDI, BUS), aunque actualmente la configuración más utilizada es Ethernet utilizando cable UTP de par trenzado categoría 5e. Aunque cada día está más extendido el uso de la fibra óptica, sobretodo para los BACKBONES (rutas principales de salida) y en menor medida se utiliza el cable coaxial cuyo uso está prácticamente obsoleto.

**2.1.14 Protocolos de red.** Los protocolos de red son un conjunto de reglas o normas gracias a los cuales es posible que hoy día dos o más hosts a través de una red puedan comunicarse, independiente de la marca o el fabricante de los equipos utilizados en el proceso de comunicación. Sin los protocolos, las computadoras receptoras no podrían reconstruir los mensajes tal y como les fueron enviados en forma de bits desde una computadora emisora. Cuando las redes de datos apenas comenzaban a ser populares, uno de los grandes problemas existentes, era el hecho de que equipos de distintos fabricantes no podían comunicarse entre si, ya que no existían protocolos que estandarizaran

bajo un conjunto de reglas global todos los equipos sin importar el fabricante, como ocurre actualmente. Estas reglas hacen posible identificar fallas en una red, identificar si un mensaje ha llegado defectuoso, si un mensaje se ha perdido en el camino, etc. Las organizaciones que regulan este tipo de protocolos y de reglas, son la ANSI (instituto americano de estándares nacionales), la IEEE (instituto de ingenieros eléctricos y electrónicos), la TIA (Asociación de la industria de las telecomunicaciones), la EIA (Asociación de industrias electrónicas) y la ITU (unión internacional de las telecomunicaciones).

## **2.2 MARCO LEGAL O NORMATIVO**

De acuerdo al artículo 75 de la Constitución Política son funciones principales de las Universidades y escuelas politécnicas la investigación, el estudio y el planteamiento de soluciones para los problemas del país, lo que supone incrementar el conocimiento mediante la publicación y difusión de sus resultados en sus medios habituales, para que éste sirva para mejorar la calidad de vida de los ciudadanos mediante su aplicación en el desarrollo de nuevos productos o procesos. La protección legal de los resultados de la investigación así como la libertad de actividades científicas y tecnológicas, están también garantizadas en el artículo 80 de la Constitución.

*DECRETO 600 DE MARZO 14 DE 2003*

*POR MEDIO DEL CUAL SE EXPIDEN NORMAS SOBRE LOS SERVICIOS DE VALOR AGREGADO Y TELEMÁTICOS Y SE REGLAMENTE EL DECRETO-LEY 1900 DE 1990*

*El Presidente de la República de Colombia, en ejercicio de sus facultades constitucionales y legales, especialmente las consagradas en los numerales 11 y 22 del artículo 189 de la Constitución Política, la Ley 72 de 1989, el Decreto-ley 1900 de 1990, la Ley 555 de 2000 y el Decreto 1130 de 1999,*

*DECRETA:*

### *CAPÍTULO I*

#### *Disposiciones generales*

*Artículo 1º. Objeto. El presente decreto reglamenta los servicios de Valor Agregado y Telemáticos y el otorgamiento de las concesiones para su prestación.*

*Artículo 2º. Definiciones.*



*Servicios de Valor Agregado. Son aquellos que utilizan como soporte servicios básicos, telemáticos, de difusión o cualquier otra combinación de estos y con ellos proporcionan la capacidad completa para el envío o intercambio de información, agregando otras facilidades al servicio soporte o satisfaciendo necesidades específicas de telecomunicaciones.*

*Para que el servicio de Valor Agregado se diferencie del servicio básico, es necesario que el usuario de aquél perciba de manera directa alguna facilidad agregada a la simple telecomunicación que le proporcione beneficios de telecomunicaciones adicionales, independientemente de la tecnología o el terminal utilizado o que el operador de servicios de Valor Agregado efectúe procesos lógicos sobre la información que posibiliten una mejora, adición o cambio al contenido de la información, de manera tal que genere un cambio neto de la misma independientemente del terminal utilizado. Este cambio a su vez debe generar un beneficio inmediato y directo, que debe ser percibido por el usuario del servicio.*

*Son servicios soporte de los servicios de Valor Agregado, los servicios básicos, los de difusión, los telemáticos y cualquier combinación de estos, prestados a través de una red de telecomunicaciones.*

*Servicios Telemáticos. Son aquellos servicios que, utilizando como soporte servicios básicos, permiten el intercambio de información entre terminales con protocolos establecidos para sistemas de interconexión abiertos.*

*Red de Valor Agregado. Es una red especializada de telecomunicaciones a través de la cual se prestan al público principalmente servicios Telemáticos y de Valor Agregado. Para que una red sea considerada de Valor Agregado, debe ofrecer características técnicas para la transmisión de la información, que permitan diferenciarla de las redes de Telefonía Pública Básica Conmutada (TPBC). Las redes de Valor Agregado están destinadas a satisfacer necesidades específicas de telecomunicación de usuarios o grupos cerrados de usuarios.*

*Las redes de Valor Agregado podrán ser nacionales o internacionales.*

*Grupo Cerrado de Usuarios: se entiende como el conjunto de usuarios de un operador que tienen las siguientes características:*

- 1. Solamente pueden realizar comunicaciones entre los integrantes del grupo.*
- 2. Su uso no genere contraprestación económica a sus integrantes, y*

*3. Pertencen a la misma persona jurídica o a un grupo de empresas de la misma matriz.*

*Los grupos cerrados de usuarios no podrán conectarse a la red de telecomunicaciones del Estado o a otras redes privadas de telecomunicaciones.*

*LEY 44 DE 1993*

*(febrero 5)*

*Diario Oficial No. 40.740, de 5 de febrero de 1993*

*Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 (VER ANEXO E)*

### **3. METODOLOGÍA**

#### **3.1 ENFOQUE DE LA INVESTIGACIÓN**

Empírico-Analítico: debido al enfoque técnico y práctico del trabajo

#### **3.2 LÍNEA DE INVESTIGACIÓN**

- Línea de investigación institucional: Tecnologías actuales y Sociedad
- Sub-línea de facultad: Sistemas de información y comunicación
- Campo temático del programa: Comunicaciones.

#### **3.3 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN**

Se realizó una Consultoría a ingenieros expertos en esta área de gestión de redes durante las visitas realizadas a las empresas. Esto para lograr la identificación de las necesidades primarias de las empresas en cuanto al software que requieren para poder monitorear una red de forma centralizada, pero a la vez eficazmente y con la menor cantidad de retardos posibles.

#### **3.4 HIPÓTESIS**

El aplicativo a desarrollar permitirá disminuir el tiempo de atención a falla creando una metodología de monitoreo proactiva, además ofrecerá una solución concreta para análisis y disponibilidad de red.

Este proyecto reducirá costos a las empresas de telecomunicaciones, monitoreará los elementos de red de una manera centralizada, necesitará pocos empleados encargados de cada elemento de red, además se desarrollará con software libre, significando un ahorro considerable teniendo en cuenta que las empresas en su gran mayoría pagan exorbitantes sumas de dinero en licencias de estos.

#### **3.5 VARIABLES**

##### **3.5.1. Variables Independientes**

- Tiempo de atención a falla.
- Valor de una licencia.

- Cantidad de dinero ahorrada al monitorear de manera centralizada.
- Cantidad de equipos en la red capaces de manejar los protocolos IP, ICMP y SNMP (Internet Protocol, Internet Control Message Protocol y Simple Network Message Protocol)

### **3.5.2. Variables Dependientes**

- Atención al cliente
- Cuenta de cobro al cliente
- Disminución del Número de empleados, al monitorear de forma centralizada.
- Disponibilidad del servicio prestado al cliente final (Service Level Agreement SLAs).

## **4. PRESENTACIÓN Y ANÁLISIS DE RESULTADOS**

Se realizó el estudio de algunas de las aplicaciones de software de monitoreo más conocidas actualmente, y el resultado se plasma en el anexo D (ver Anexo D), Teniendo en cuenta los precios que poseen cada uno de los aplicativos estudiados en el Anexo D, y la consulta de precios de otras herramientas que brinda el mercado, Se realizó un estudio de costos, acerca de cuanto se podría ahorrar con el proyecto a una empresa de telecomunicaciones y al país, para que sus costos de operación no se incrementen de una forma dramática y el resultado se puede observar en el anexo F.

Se realizaron visitas a empresas de gran influencia en el campo de las telecomunicaciones de Colombia, las cuales son:

- Telefónica Telecom
- BCSC (Banco Caja Social)

Dando como resultado, reflexiones, recomendaciones y observaciones hechas por ingenieros expertos en el tema de gestión de redes, así como opiniones personales de los autores del proyecto, los cuales se citan en el Anexo A.

Además durante estas visitas se elaboraron entrevistas y se diligenció un documento llamado checklist, con el cual se llevo a cabo una investigación organizada y precisa a la hora de investigar puntos clave para el desarrollo del proyecto planteado, los resultados y entrevistas del checklist se documentan en el anexo G.

Teniendo en cuenta estas apreciaciones, el resultado es un aplicativo orientado a Web dividido en 5 secciones:

### **4.1 PÁGINA DE PRESENTACIÓN O INICIO**

Es la página desde la cual el usuario accederá al programa, mediante un nombre de usuario y una contraseña. Allí también aparecerá un mensaje de bienvenida al usuario registrado y el logo del programa.

### **4.2 MONITOREO DE RED**

Se presenta una interfaz gráfica por medio de la cual se obtiene el estado actual de cada uno de los elementos de la red, con datos de interés relacionados con cada elemento que interactúa en la red, como son:

a. Presentación de la información necesaria para contactar al responsable del rendimiento óptimo del elemento (número telefónico, y ubicación de la persona). Estos datos pueden ser actualizados cuando sea necesario y cuantas veces sea necesario para que sea posible brindar una información actualizada al usuario del programa y así este pueda tomar medidas inmediatas y pertinentes ante un fallo o inconveniente en la red.

b. Una lista en la cual son organizadas las direcciones IP de los dispositivos pertenecientes a la red, a la cual se le puede dar click para enviar un ping inmediato y ver su resultado, y su respectivo estado actual, siendo estos estados representados mediante cuadros de tres colores distintos, cada uno con un significado diferente y respetando las siguientes prioridades:

– Rojo: el dispositivo no ha respondido ninguna de las peticiones de ping dentro del tiempo establecido, lo cual puede significar errores de hardware o software.

– Intermitente: el dispositivo ha respondido algunos pings y otros no, lo cual indica un enlace con problemas y con peligro de pasar a color rojo.

– Verde: indica que el enlace está funcionando correctamente y ha respondido a todas las peticiones de ping enviadas bajo un tiempo de espera razonable.

c. La administración es una parte fundamental y se ubica en la zona inferior de la Pantalla de monitoreo. Esta herramienta permite realizar una administración completa de la pantalla de monitoreo, ya que inserta, elimina y modifica los datos mostrados de una manera amigable, por medio de la pantalla.

d. En la parte inferior de nuestra interfaz, también se lleva un historial de eventos que permite conocer el comportamiento del dispositivo dentro de la red, en este llamado Log de eventos se registra durante todo un día los cambios de estado ocurridos en algún elemento de red, si el evento es crítico se genera una alerta mediante pop ups y durante el tiempo que esté crítico el elemento de red despliega un mensaje de alerta por una pantalla publik, y al final del día se guardaran los eventos en históricos para efectos de interés del usuario.

### **4.3 ANÁLISIS DE RED**

Aquí se trabaja bajo el apoyo de MRTG que es una herramienta muy importante a la hora de interactuar con un enrutador y sacar las gráficas del conteo de bits de entrada y salida de nuestro elemento de red, de esta manera el aplicativo arroja los datos pertinentes y los gráfica, para mostrar al cliente de manera amigable las gráficas correspondientes, que serán administradas mediante una consola de administración la cual está ubicada en la parte inferior de la interfaz, esta consola será capaz de escoger los elementos de red, los cuales serán examinados con

MRTG, y también los podrá eliminar para que no sean más analizados con la herramienta. Todos los resultados se guardarán en históricos para que el usuario si lo desea pueda ver un día específico.

#### **4.4 DISPONIBILIDAD**

En esta parte del aplicativo el cliente o el operador puede visualizar el desempeño asociado a cada elemento de red, estos resultados se grafican para el respectivo día, mes y año. El desempeño del elemento se basa en los estados y el tiempo de duración que estuvo normal, intermitente o crítico, basándose como principal herramienta del log de eventos, además algo muy interesante de este modulo es que a medida que hay una caída de un elemento de red, este abre una pantalla de dialogo preguntando quien es el responsable, y dependiendo de quien se escoja, si el prestador del servicio o el cliente, asi mismo se afecta la disponibilidad de este elemento.

#### **4.5 DESEMPEÑO**

Este módulo va a graficar la latencia ligada a cada elemento de red que se esta monitoreando, esto con el fin de facilitar de manera amigable al usuario y al operador de red, el estudio y comportamiento de un elemento de red. Además de de ser una gran herramienta visual, a la hora de realizar informes o presentaciones relacionadas con los comportamientos de la red.

Con esto se concluye que el aplicativo implementado se adecúa a las necesidades de las empresas de telecomunicaciones en Colombia dejando de lado las costosas licencias de programas robustos, ya que todo el aplicativo se encuentra en lenguajes de programación libre, y que después de las visitas realizadas a Telecom y el BCSC, se dan soluciones específicas a necesidades específicas con este proyecto,

Es de gran importancia tener desarrollos ingenieriles en el campo de monitoreo de redes con mano de obra nacional, ya que esto facilita el acondicionamiento de las redes del país a un aplicativo que sea orientado a las mismas y no se tengan que adaptar desarrollos extranjeros, que no fueron concebidos pensando en las redes y empresas colombianas.

## **5. DESARROLLO INGENIERIL**

Para el desarrollo del aplicativo se requirió llevar a cabo las siguientes tareas:

### **5.1 REQUISITOS**

Se analizaron los requisitos del aplicativo como primera etapa para crearlo. Los cuales son:

- Lenguaje de programación de licencia libre para evitar el gasto desmesurado de dinero en licencias.
- Brindar a los clientes un software que brinde soluciones que cumpla sus expectativas.
- Se requiere de la habilidad y experiencia en la ingeniería de gestión por parte de las empresas visitadas, para reconocer los requisitos incompletos, ambiguos o contradictorios.

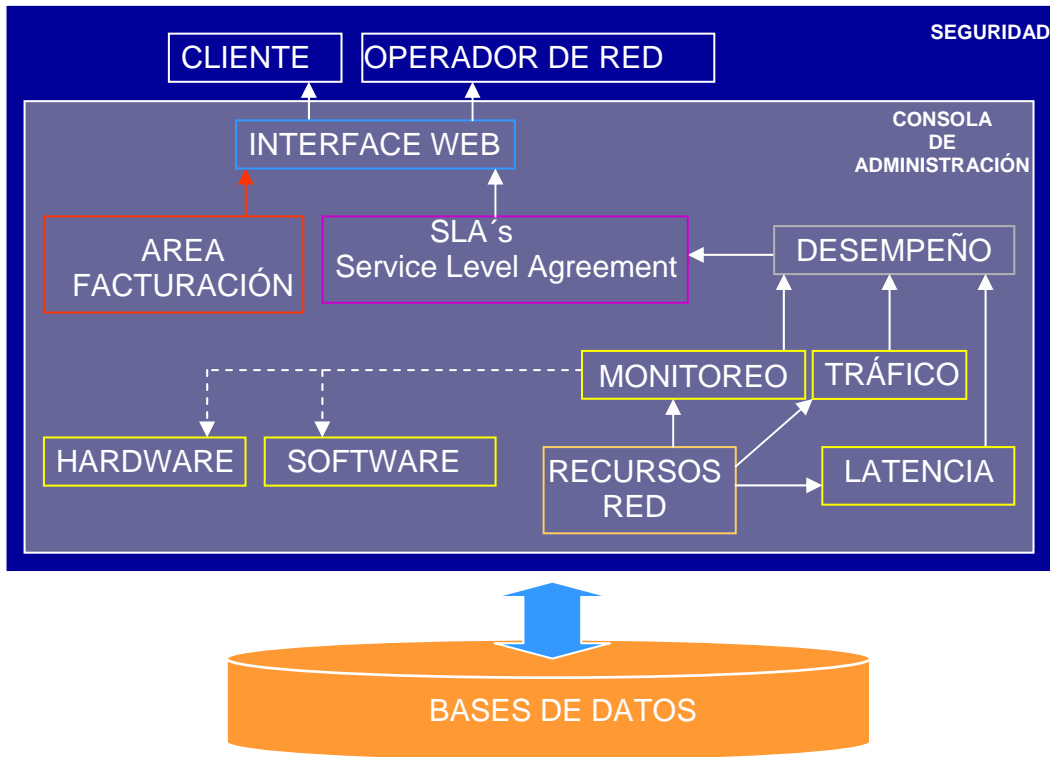
### **5.2 ESPECIFICACIÓN**

Se disminuirá el tiempo de atención a falla, además de descubrir los requerimientos básicos de las empresas de telecomunicaciones creando una metodología de gestión proactiva basada en el siguiente flujo de proceso. Ver figura 6.

En el proceso se ve un módulo principal, que es el de consola de administración con el cual se manejan los recursos de red que a su vez son monitoreados en hardware y software.



Figura 6. Esquema de monitoreo para el aplicativo



Los recursos de red proporcionan los datos de tráfico y latencia que junto con el monitoreo permiten determinar el desempeño de la red mediante una interfaz web que puede ser visualizada por el cliente, operador de red o por el administrador de red, teniendo en cuenta las respectivas restricciones de acceso según perfil de usuario.

Todos estos resultados se almacenan en una base de datos que pueda ser alcanzable incluso por otros sistemas dentro de una organización; tal es el caso del Área de Facturación, que se incluye dentro del gráfico anterior con el objetivo de dar más claridad acerca de la posible interacción que se puede tener entre el sistema propuesto con un sistema de facturación, aclarando que el módulo de facturación no es un objetivo ni alcance de este proyecto.

### 5.3 DISEÑO Y ARQUITECTURA

El aplicativo funciona mediante tres scripts desarrollados en lenguaje batch, que corren mediante el administrador de tareas de Windows así:

- a. Principal: corre cada dos minutos en Background.
- b. MRTG: corre cada cinco minutos en Background.
- c. Remover\_eventos: corre cada 24 horas en Background.

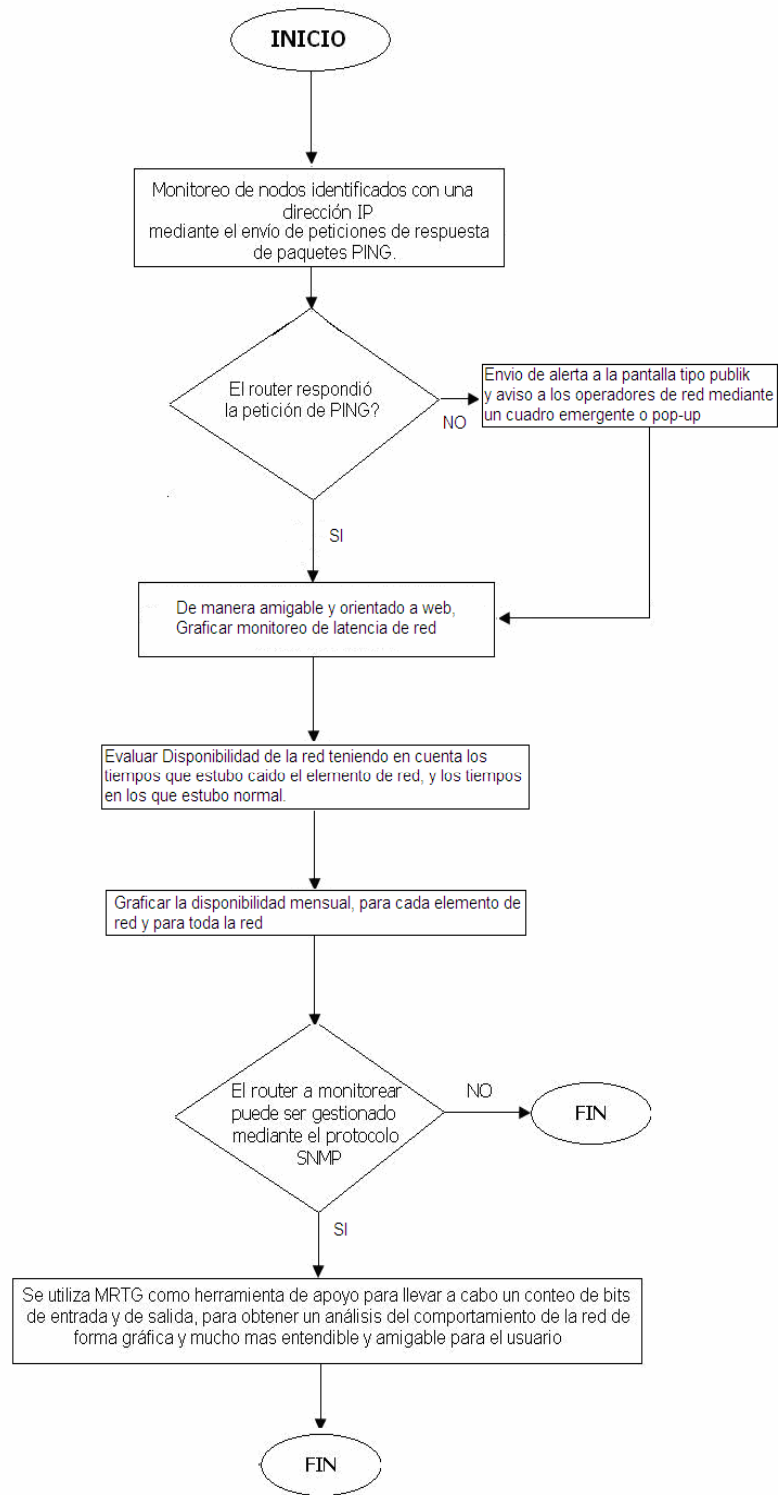
El primer script lanzará 4 pings de 8 bytes de datos al mismo tiempo al pull de direcciones que se escoja por parte del usuario, y el segundo ejecuta otra tarea ligada a crear las gráficas de conteo de bits de entrada y salida de los elementos de red escogidos por el usuario mediante MRTG. De estos resultados se analizan los datos y se muestran orientados a Web de una manera amigable mediante PHP. Del procesamiento de estos datos salen las siguientes interfaces Web:

- Monitoreo: ilustra los estados de red, eventos ocurridos en la misma y la consola de administración, para agregar borrar o modificar los elementos de red a tratar.
- Análisis De Red: da a conocer al usuario las gráficas diarias, mensuales y anuales de conteo de bits de entrada y salida proporcionada por la herramienta MRTG.
- Disponibilidad: aquí se muestra al usuario de manera gráfica la latencia de red y el desempeño obtenido de los eventos para cada elemento de red

Y el tercero guarda los eventos ocurridos en un día en una carpeta llamada historicos, la cual si así lo desea el usuario, se puede acceder mediante la consola de administración.

Para mayor entendimiento se diseñó de manera general el siguiente diagrama de flujo para el aplicativo:

Figura 7. Diagrama de Flujo del funcionamiento del programa.



## 5.4 PRUEBAS

Se realizaron comprobaciones en cuanto a que el software realice correctamente las tareas indicadas en la especificación. Para esto se realizaron pruebas por separado para cada módulo del aplicativo, para luego probarlo de forma integral. Para esto se consiguieron a manera de alquiler 3 enrutadores, los cuales fueron conectados en red para así poner el aplicativo a funcionar. Además se tuvo la suerte de poder probar el aplicativo en una red real como lo es la del BCSC (Banco Caja Social), esto gracias a que el asesor de este proyecto Msc., Ing. HAROLD ALEXANDER PIÑEROS siendo el encargado de dicha red, hizo las gestiones necesarias para esto y así se pudo realizar esta parte tan importante en el desarrollo de este proyecto. Se destaca el hecho que mediante el software que posee el BCSC (HP Openview) el monitoreo se hacia confuso por contar con 364 enlaces, como también la identificación de caídas de nodos y enlaces, pero al realizar esta prueba, este problema se soluciono ya que:

- El aplicativo se comportó de manera excelente a la hora de monitorear los elementos de red en tiempo real, lo cual se puede observar en la figura, aclarando que por exigencia del BCSC no se muestran la IP's por motivos de seguridad y privacidad del banco (ver figura 8).

Figura 8. Monitoreo en tiempo real de la red del BCSC

**Monitoreo de Red**  
Normal ■ Intermittente ■ Crítico ■

Ubicacion	Direccion IP	Estado	Contacto	No.Telefono
Colmena_La_Dorada		■	Fernando Vanegas	968571276
Colmena_Antiguo_Country		■	Bernardo Garcia	2564526
Colmena_Arauca		■	Iris Castellanos	978852970
Colmena_Av_Cero		■	Gladys Torrado	975719354
Colmena_Barranquilla_Ppal		■	Luz Dary Perez	953413442
Colmena_Bquilla_Calle_72		■	Ingrid Molinarez	953457203
Colmena_Bquilla_Calle_92		■	Ingrid Molinarez	953457203
Colmena_Bquilla_Prado		■	Nasly Drago	953565659
Colmena_Bucaramanga_Carrera_33		■	Claudia Arenas	976349908
Colmena_Calle_13		■	Sandra Gomez	3701294
Colmena_Cartagena_Bocagrande		■	Claudia Vivero	956550614
Colmena_Cartagena_Principal		■	Gina Perez	956600038

Nodo	Fecha	Hora	Estado
	01/11/2007	08:24 p.m.	Intermittente
	01/11/2007	07:12 p.m.	Normal
	01/11/2007	07:09 p.m.	Intermittente
	01/11/2007	06:54 p.m.	Normal
	01/11/2007	06:51 p.m.	Intermittente
	01/11/2007	06:42 p.m.	Normal
	01/11/2007	06:39 p.m.	Intermittente
	01/11/2007	06:24 p.m.	Normal
	01/11/2007	06:21 p.m.	Intermittente
	01/11/2007	06:03 p.m.	Normal
	01/11/2007	06:00 p.m.	Intermittente
	01/11/2007	05:27 p.m.	Normal

**Administración**  
Insertar Un Nuevo Elemento De Red

Direccion IP: [ ] [ ] [ ] [ ]

Ubicacion IP: [ ]      Contacto: [ ]      Telefono: [ ]

Nombre: [ ]      Apellido: [ ]

[ Insertar ]    [ Limpiar ]  
[Volver](#)

- El monitoreo de tráfico de entrada y salida de los recursos de red se realizó de manera eficaz al graficar únicamente los elementos de red que se necesitaban, y

con la facilidad de estar indicando el consumo diario, semanal y anual (ver figuras 9, 10,11 y 12).

Figura 9. Monitoreo en tiempo real de trafico para un elemento de red de el BCSC

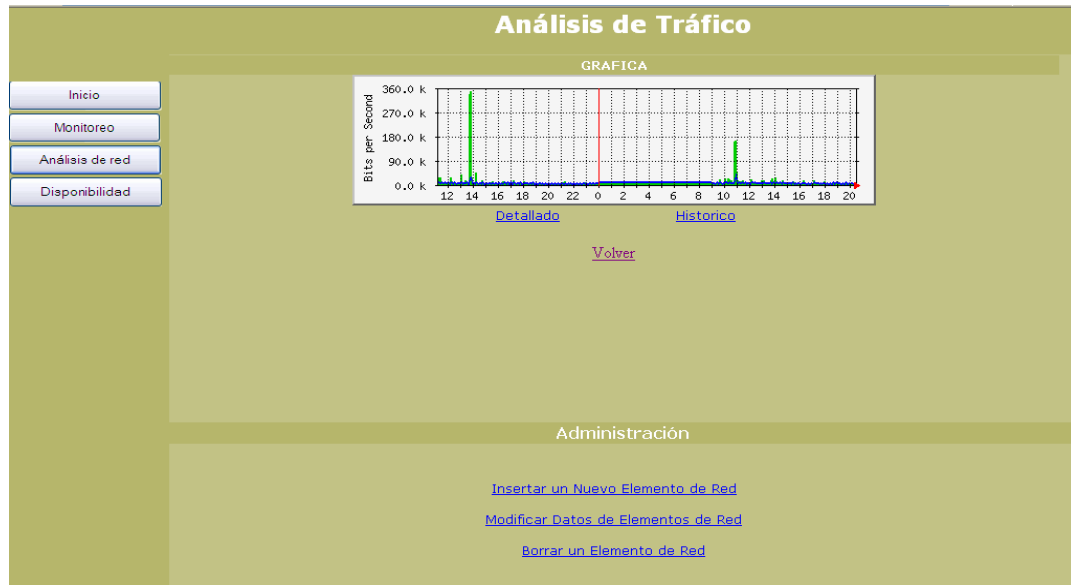


Figura 10. Monitoreo en tiempo real del análisis de trafico Detallado para un elemento de red del BCSC

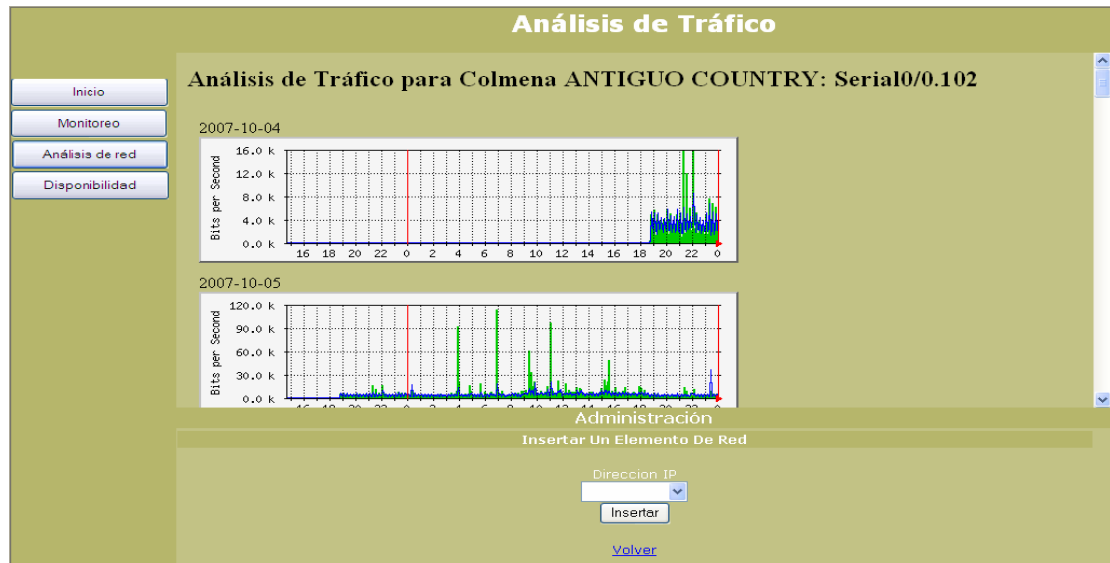


Figura 11. Monitoreo en tiempo real del análisis de tráfico en Históricos para un elemento de red del BCSC 1

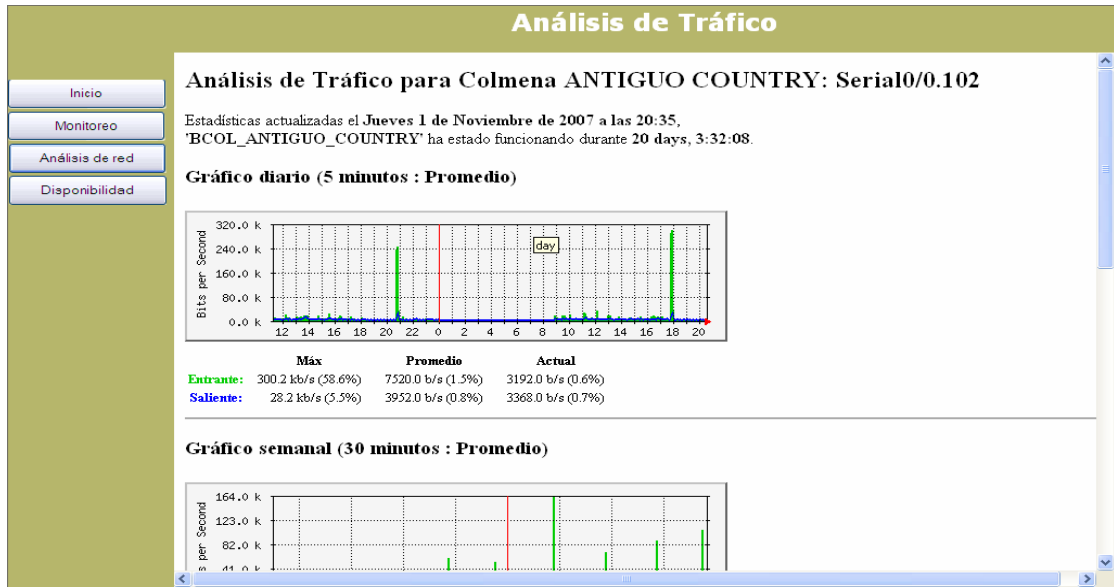
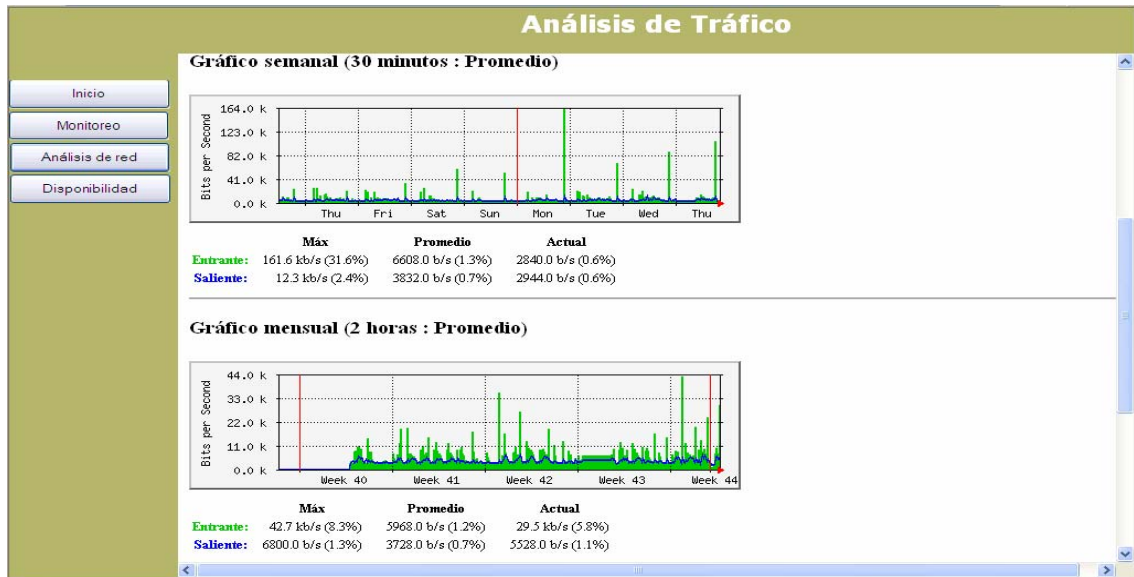


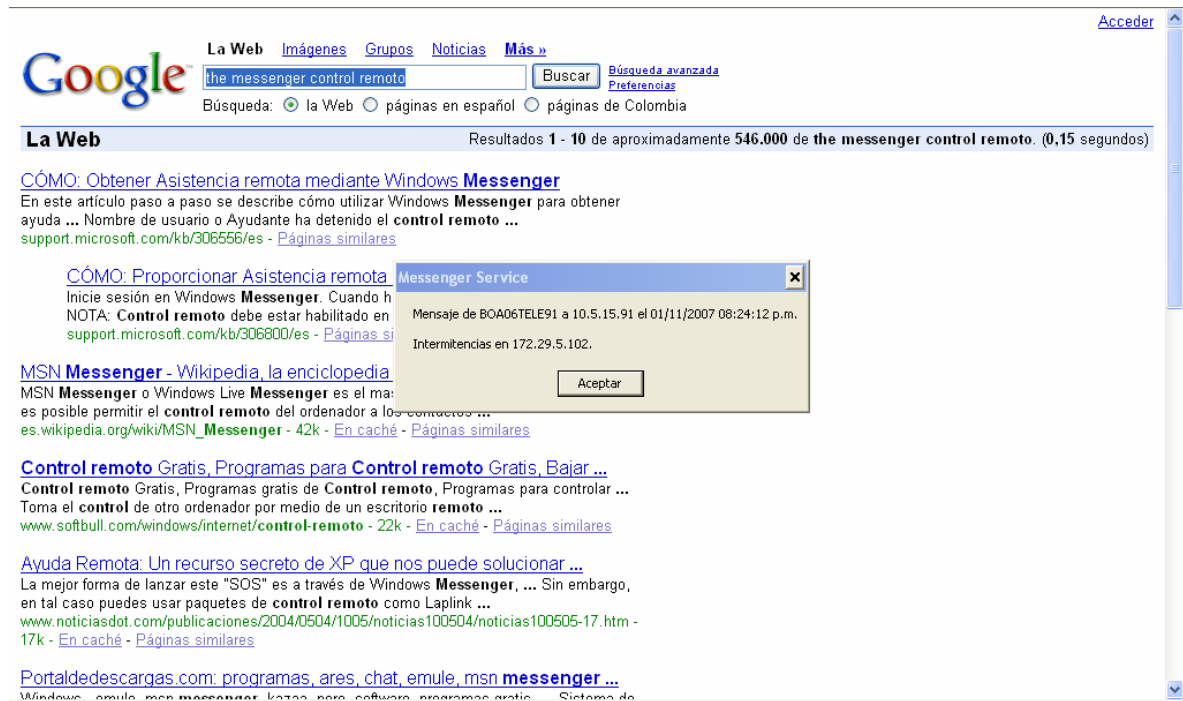
Figura 12. Monitoreo en tiempo real del análisis de tráfico en Históricos para un elemento de red del BCSC 2



- El tiempo de atención a falla se redujo debido a que en la medida que un elemento de red cambiaba su estado a crítico, el aplicativo enviaba unas ventanas emergentes a los computadores personales de los operadores de red, avisando el evento inmediatamente, para que estos tomaran las respectivas decisiones. A

continuación podemos observar uno de esos pop-ups desplegado al computador personal de un operador de red, mientras desarrollaba otras actividades:

Figura 13. Pop-up de aviso critico desplegado a un operador de red del BCSC



Siendo esta prueba un éxito rotundo.

## 5.5 MANUAL DEL USUARIO

### 5.5.1 Requerimientos básicos para el funcionamiento optimo del aplicativo:

Sistema Operativo Windows XP, Windows XP SP1 o Windows XP SP2.

- PHP 5 o superior
- Apache Server 2.059 o superior
- MySQL Server 6.0 o superior
- Navegador de Internet, debe ser: Internet Explorer versión 4 ó superior.
- Perl (Debido a que es requerido por MRTG)
- MRTG-2.15.2

– phpMyAdmin

**5.5.2 Instalación del aplicativo.** Después de cumplir los requerimientos básicos del sistema, se crea una carpeta en:

```
C:\www\mrtg\
```

Y otra en:

```
C:\suggest\bin\
```

Después hay que copiar la carpeta bin incluida en el CD en C:\suggest\bin\, y la carpeta PHP en C:\www\mrtg\.

Ya con los archivos en sus respectivas ubicaciones, hay que decirle al apache donde se encuentran nuestros archivos así que se busca en el httpd.conf del servidor, la parte donde dice:

```
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "C:/Archivos de programa/Apache Group/Apache/htdocs"
```

Y se sustituye la carpeta htdocs del apache por:

```
C:\www\mrtg\
```

Ahora se busca el DirectoryIndex y sale algo como esto:

```
#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
# The index.html.var file (a type-map) is used to deliver content-
# negotiated documents. The MultiViews Option can be used for the
# same purpose, but it is much slower.
#
DirectoryIndex index.html index.html.var
```

Y se procede a cambiar la ultima linea de commando de modo que quede asi:

```
#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
```



# The index.html.var file (a type-map) is used to deliver content-  
 # negotiated documents. The MultiViews Option can be used for the  
 # same purpose, but it is much slower.  
 #

DirectoryIndex frames.php index.html index.htm index.php index.php3 index.php4  
 index.php5 index.phtml index.html.var

AddType application/x-httpd-php .php .php3 .php4 .php5 .phtml

AddType application/x-httpd-php-source .phps

Y se guardan los cambios hechos en este archive.

Ahora mediante phpMyAdmin, hay que crear las siguientes tablas teniendo en cuenta que no se debe cambiar el nombre de la tabla ni los encabezados de cada campo:

Tabla Alberto:

Campo	Tipo	Cotejamiento	Nulo	Extra
ip	varchar(100)	latin1_swedish_ci	No	
estado	varchar(100)	latin1_swedish_ci	No	
Ubicacion	varchar(100)	latin1_swedish_ci	No	
Encargado	varchar(100)	latin1_swedish_ci	No	
Tel	varchar(100)	latin1_swedish_ci	No	

Tabla clientes

Campo	Tipo	Cotejamiento	Nulo	Extra
Id	int(255)		No	
nombre	varchar(16)	latin1_swedish_ci	No	
telefono	varchar(16)	latin1_swedish_ci	No	
Ubicacion	varchar(100)	latin1_swedish_ci	No	
Responsable	varchar(100)	latin1_swedish_ci	No	
Tel	varchar(100)	latin1_swedish_ci	No	

Tabla eventos

Campo	Tipo	Cotejamiento	Nulo	Extra
id	int(255)		No	auto_increment
nodo	varchar(100)	latin1_swedish_ci	No	
fecha	varchar(100)	latin1_swedish_ci	No	

Campo	Tipo	Cotejamiento	Nulo	Extra
hora	varchar(100)	latin1_swedish_ci	No	
estado	varchar(100)	latin1_swedish_ci	No	

Tabla Latencia1:

Campo	Tipo	Cotejamiento	Nulo	Extra
Enrutador	varchar(100)	latin1_swedish_ci	No	
Latencia	text	latin1_swedish_ci	No	

Tabla machado

Campo	Tipo	Cotejamiento	Nulo	Predeterminado	Extra
Id	varchar(100)	latin1_swedish_ci	Sí	NULL	
Ip	varchar(100)	latin1_swedish_ci	No		

Tabla sanchez

Campo	Tipo	Cotejamiento	Nulo	Extra
Num	varchar(100)	latin1_swedish_ci	No	
Direccion	varchar(100)	latin1_swedish_ci	No	
Ubicacion	varchar(100)	latin1_swedish_ci	No	
Responsable	varchar(100)	latin1_swedish_ci	No	
Tel	varchar(100)	latin1_swedish_ci	No	

Tabla tráfico

Campo	Tipo	Cotejamiento	Nulo	Extra
Elemento	varchar(255)	latin1_swedish_ci	No	

Tabla tráfico1

Campo	Tipo	Cotejamiento	Nulo	Extra
Id	int(255)		No	auto_increment
Elemento	varchar(100)	latin1_swedish_ci	No	

Ahora sólo queda crear unas cuantas tareas mediante el tasks de Windows, y para ello se hace lo siguiente:

Clic en inicio → ejecutar → tasks → OK

Aquí se crean 3 tareas:

- C:\Suggest\bin\runhide.exe principal.bat. Que se ejecute todos los dias de la semana cada 3 minutos.
- C:\mrtg-2.15.2\bin\runhide.exe C:\Perl\bin\perl.exe mrtg mrtg.cfg. Cada 5 min
- C:\Suggest\bin\runhide.exe remover\_eventos.bat. Que se ejecute todos los dias alas 11:49 pm.

Y listo el aplicativo quedo instalado en la pagina <http://localhost/gestion.php> para empezar a trabajar con el.

### 5.5.3 Operación De Funciones Básicas

**a. Ingreso al sistema.** Lo primero que se debe hacer es crear los usuarios que vayan a hacer uso de la aplicación.

Luego de estar registrado, el usuario podrá acceder al aplicativo mediante una autenticación en la primera pantalla del programa, y de esta forma se accederá a la página principal de este, que tiene un aspecto como el siguiente (ver Figura 14):

Figura 14. Pantalla de Monitoreo de red

**Monitoreo de Red**  
Normal ■ Intermitente ■ Crítico ■

Dirección IP	Estado	Ubicación	Contacto	No.Telefono
<a href="#">190.66.3.33</a>	■	A	prueba MRTG	1111111
<a href="#">200.118.215.163</a>	■	Cedritos	Carlos Gil	8888888
<a href="#">200.118.62.182</a>	■	Bogota	TV Cable	3456786
<a href="#">67.45.67.90</a>	■	Cali	Henry Pacheco	56788
<a href="#">122.89.34.78</a>	■	Medellin	Jairo Orobio	92814813248
<a href="#">129.123.89.56</a>	■	Cartago	Maria Cruz	73930
<a href="#">23.45.78.90</a>	■	Pitalito	Sonia Braga	739393
<a href="#">127.0.0.0</a>	■	Leticia	Carlos Ferrer	793983
<a href="#">4.4.4.4</a>	■	La Dorada	Diana Tovar	52382392
<a href="#">2.2.2.22</a>	■	caracas	Fredy Sandoval	6666666
<a href="#">23.45.67.78</a>	■	gigtkg	Nombre Apellido	25667
<a href="#">34.67.23.24</a>	■	Libano	Juan Suarez	1000000
<a href="#">69.79.216.1</a>	■	gateway	TV Cable	6500500

Eventos				Administración	
Nodo	Fecha	Hora	Estado		
192.168.1.1	17/10/2007	12:10 a.m.	INTERMITENTE	<a href="#">Insertar un Nuevo Elemento de Red</a>	
200.118.215.163	16/10/2007	11:55 p.m.	DOWN	<a href="#">Modificar Datos de Elementos de Red</a>	
200.118.62.182	16/10/2007	11:55 p.m.	DOWN	<a href="#">Borrar un Elemento de Red</a>	
67.45.67.90	16/10/2007	11:55 p.m.	DOWN		
69.79.216.1	16/10/2007	11:55 p.m.	DOWN		
192.168.1.1	16/10/2007	11:55 p.m.	UP		
67.45.67.90	15/10/2007	10:25 a.m.	UP		
200.118.62.182	15/10/2007	10:24 a.m.	INTERMITENTE		
192.168.1.1	15/10/2007	10:24 a.m.	INTERMITENTE		
192.168.1.1	15/10/2007	10:23 a.m.	UP		
200.118.62.182	15/10/2007	10:21 a.m.	UP		

Esta pantalla se divide en 4 secciones distintas que podrían discriminarse así:

**b. Menú Principal:** En esta sección se presentan 4 opciones, gracias a las cuales se puede elegir la acción que se desea realizar, ya sea monitoreo, análisis de red, disponibilidad, o salir del programa y regresar a la pantalla de inicio. Esta sección tiene el siguiente aspecto:

Figura 15. Menú principal



**c. Monitoreo de red.** Esta pantalla muestra el estado de los enlaces que están siendo monitoreados permanentemente, e indica el estado de cada uno de ellos (disponible, no disponible o intermitente). Los estados se diferencian mediante una convención de colores que identifican cada uno de ellos.

Además de esto, se puede consultar allí información de suma utilidad e importancia acerca del enlace que está siendo monitoreado, como es el encargado del enlace, la forma como se puede contactar a este encargado y la

ubicación del enlace (ver Figura 16).

Figura 16. Enlaces monitoreados y su información correspondiente

Monitoreo de Red				
Normal ■ Intermitente ■ Crítico ■				
Dirección IP	Estado	Ubicación	Contacto	No. Telefono
<a href="#">190.66.3.33</a>	■	A	prueba MRTG	1111111
<a href="#">200.118.215.163</a>	■	Cedritos	Carlos Gil	8888888
<a href="#">200.118.62.182</a>	■	Bogota	TV Cable	3456786
<a href="#">67.45.67.90</a>	■	Cali	Henry Pacheco	56788
<a href="#">122.89.34.78</a>	■	Medellin	Jairo Orobio	92814813248
<a href="#">129.123.89.56</a>	■	Cartago	Maria Cruz	73930
<a href="#">23.45.78.90</a>	■	Pitalito	Sonia Braga	739393
<a href="#">127.0.0.0</a>	■	Leticia	Carlos Ferrer	793983
<a href="#">4.4.4.4</a>	■	La Dorada	Diana Tovar	52382392
<a href="#">2.2.2.22</a>	■	caracas	Fredy Sandoval	6666666
<a href="#">23.45.67.78</a>	■	gjtqj	Nombre Apellido	25667
<a href="#">34.67.23.24</a>	■	Libano	Juan Suarez	1000000
<a href="#">69.79.216.1</a>	■	gateway	TV Cable	6500500

Los enlaces se visualizan teniendo como prioridad aquellos que están en estado CRITICO o no disponible y que aquí se representa con un cuadrado de color rojo, luego, los que se encuentran en estado INTERMITENTE y finalmente aquellos que se encuentran en estado NORMAL o que no están en correcto funcionamiento.

Si se requiere conocer información un poco más detallada de forma inmediata, se puede hacer clic en el enlace que se requiera y de esta forma se hará ping de forma automática al enlace requerido, obteniendo en una nueva pantalla el resultado del ping y sus respectivos detalles.

**d. Eventos.** Aquí se pueden ver los eventos que han ocurrido organizados de acuerdo al momento en que sucedieron. En esta pantalla se puede observar información como la descripción del enlace, la hora del evento, la fecha del evento y el nuevo estado del enlace, que puede ser NORMAL, INTERMITENTE o CRITICO.

Figura 17. Eventos almacenados en una tabla

Eventos			
Nodo	Fecha	Hora	Estado
192.168.1.1	17/10/2007	12:10 a.m.	INTERMITENTE
200.118.215.163	16/10/2007	11:55 p.m.	DOWN
200.118.62.182	16/10/2007	11:55 p.m.	DOWN
67.45.67.90	16/10/2007	11:55 p.m.	DOWN
69.79.216.1	16/10/2007	11:55 p.m.	DOWN
192.168.1.1	16/10/2007	11:55 p.m.	UP
67.45.67.90	15/10/2007	10:25 a.m.	UP
200.118.62.182	15/10/2007	10:24 a.m.	INTERMITENTE
192.168.1.1	15/10/2007	10:24 a.m.	INTERMITENTE
192.168.1.1	15/10/2007	10:23 a.m.	UP
200.118.62.182	15/10/2007	10:21 a.m.	UP

Y además se genera una alerta automáticamente en una pantalla tipo publik acerca de los elementos que se encuentran en estado crítico para dar una mejor asistencia rápida de atención a falla, así como se muestra en la figura 18 y 19:

Figura 18. Alerta generada en el publik

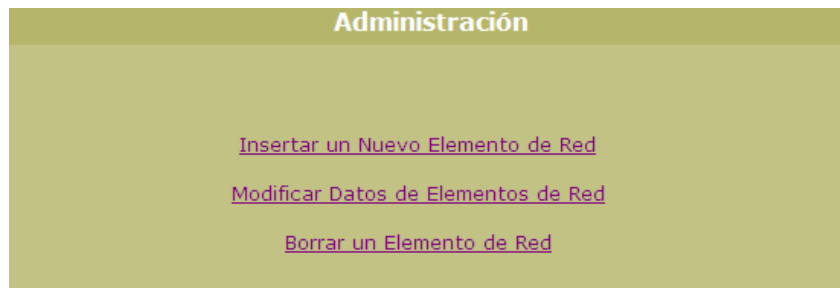


Figura 19. Dirección del nodo en estado de alerta



**e. Administración.** Esta pantalla sólo será visible para los administradores, registrados como tal en la aplicación. Desde aquí se pueden insertar nuevos enlaces que se requieran monitorear, modificar y actualizar datos ya existentes y borrar elementos que ya no son de utilidad. La ventana de administración tiene la siguiente forma:

Figura 20. Menú de la consola de administración del programa



Como se puede observar, cada opción se encuentra en forma de link y cada una dirigirá al usuario a una ventana nueva. A continuación se describirá cada una de las tres opciones que se muestran en la ventana de administración.

**f. Insertar nuevo elemento de red.** En esta opción ventana el usuario puede crear nuevos enlaces, llenando la información requerida en cada una de las casillas. Se deben suministrar datos como la Dirección IP, la Ubicación IP, el nombre y el apellido del contacto o encargado del enlace, y finalmente el teléfono de este último y se ve como en la Figura 21.

Figura 21. Pantalla de inserción de un nuevo elemento o enlace a ser monitoreado

Administración

Insertar Un Nuevo Elemento De Red

Dirección IP

Ubicación IP

Contacto

Telefono

Nombre

Apellido

Insertar

Limpiar

[Volver](#)

Si los datos no son correctos y se desea borrar una o mas casillas, se selecciona la opción limpiar, mediante la cual todas las casillas se restaurarán y quedarán en blanco nuevamente. Si la información es correcta, se selecciona la opción insertar registro, mediante la cual los datos serán almacenados, y el nuevo enlace estará listo para ser monitoreado por la aplicación. Una vez se elija la opción insertar, se obtendrá la siguiente pantalla:

Figura 22. Confirmación de inserción y configuración de nuevo elemento a monitorear

Administración

Elemento de Red Insertado

[Desea insertar un nuevo Elemento de Red](#)

[Regresar a Opciones](#)

Finalmente se despliega un menú que permite elegir entre insertar más nodos, o regresar a la página inicial de administración.

**g. Modificar datos de elementos de red.** Cuando se elige esta opción en la página inicial de administración, se le brinda al usuario la opción de elegir el elemento o enlace cuya información desea modificar.



Posteriormente se le da la opción al usuario de modificar la IP, la ubicación, el nombre y el teléfono del encargado, del enlace cuya información se desea modificar. Esta pantalla tiene un aspecto como el que se muestra en la siguiente figura:

Figura 23. Pantalla de Modificación información acerca de elementos de red

Administración

Modificación Datos de Elementos de Red

172.29.1.226

Ubicacion      Contacto      No. Telefonico

Colmena\_Ced      Sigifredo Quintero      3325

Modificar

[Volver](#)

**h. Borrar un elemento de red.** En esta opción se puede elegir el elemento o enlace que se desea eliminar de aquellos que ya están siendo monitoreados, y se selecciona la opción borrar, lo cual borra el registro de la página principal de monitoreo (ver Figura 24).

Figura 24. Pantalla de eliminación de un elemento de red o enlace

Administración

Borrar un Elemeto De Red

Direccion IP

23.45.78.90

Borrar

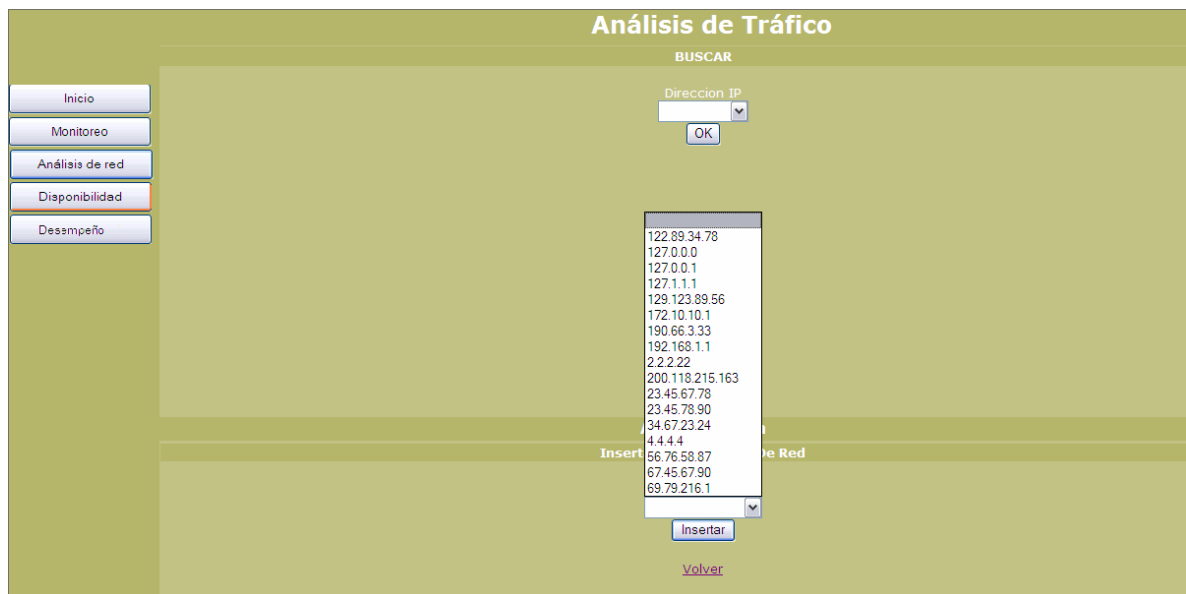
[Volver](#)

## i. Análisis de tráfico

En esta se tiene 2 secciones:

- Administración. En esta sección se puede escoger insertar un nuevo elemento de red ya previamente insertado en el monitoreo principal, para analizar el conteo pertinente de bits de entrada y salida con MRTG (ver figura 25), o borrar un elemento de red cuando no se desee analizar mas este nodo mediante MRTG.

Figura 25. Pantalla de inserción de un elemento de red o enlace para el análisis de tráfico



- Buscar. En esta se puede obtener un análisis del tráfico mediante el conteo de bits de entrada y de salida de un enlace previamente insertado en la consola de administración de análisis de tráfico.

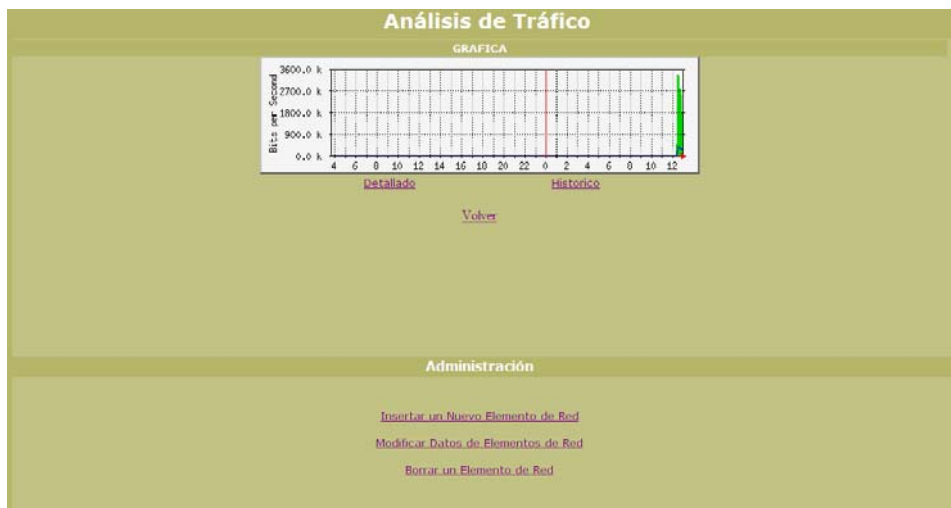
Se elige la dirección IP del enlace del cual se quiere tener una descripción gráfica de su tráfico, y se selecciona OK. Esta es la pantalla de selección del enlace:

Figura 26. Pantalla de análisis de tráfico



Después de seleccionado el enlace, se obtendrá una gráfica con la ayuda de MRTG, como la que se observa a continuación, que muestra los bits por segundo manejados durante instantes de tiempo determinados:

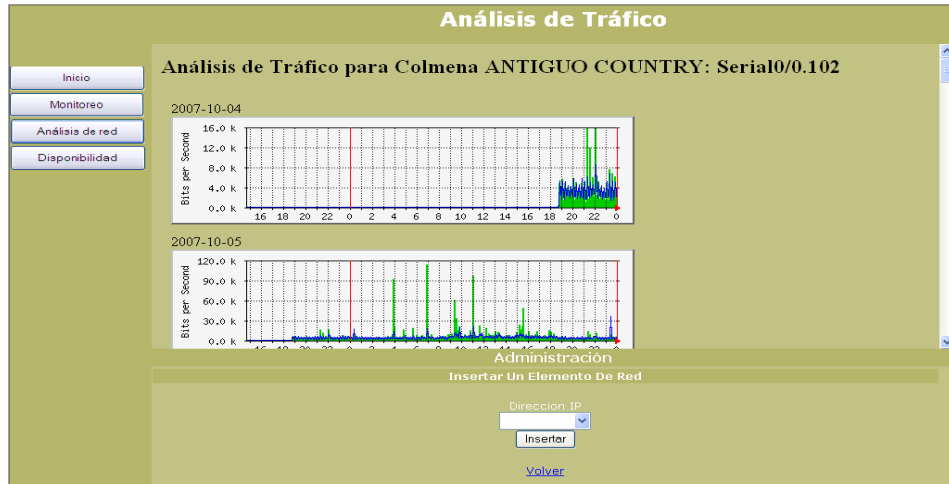
Figura 27. Gráfica de análisis de tráfico sobre el nodo elegido por el usuario en la pantalla anterior.



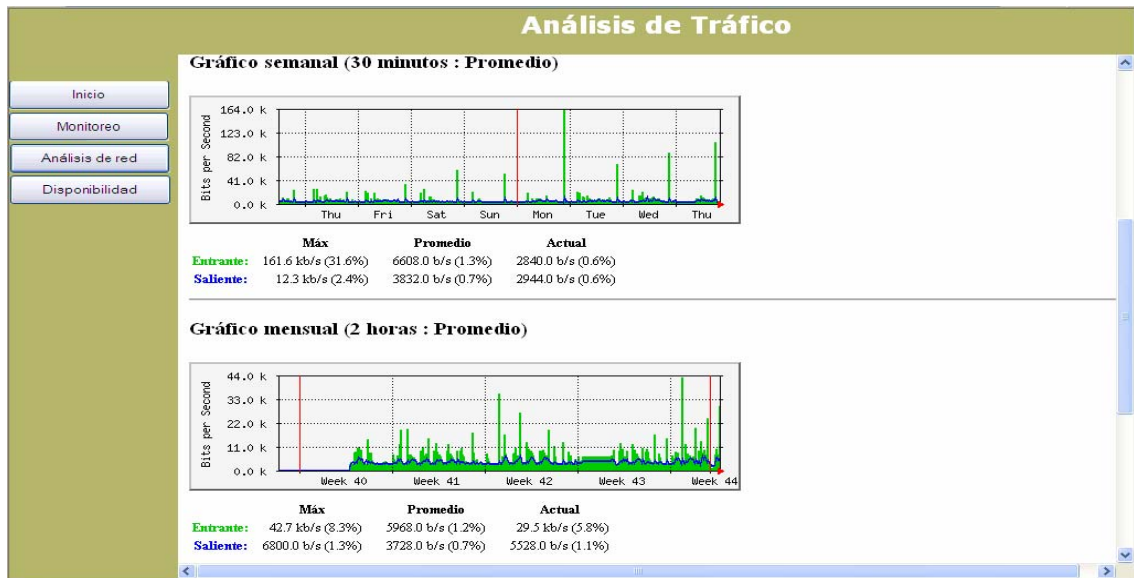
Después se tienen 2 opciones las cuales son:

- Detallado. Esta opción lleva a una pantalla, la cual ofrece el conteo de entrada y salida de bits, ocurrido para cada puerto que posea el router, ya sea serial o ethernet. Para mayor claridad se muestra en la siguiente grafica:

Figura 28. Gráfica Detallada de análisis de tráfico sobre el nodo elegido por el usuario.

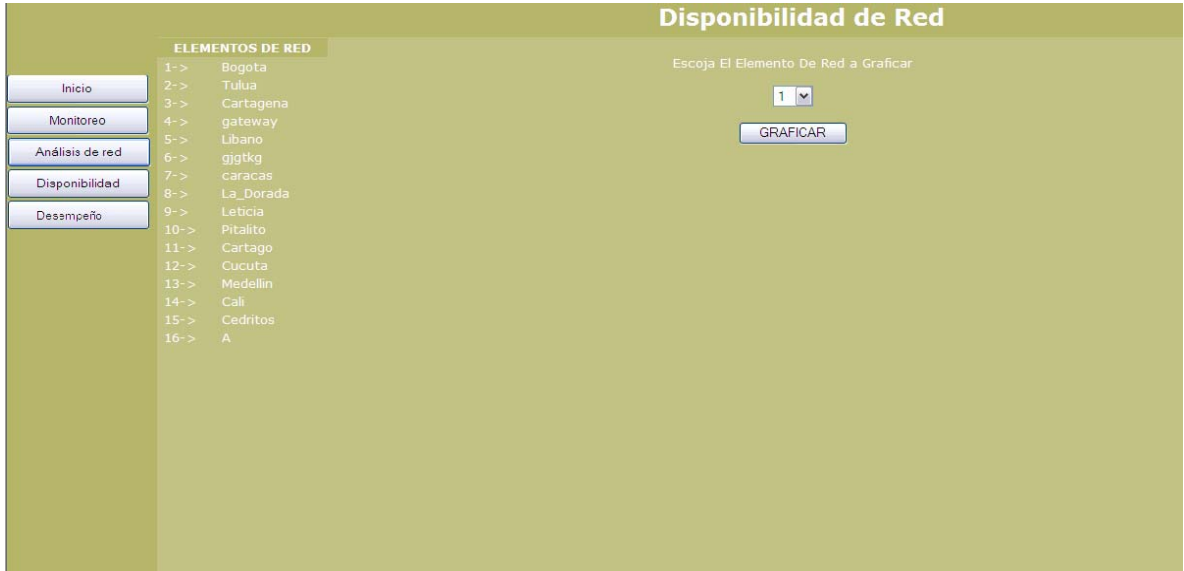


– Históricos. Aquí tenemos otras gráficas de conteo de entrada y salida de bits, pero esta vez se tienen para el día, semana, mes y año, como se tiene en la siguiente figura como ejemplo:



**j. Disponibilidad.** La pantalla principal de Disponibilidad de red tiene la siguiente forma:

Figura 29. Pantalla principal de disponibilidad de red



En esta página se le da la opción al usuario de escoger el nodo cuya disponibilidad se quiere monitorear. Una vez elegido el nodo, se despliega la gráfica de disponibilidad de ese enlace tal y como se muestra en la figura 30.

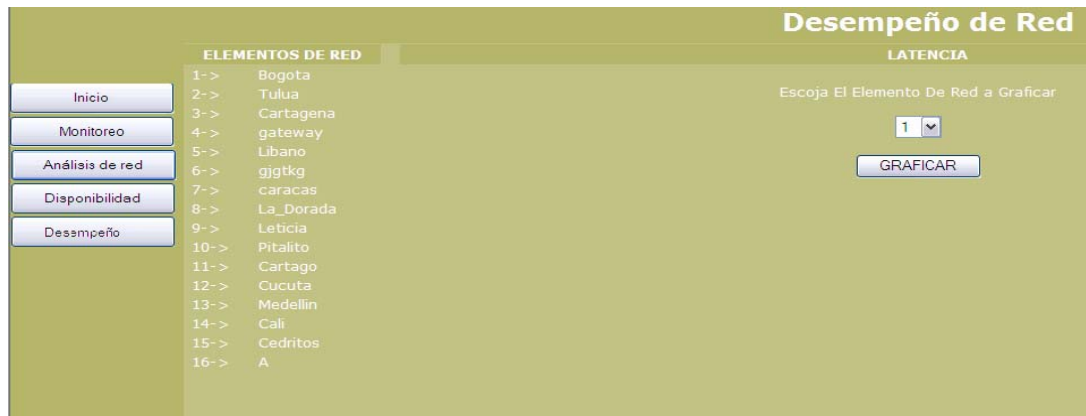
Figura 30. Grafica de desempeño de un enlace determinado



En esta gráfica el usuario puede observar la disponibilidad de la red a los diferentes días y meses, la cual depende de los instantes de tiempo, en los que el elemento de red estuvo Crítico, Intermitente o Normal.

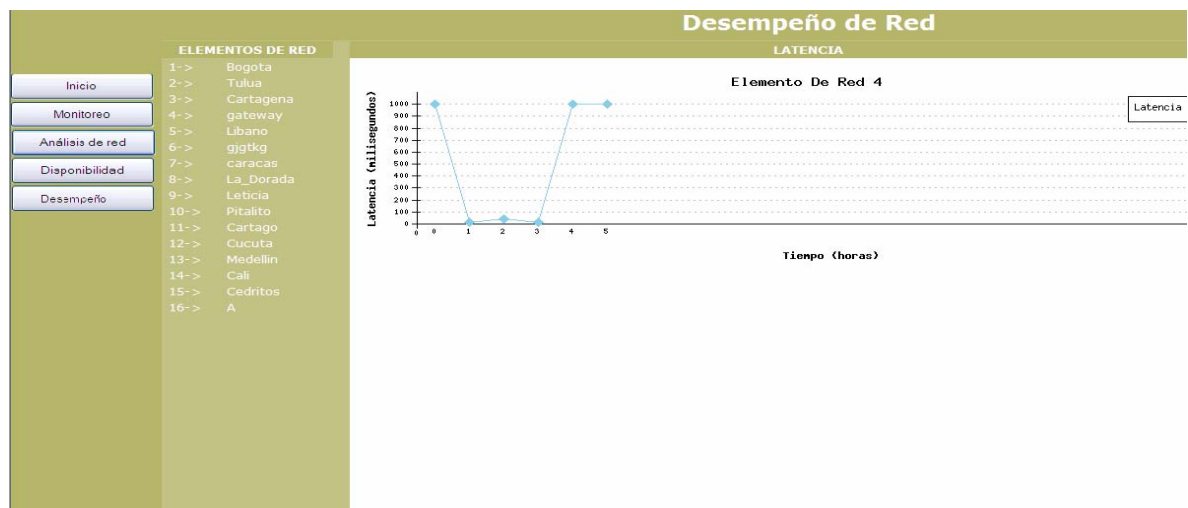
**k. Desempeño.** La pantalla principal de Desempeño de red tiene la siguiente forma:

Figura 31. Pantalla principal de disponibilidad de red



En esta página se le da la opción al usuario de escoger el nodo cuya Latencia se quiere monitorear. Una vez elegido el nodo, se despliega la gráfica de latencia para diferentes instantes de tiempo de ese enlace, tal y como se muestra en la figura 32.

Figura 32. Gráfica de latencia de un enlace elegido por el usuario



En esta gráfica el usuario puede observar la latencia de la red para el elemento de red que haya elegido, a las diferentes horas del día.

Y con esto se concluye con este manual de usuario el cual ilustra el funcionamiento básico del aplicativo.

## 6. CONCLUSIONES

- El tiempo de atención a falla puede disminuirse ostensiblemente mediante generación de alertas como pop-ups, durante la aparición de un evento crítico (que afecte el funcionamiento de un enlace). Para hacer la alerta aun más llamativa y sugerente para el usuario, puede utilizarse una herramienta una pantalla tipo Publik, la cual despliega un mensaje de alerta advirtiendo sobre el elemento de red que se encuentre en estado crítico.
- La accesibilidad de un programa de monitoreo puede mejorarse infinitamente haciéndolo asequible desde cualquier parte del mundo, lo cual se logra orientando la aplicación a Web.
- Una interfaz gráfica y amable con el usuario, logra que este cuente con facilidades de administración para el ingreso, borrado, y modificación de elementos de red desde cualquier host que tenga acceso al servidor donde se encuentra el programa, ahorrándole tiempo al usuario en procedimientos rutinarios.
- Los costos que las empresas de telecomunicaciones deben pagar al adquirir un aplicativo de monitoreo puede verse reducido de forma considerable al utilizarse software de licencia libre en la creación de este aplicativo.
- Mediante las pruebas realizadas en el BCSC (Banco Caja Social) se concluye que el aplicativo desarrollado disminuyo el tiempo de atención a falla, esto gracias a la solución planteada por listas, y a las ventanas emergentes pop-ups a los ingenieros encargados de estos nodos.
- En los checklist tomados a las empresas visitadas se observa que las redes como Telecom no están unificadas, teniendo que tener demasiados aplicativos, incrementando los gastos de operación, que a su vez se ve reflejado en la factura de los clientes.

## 7. RECOMENDACIONES

Una empresa de telecomunicaciones debe adquirir sus elementos de red de tal manera que estos elementos utilicen unos protocolos de comunicación estándar, además de contar con la capacidad de utilizar protocolo IP, los equipos antiguos deben poder también ser identificados y manejados bajo protocolo IP, ya que existen debilidades en aspectos como la falta estandarización de los protocolos y líneas de comando de los diferentes productos de hardware de telecomunicaciones existentes en el mercado, causando que las empresas deban contratar personal y capacitarlo para que este sólo pueda empezar a producir resultados después de seis meses o un año de poner en práctica la preparación. La recomendación que se ofrece a las empresas es tener desarrollos ingenieriles en el campo de monitoreo de redes con mano de obra nacional, ya que esto facilita el acondicionamiento de las redes del país a un aplicativo que sea orientado a las mismas y no se tenga que adaptar desarrollos extranjeros, que no se desarrollaron pensando en las redes y empresas colombianas.

Como propuesta a mediano y largo plazo se tiene la expansión del software hacia al menos otra capa del modelo TMN, para hacerlo más integral y de esta forma las empresas no necesitarían adquirir varios paquetes de software de varios fabricantes distintos, sino que adquirirían un paquete integral de un sólo fabricante y solo necesitarían adquirir la licencia de un programa.

Una recomendación importante a tener en cuenta es que las empresas de telecomunicaciones deberían emplear ingenieros para investigación en el campo de la gestión de redes, ya que si logran adecuar diseños propios a sus redes no tendrían que pagar costosas sumas de dinero en licencias y soporte técnico, lo cual conllevaría e influiría en que los precios de los servicios prestados por la empresas proveedoras de servicios de telecomunicaciones se redujeran y beneficiaran en gran medida al usuario final.



## **BIBLIOGRAFÍA**

ANDREWS S. TANENBAUM, Redes de Computadoras, 2003 Pearson Educacion de México S.A, Cuarta Edicion.

BEHROUZ FOROUZAN, Data Communications and Networking, 2007 McGraw-Hill Higher Education, cuarta edicion.

BEHROUZ FOROUZAN, TCP/IP Protocol Suite, 2006 McGraw-Hill Higher Education, tercera edición.

CISCO SYSTEMS, Cisco Networking Academy program CCNA 1 y 2, 2004 Person Education S.A, tercera edición.

CISCO SYSTEMS, Cisco Networking Academy program CCNA 3 y 4, 2004 Person Education S.A, tercera edición.

HUGH E. WILLIAMS, DAVID LANE, Web Database Applications, Publisher: O'Reilly, First Edition March 2002, ISBN: 0-596-00041-3, 582 pages

KLINE KEVIN con KLINE DANIEL, SQL in a Nutshell, Printed in the United States of America, Published by O'Reilly & Associates, Inc., 101 Morris Street, Sebastopol, CA 95472.

## **ANEXOS**

## **ANEXO A REPORTE DE VISITA A EMPRESAS**

A continuación se da el resultado de las visitas realizadas a empresas líderes en telecomunicaciones mediante reflexiones, recomendaciones y observaciones realizadas por ingenieros expertos en el tema de gestión de redes, así como opiniones personales de los autores del proyecto y se plasma en el orden en que se visitó cada empresa:

- Telecom: La gestión de red se encuentra ubicada en el segundo piso de la conocida “Pirámide De Telecom” inspirada en el modelo TMN.

Desde este punto se realiza el monitoreo centralizado de la amplia red de Telefónica Telecom, dividiendo este monitoreo en grupos específicos y especializados, entre los cuales se tiene:

- Monitoreo de elementos de red que se encuentran bajo IP's,
- Monitoreo la Red de telefonía IP.
- Monitoreo de la red eléctrica.
- Monitoreo de la red de banda ancha.
- Monitoreo de la red de telefonía pública conmutada.

Respecto a los ingenieros encargados de monitorear los elementos de red que se encuentran bajo IP, los autores observaron que trabajan en la elaboración de scripts que según el ing. Javier Santiago (que fue el guía en dicha visita), son scripts de programas de costosas licencias, y que tienen que estar adecuando constantemente a la red.

Otro de los aspectos relevantes es que los ingenieros encargados, deben realizar muchas tareas de manera manual, ya que la interfaz gráfica no se encuentra desarrollada, o en su defecto no es lo suficientemente eficiente.

Según el ing. Javier Santiago hoy en día en las redes de Telefónica Telecom, se están adquiriendo y adaptando equipos de toda índole, para que trabajen bajo protocolo IP y así sean capaces de ser monitoreados de manera centralizada y desde Internet, y con esto ahorrar en la contratación de empleados, ya que en la antigua Telecom se debía tener por cada estación o nodo un encargado que monitoreara el elemento de manera personal.

En los computadores utilizados para el monitoreo de red en Telefónica Telecom,

se observó una gran diversidad de sistemas de gestión, y los autores observaron los siguientes pantallazos de estos, en su respectivo funcionamiento habitual:

Figura. Pantallazo de sistema de gestión utilizado en Telecom

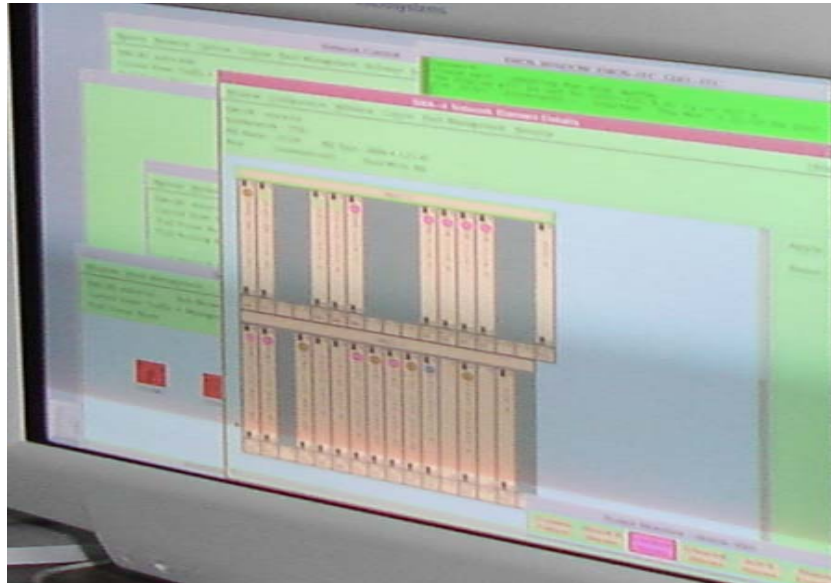
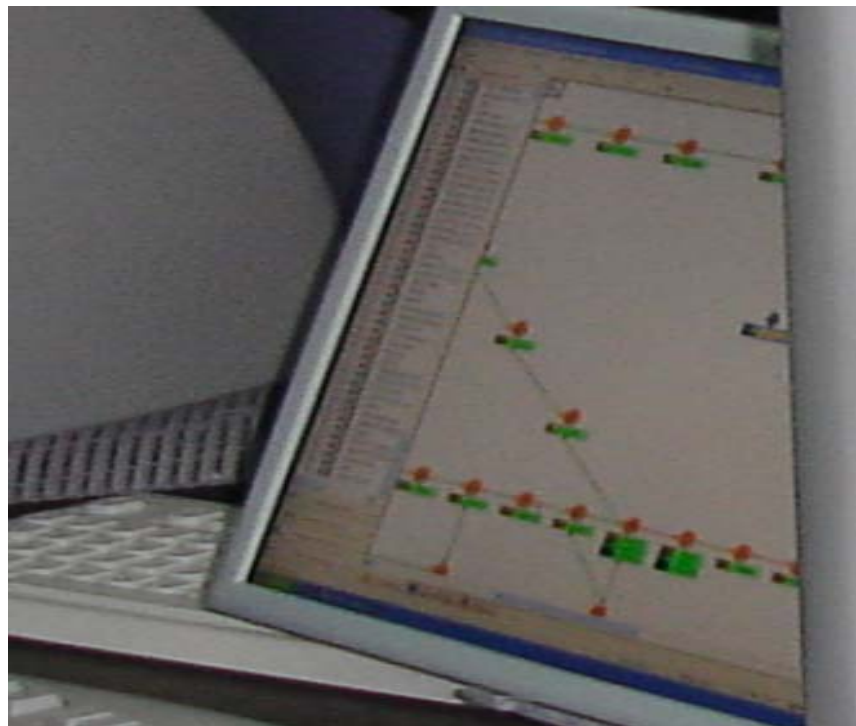


Figura. Pantallazo de otro de los sistemas de gestión utilizado en Telecom



Otro de los aspectos importantes que los autores observaron, fue la manera como se realizaba el monitoreo a manera grupal, la cual se hacia mediante las siguientes pantallas gigantes :

Figura. Pantallas gigantes utilizadas en Telecom



Estas pantallas gigantes solo se encienden cuando llega el momento en que algún político, cliente, o personaje importante realice una visita a este sitio, dejándolo solo para protocolo y no de manera de ayuda para el monitoreo por parte de los ingenieros, ya que según el ingeniero guía de la visita, estas pantallas generan un gasto en dinero considerable, ya que la manera que se proyecta la información en ellas, es mediante un proyector, el cual posee un reflector bastante costoso y que su tiempo de vida es aproximadamente un mes y medio, teniendo así que comprarlo de una manera seguida.

- BCSC (Banco Caja Social): se encuentra ubicado en la calle 59 con carrera 13 en el sexto piso del edificio del BCSC. Desde este punto se realiza el monitoreo centralizado de la red de datos que esta compuesta por enlaces de banda ancha hacia las sucursales y a cajeros electrónicos.

Este monitoreo se realiza mediante la herramienta conocida en el mercado como HP openview NNM mediante la cual se visualizan estado de los nodos y enlaces que componen la red de datos del BCSC. El aplicativo HP Openview NNM lo publican sobre una pantalla de plasma de aproximadamente 42 pulgadas en la cual se tiene desplegada la red sobre un mapa grande. Destacando el hecho que por contar con 364 enlaces se hace confusa la identificación de caídas de nodos y enlaces. El monitoreo que se hace mediante la pantalla de plasma por seguridad del banco no se le permitio a los autores tomar fotos, entonces, para mejor entendimiento se muestra algo parecido en la siguiente figura:

Figura. Ejemplo de pantalla de plasma utilizada en el BCSC



Cabe resaltar que al preguntar a un ingeniero que esta a cargo del monitoreo y gestión de la red, si dentro de esta amplia red existe algún equipo que no maneje el protocolo IP, y la respuesta a esto fue que todos los equipos manejan este protocolo, y con esto son capaces de ser monitoreados de una manera centralizada. Otra pregunta fue que si le gustaba la manera como HP openview mostraba en un mapa los enlaces que estaban normal o critico, y la respuesta fue que no era funcional a la hora de observar cuales enlaces estaban críticos, ya que era difícil con tantos enlaces saber cual estaba caído y cual no teniendo así que mirar con detenimiento durante mucho tiempo hasta descubrir esto.

## **ANEXO B ESTADO DEL ARTE**

Teniendo en cuenta los interrogantes proferidos por el jurado el día 20 de octubre de 2006, se incluyen las siguientes observaciones:

### **ESTADO DEL ARTE**

Se realizó una visita a una empresa de telecomunicaciones y se consultó con ingenieros de amplia experiencia en el tema; se identificaron las causas fundamentales por las que es necesaria la gestión de red son:

1- Los sistemas de información cada vez juegan un papel más preponderante en la estructura de control y gestión de las empresas de telecomunicaciones en Colombia.

2- La información que manejan las empresas en Colombia tiende a ser cada día mayor y a estar más dispersa.

3-En la mayoría de los sistemas de redes existen productos y servicios de múltiples fabricantes los cuales incorporan diversas tecnologías que provocan un constante aumento de la complejidad de los recursos gestionados tanto en cantidad como en heterogeneidad.

Al detectar las causas fundamentales de necesitar gestionar las redes, se ratifica que el adecuado empleo de las tecnologías de Gestión de Red nos permite:

1-Mejorar la eficiencia, la disponibilidad y el rendimiento de las redes.

2-Aumentar la relación calidad/costo en el diseño de las redes a partir de una mejor selección del equipamiento y de las herramientas a emplear en función de la Gestión de Red.

3-Disminuir los costos de funcionamiento de las redes, aumentando la satisfacción de los usuarios y reduciendo la necesidad de recursos humanos en la operación de la red.

Otro aspecto que se trató a manera de consulta (con los ingenieros contactados y que están asociados en esta área de gestión de red) son los principales aspectos asociados a la Gestión y Planificación de Redes y Servicios llegando a las siguientes conclusiones:

1-Gran variedad de problemas tecnológicos, ligados a las tecnologías que se necesitan gestionar y a la realización de la propia gestión.

2-Gran saturación de productos comerciales en un marco de alta competitividad, pese a normas internacionales que buscan interoperabilidad, lo que hace necesario mantener una dirección correcta y no confundirse.

3-Necesidad de aplicar coordinadamente gran cantidad de conocimiento para gestionar una red dado el constante aumento de la complejidad de los recursos a gestionar tanto en cantidad como en heterogeneidad. El éxito se logra con una formación sólida y permanente actualización.

4-Normalmente la planificación de una red no parte de cero sino de un conjunto de sistemas existentes (costosos) los cuales hay que interconectar, lo que hace que se deba trabajar con medios y técnicas prefijadas obligando a los nuevos productos a convivir con los anteriores y en su conjunto mantenerlos y gestionarlos.

5-Para gestionar una red no es necesario ser un experto en ella, sino ser capaz de abstraerse para observar a la misma y a sus servicios de telecomunicación como “objetos” que necesitan ser gestionados (no entrando en los detalles de los mismos) y modelarlos de acuerdo a los modelos de información existentes y a nuevos que puedan definirse.

Adicionalmente, se ha podido observar que en el mercado existen factores que influyen notoriamente en la unificación de sistemas de gestión de red tales como:

\*Heterogeneidad en la tecnología de las redes

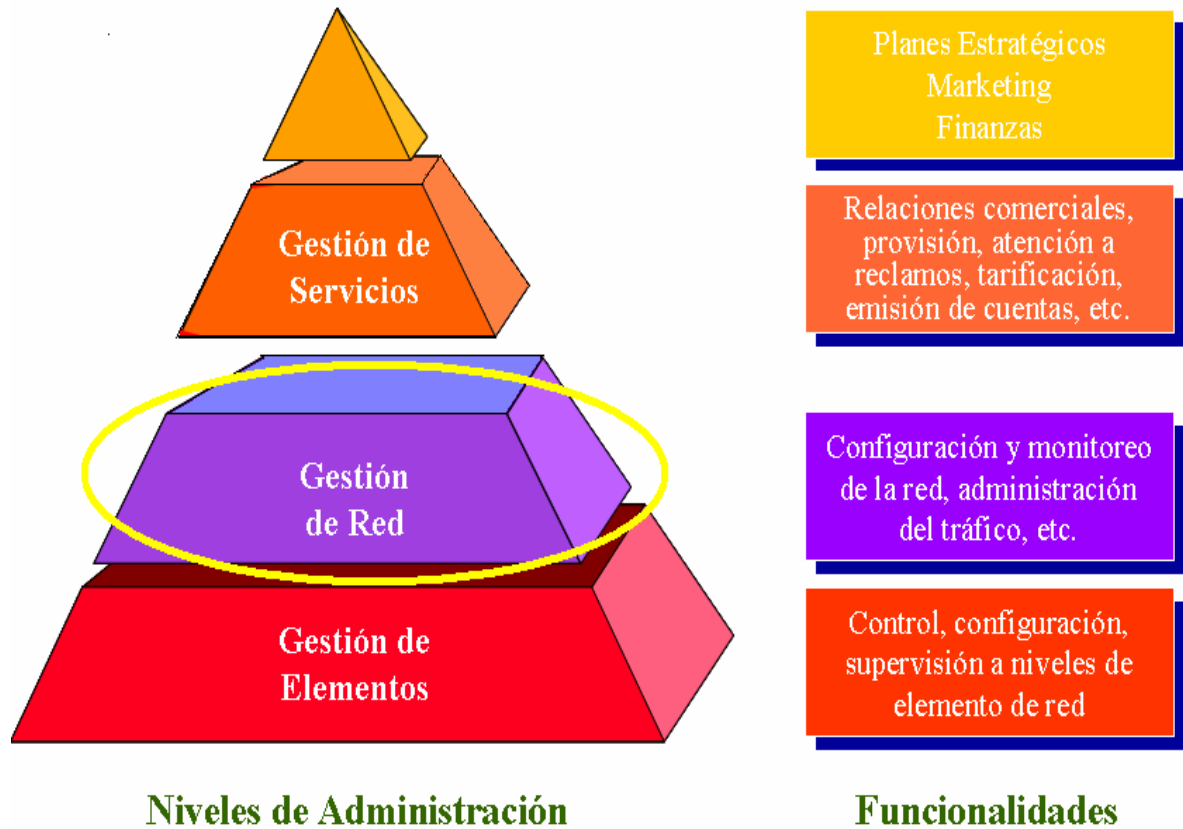
\*Creciente liberalización y competencia entre las empresas operadoras.

\*Necesidad de incorporar a las redes existentes nuevos servicios de alta calidad para lo cual los operadores de redes tendrán que reorganizar sus recursos en base a métodos de gestión y control que tengan el menor impacto económico posible.

La tendencia, para atender los factores expuestos anteriormente, es generar aplicaciones y soluciones que estén de acuerdo a las características y lineamientos que estipula la arquitectura de TMN. Ver la siguiente figura Arquitectura TMN.



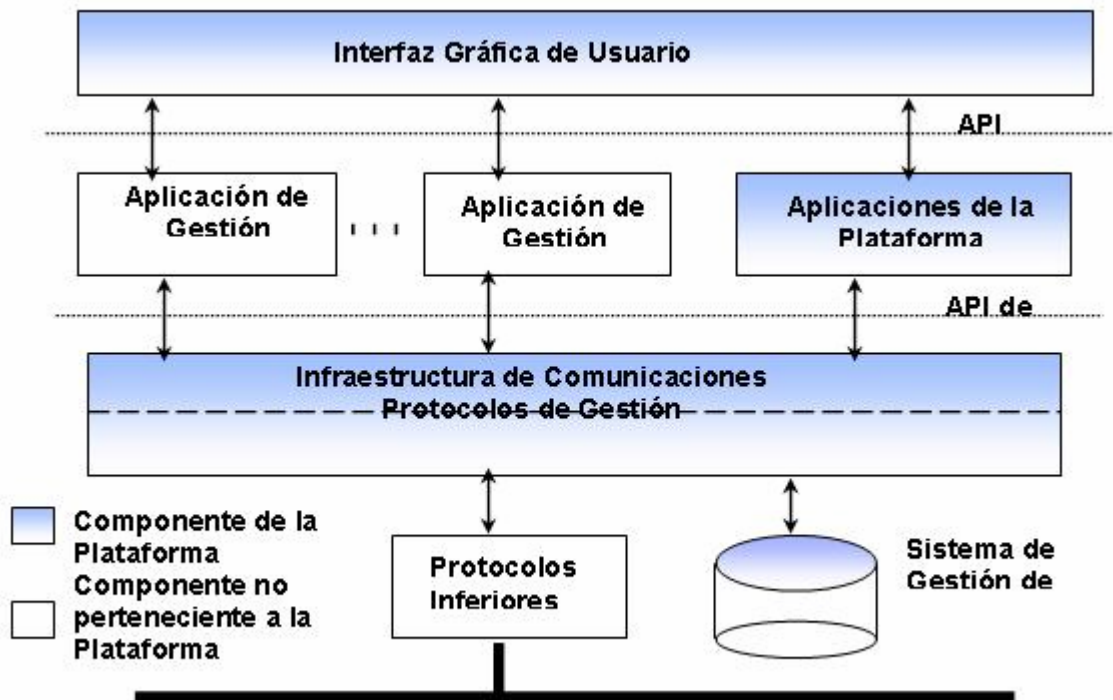
Figura. Esquema piramidal de la arquitectura TMN



Conceptos básicos a tener en cuenta

1. Surge por la necesidad de que exista un sistema común de apoyo a la operación de redes de telecomunicación.
2. Solución propuesta: estructura de red de gestión que permite interconectar diferentes sistemas de gestión con los equipos de telecomunicación.
3. Las funciones de gestión deben estar separadas de las de telecomunicación.

Figura. Componentes típicos de una Plataforma de Gestión de Red



Principales Plataformas de Gestión que existen actualmente en el mercado

- 1 SunNet Manager de Sun Microsystems.
- 2 OpenView de Hewlett-Packard.
- 3 NetView/6000 de IBM.
- 4 Tivoli
- 5 Micromuse
- 6 PolyCenter de DEC.
- 7 Spectrum de Cabletron.
- 8 ISM de Bull.
- 9 OverLord de NetLabs.

## **ANEXO C METODOLOGÍA DE DISEÑO**

Este proyecto se desarrollará teniendo en cuenta una metodología acorde a los siguientes parámetros:

- El estudio de las necesidades de las empresas
- Estudio de programas de gestión existentes en el mercado
- Diseño de módulos a tratar en nuestra aplicación para gestionar elementos de red
- Implementación de la solución
- Pruebas de la implementación desarrollada, de forma tal que la aplicación de la metodología descrita conlleve a la realización de este proyecto conforme al diagrama de flujo explicado en el desarrollo ingenieril.

## **ANEXO D**

### **ESTUDIO DE ALGUNAS DE LAS APLICACIONES DE SOFTWARE DE MONITOREO MAS CONOCIDAS ACTUALMENTE**

#### **Multi Router Traffic Grapher (MRTG)**

MRTG (Multi Router Traffic Grapher) es una herramienta de licencia gratuita, escrita en C y Perl por Tobias Oetiker y Dave Rand, que se utiliza para supervisar la carga de tráfico de interfaces de red. MRTG genera páginas HTML con gráficos que proveen una representación visual de este tráfico.

MRTG utiliza SNMP (Simple Network Management Protocol) para recolectar los datos de tráfico de un determinado dispositivo (enrutadores o servidores), por tanto es requisito contar con al menos un sistema con SNMP funcionando y correctamente configurado. SNMP manda peticiones con dos objetos identificadores (OIDs) al equipo. Una base de control de información (MIBs) controla las especificaciones de los OIDs. Después de recoger la información la envía sin procesar mediante el protocolo SNMP. MRTG graba la información en un diario del cliente. El software crea un documento HTML de los diarios, estos tienen una lista de gráficas detallando el tráfico del dispositivo. El software viene configurado para que se recopilen datos cada 5 minutos pero el tiempo puede ser modificado.

La aplicación de MRTG consiste es una serie de scripts escritos en lenguaje PERL que usan el protocolo de red SNMP (Simple Network Management Protocol) para leer los contadores de tráfico que están ubicados en los conmutadores (switch) o los encaminadores (routers) y mediante sencillos y rápidos programas escritos en lenguaje C y crea imágenes en formato PNG que representa el estado del tráfico de nuestra red. Estos gráficos los inserta en una página web que se puede consultar mediante cualquier navegador. Cabe hacer notar que para poder ver los resultados se debe tener instalado un servidor WEB en la máquina que tenga instalado el MRTG.<sup>10</sup>

#### **HP Openview**

HP tiene una larga historia en adquisición de compañías de software de gestión de red. En 2004 Hewlett Packard compro Novadigm y its Radia suite; en 2005, adquirio Peregrine y its leading IT asset and service management software portfolio. Estas se integraron en la unidad de negocio HP OpenView para crear un software de gestión de empresa de solución distribuida. En noviembre de 2006 HP completó

---

<sup>10</sup> Enciclopedia virtual libre, <http://es.wikipedia.org/wiki/MRTG.>, Octubre 1 de 2007, 3:05 P.M

su adquisición de Mercury Interactive Corp, y desde febrero de 2007 se hace integración de la aplicación Mercury.<sup>11</sup>

Debido a esta evolución, Hewlett Packard ofrece una amplia gama de productos asociados a la administración de redes, entre esos tenemos:

- HP OpenView Network Node Manager (OV NNM)
- HP OpenView Operations (OVO) — monitor systems and applications using agents
- HP OpenView ServiceCenter (formerly Peregrine ServiceCenter)
- HP OpenView AssetCenter (formerly Peregrine AssetCenter)
- HP OpenView Service Desk (OVSD)
- HP OpenView Internet Services (OVIS)
- HP OpenView Service Navigator
- HP OpenView Service Navigator
- HP OpenView Transaction Analyzer (OVTA)
- HP OpenView SOA Manager
- HP OpenView Reporter OpenView Reporter

Las funciones principales de HP openview es monitorear, controlar y mantener sistemas y aplicaciones en ambientes distribuidos.

Este software fue diseñado para ayudar a los administradores de red a detectar, resolver y prevenir problemas que ocurren en la red de cualquier empresa.

HP openview permite incorporar SPIs (Smart Plug In, agentes predefinidos) para la administración de infraestructura básica, para Sistemas operativos como Microsoft Windows, HP-UX, Sun Solaris, Linux, IBM AIX, así como también SPI para bases de datos (Oracle, Microsoft SQL).

Este software ofrece una solución a la administración mediante mapas de sofisticada tecnología que muestran complejas dependencias entre los elementos administrados. Además muestra de manera inmediata las fallas ocurridas en la red, pero con dificultad en las redes muy extensas, para la observación por parte de los operadores de red, esto deja la reducción de los tiempos de recuperación y caídas a la compleja observación de estos complicados mapas. Otro servicio para destacar, que ofrece HP openview es que monitorea constantemente el desempeño y disponibilidad de los sistemas.

Mediante los Smart Plug-Ins (SPIs), HP openview administra las aplicaciones de la empresa desde su consola HP openview, estos SPIs están incluidas para muchas de las aplicaciones, como lo son, integración de aplicaciones,

---

<sup>11</sup> Wikipedia The Free Encyclopedia, <http://en.wikipedia.org/wiki/OpenView.>, noviembre 1 de 2007, 6:36 A.M

aplicaciones e-commerce, bases de datos, servidores de aplicaciones web, servidores de directorio, administración de documentos, hardware y dispositivos de red.

Los costos aproximados de HP Openview por un año, los tenemos en la siguiente tabla:

Sistema de Gestión	precio
HP Openview Network Node Manager Starter Edition 7.5. Hasta 250 nodos	8.306,00 €
HP OpenView Network Node Manager Advanced Edition 7.5. hasta 250 nodos	14.963,00 €
Media (requerido)	402,00 €
Manuales (inglés)	402,00 €

## WhatsUp Gold v11

Este aplicativo ofrece un monitoreo de redes profundo, por medio de identificación y mapas de las direcciones mac o direcciones IP (ver siguiente figura), y de esta forma se da a conocer la conectividad entre los puertos y dispositivos específicos de un elemento de red, permitiendo la localización de los recursos.

Figura. Muestra de mapa desplegado por whatsapp



Fuente: <http://www.version.com.mx/Ipswitch/pdf/Datasheet-WUG.pdf>

La resolución de problemas se hace dando alertas vía correo electrónico, beeper, teléfono celular, SMS, audio y alertas en la bandeja de tareas del sistema, Redireccionando SNMP y reiniciando servicios que son críticos al negocio.

Whatsup Además utiliza el protocolo SNMP para monitorear octetos y identificar las fluctuaciones anormales, ancho de banda y además, determinar disponibilidad de paginas HTTP (ver siguiente figura).

Figura. Muestra de la utilización del protocolo SNMP en Whatsup



Fuente: <http://www.version.com.mx/ipswitch/pdf/Datasheet-WUG.pdf>

Es importante destacar que el WhatsUp utiliza el Windows Management Instrumentation (WMI) de Microsoft para coleccionar información histórica y en tiempo real sobre los dispositivos Windows de la red.

WMI es un estándar de Microsoft Windows para obtener información de sistemas bajo Windows. WMI viene instalado automáticamente como “default” en sistemas Windows 2000, 2003 y XP.<sup>12</sup>

Los costos aproximados de Whatsup por un año, los tenemos en la siguiente tabla:

WhatsUp Gold Premium	Precio
Hasta 100 dispositivos	\$2.595,00
Hasta 300 dispositivos	\$3.795,00
Hasta 500 dispositivos	\$4.995,00
Mayor a 500 dispositivos	\$6.995,00

Los precios de renovación Anuales son los siguientes:

Whatsup Gold Premium	Precio
Hasta 100 dispositivos	\$ 795
Hasta 300 dispositivos	\$ 995
Hasta 500 dispositivos	\$ 1.295
Mayor a 500 dispositivos	\$ 1.695

<sup>12</sup> Enciclopedia virtual libre, <http://www.ipswitch.com/international/spanish/whatsupgold.asp>, Octubre 1 de 2007, 3:05 P.M

**ANEXO E**  
**LEY 44 DE 1993**

EL CONGRESO DE COLOMBIA,

DECRETA:

CAPÍTULO I.

DISPOSICIONES ESPECIALES.

ARTÍCULO 1o. Los empleados y funcionarios públicos que sean autores de obras protegidas por el Derecho de Autor, podrán disponer contractualmente de ellas con cualquiera entidad de derecho público.

ARTÍCULO 2o. El artículo 29 de la Ley 23 de 1982, quedará así:

Los derechos, consagrados a favor de los artistas intérpretes o ejecutantes, de los productores de fonogramas y de los organismos de radiodifusión tendrán la siguiente duración:

Cuando el titular sea persona natural, la protección se dispensará durante su vida y ochenta años más a partir de su muerte.

Cuando el titular sea persona jurídica, el término de protección será de cincuenta años, contados a partir del último día del año en que tuvo lugar la interpretación o ejecución, la primera publicación del fonograma o, de no ser publicado, de su primera fijación, o la emisión de su radiodifusión.

CAPÍTULO II.

DEL REGISTRO NACIONAL DEL DERECHO DE AUTOR.

ARTÍCULO 3o. Se podrán inscribir en el Registro Nacional del Derecho de Autor.

a) Las obras literarias, científicas y artísticas:

b) Los actos en virtud de los cuales se enajene el Derecho de Autor, así como cualquier otro acto o contrato vinculado con los derechos de autor o los derechos conexos;

c) Los fonogramas;



d) Los poderes de carácter general otorgados a personas naturales o jurídicas para gestionar ante la Dirección Nacional del Derecho de Autor, o cualquiera de sus dependencias, asuntos relacionados con la Ley 23 de 1982.

ARTÍCULO 4o. El registro de las obras y actos sujetos a las formalidades del artículo anterior tiene por objeto:

a) Dar publicidad al derecho de los titulares y a los actos y contratos que transfieran o cambien ese dominio amparado por la ley;

b) Dar garantía de autenticidad y seguridad a los títulos de derechos de autor y derechos conexos y a los actos y documentos que a ellos se refiere.

ARTÍCULO 5o. El registro de las obras y actos deben ajustarse, en lo posible, a la forma y términos preestablecidos por el derecho común para el registro de instrumentos públicos.

Tal diligencia será firmada en el libro o libros correspondientes por el funcionario competente.

ARTÍCULO 6o. Todo acto en virtud del cual se enajene el Derecho de Autor, o los Derechos Conexos así como cualquier otro acto o contrato vinculado con estos derechos, deberá ser inscrito en el Registro Nacional del Derecho de Autor como condición de publicidad y oponibilidad ante terceros.

ARTÍCULO 7o. El editor, el productor de obras audiovisuales, el productor fonográfico y videograbador, establecidos en el país, de toda obra impresa, obra audiovisual, fonograma o videograma, o el importador de libros, fonogramas o videogramas que circulen en Colombia deberá cumplir, dentro de los 60 días hábiles siguientes a su publicación, transmisión pública, reproducción o importación, con el depósito legal de las mismas ante las entidades y en la cantidad definida en el reglamento que para el efecto expedirá el Gobierno Nacional.

<Inciso modificado por el artículo 72 del decreto 2150 de 1995. El nuevo texto es el siguiente:> La omisión del Depósito Legal a que se refiere este artículo, ocasionará al editor, productor de obras audiovisuales, productor fonográfico, videograbador, o importador, según el caso, una multa igual a 10 veces el valor comercial de cada ejemplar no depositado, la cual será impuesta por el Director de la Biblioteca Nacional, mediante resolución motivada.

<Notas de Vigencia>

<Jurisprudencia - Vigencia>

<Legislación Anterior>

ARTÍCULO 8o. Toda obra que sea presentada como inédita para efectos de la inscripción en el Registro Nacional del Derecho de Autor, sólo podrá ser consultado por el autor o autores de la misma.

ARTÍCULO 9o. El Gobierno Nacional establecerá los requisitos y procedimientos de inscripción ante el Registro Nacional del Derecho de Autor.

CAPÍTULO IV.

DE LAS SANCIONES.

ARTÍCULO 51. Incurrirá en prisión de dos (2) a cinco (5) años y multa de cinco (5) a veinte (20) salarios legales mínimos mensuales:

1. Quien publique una obra literaria o artística inédita, o parte de ella, por cualquier medio, sin la autorización previa y expresa del titular del derecho.
2. Quien inscriba en el registro de autor una obra literaria, científica o artística a nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado, modificado o mutilado, o mencionando falsamente el nombre del editor, productor fonográfico, cinematográfico, videográfico o de soporte lógico.

<Jurisprudencia Vigencia>

3. Quien de cualquier modo o por cualquier medio reproduzca, enajene, compendie, mutile o transforme una obra literaria, científica o artística, sin autorización previa y expresa, de sus titulares.
4. Quien reproduzca fonogramas, videogramas, soporte lógico u obras cinematográficas sin autorización previa y expresa del titular, o transporte, almacene, conserve, distribuya, importe, venda, ofrezca, adquiera para la venta o distribución o suministre a cualquier título dichas reproducciones.

<Jurisprudencia Vigencia>

PARÁGRAFO. Si en el soporte material, carátula o presentación de la obra literaria, fonograma, videograma, soporte lógico u obra cinematográfica se emplea el nombre, razón social, logotipo o distintivo del titular legítimo del derecho, las penas anteriores se aumentarán hasta en la mitad.

ARTÍCULO 52. Incurrirá en prisión de uno (1) a cuatro (4) años y multa de tres (3) a diez (10) salarios legales mínimos mensuales:

1. Quien represente, ejecute o exhiba públicamente obras teatrales, musicales, fonogramas, videogramas, obras cinematográficas o cualquier otra obra literaria o artística, sin autorización previa y expresa del titular de los derechos correspondientes.

2. Quien alquile o de cualquier otro modo comercialice fonogramas, videogramas, soportes lógicos u obras cinematográficas sin autorización previa y expresa del titular de los derechos correspondientes.

<Jurisprudencia Vigencia>

3. Quien fije, reproduzca o comercialice las representaciones públicas de obras teatrales o musicales, sin autorización previa y expresa del titular de los derechos correspondientes.

4. Quien disponga o realice la comunicación, fijación, ejecución, exhibición, comercialización, difusión o distribución, representación o de cualquier modo o por cualquier medio conocido o por conocer utilice una obra sin autorización previa y expresa de su titular.

5. Quien presentare declaraciones falsas destinadas directa o indirectamente al pago o distribución de derechos económicos de autor, alterando los datos referentes a la concurrencia de público, clase, precio y número de entradas vendidas para un espectáculo o reunión, número de entradas distribuidas gratuitamente, de modo que pueda resultar perjuicio para el autor.

6. Quien presentare declaraciones falsas destinadas directa o indirectamente al pago o distribución de derechos económicos de autor, alterando el número de ejemplares producidos, vendidos, o distribuidos gratuitamente de modo que pueda resultar perjuicio para el autor.

7. Quien presentare declaraciones falsas destinadas a la distribución de derechos económicos de autor, omitiendo, sustituyendo o intercalando indebidamente los datos de las obras respectivas.

8. Quien realizare acciones tendientes a falsear los ingresos reales de un espectáculo o reunión.

9. Quien retransmita, fije, reproduzca o por cualquier medio sonoro o audiovisual divulgue, sin la autorizaci3n previa y expresa del titular las emisiones de los organismos de radiodifusi3n.

10. Quien recepcione, difunda o distribuya por cualquier medio, sin autorizaci3n previa y expresa del titular, las emisiones de la televisi3n por suscripci3n.

PARÁGRAFO. En los procesos por los delitos previstos en este artículo, la acción penal se extinguirá por desistimiento del ofendido, cuando el procesado antes de dictarse sentencia de primera instancia, indemnice los perjuicios causados.

<Jurisprudencia Vigencia>

ARTÍCULO 53. Las penas previstas en los artículos anteriores se aumentarán hasta en la mitad en los siguientes casos:

1. Cuando en la realización del hecho punible hayan intervenido dos (2) o más personas.
2. Cuando el perjuicio económico causado por el hecho punible sea superior a cincuenta (50) salarios legales mínimos mensuales, o siendo inferior, ocasione grave daño a la víctima.

<Jurisprudencia Vigencia>

ARTÍCULO 54. Las autoridades de policía harán cesar la actividad ilícita, mediante:

1. La suspensión de la actividad infractora.
2. La incautación de los ejemplares ilícitos, de los moldes, planchas, matrices, negativos, soportes, cintas, carátulas, diskettes, equipos de telecomunicaciones, maquinaria, y demás elementos destinados a la producción o reproducción de ejemplares ilícitos o a su comercialización.
3. El cierre inmediato del establecimiento, si se trata de local abierto al público y la suspensión o cancelación de la licencia de funcionamiento.

<Jurisprudencia Vigencia>

ARTÍCULO 55. Las publicaciones, ejemplares, reproducciones, moldes, planchas, matrices, negativos, cintas, carátulas o etiquetas incautadas serán sometidos a inspección judicial con la ayuda del perito, y una vez demostrada por este medio su ilegitimidad, serán destruidas por las autoridades de policía judicial, en presencia del funcionario judicial y con citación de la defensa y la parte civil.

<Jurisprudencia Vigencia>

ARTÍCULO 56. Los bienes incautados, destinados directa o indirectamente para la producción, reproducción, distribución, transporte o comercialización de los ejemplares ilícitos, serán embargados y secuestrados o decomisados de oficio y, previo avalúo, los que no deban ser destruidos se adjudicarán en la sentencia

condenatoria a los perjudicados en el hecho punible, a título de indemnización de perjuicios o se dispondrá su remate para tal fin.

ARTÍCULO 57. Para la tasación de los perjuicios materiales causados por el hecho, se tendrá en cuenta:

1. El valor comercial de los ejemplares producidos o reproducidos sin autorización.
2. El valor que hubiere percibido el titular del derecho de haber autorizado su explotación.
3. El lapso durante el cual se efectuó la explotación ilícita.

ARTÍCULO 58. Las investigaciones a que den lugar los hechos punibles tipificados en los artículos 51 y 52 de esta Ley, se adelantarán conforme al proceso ordinario. Si el imputado es capturado en flagrancia o existe confesión simple de su parte, se seguirá el procedimiento abreviado que la ley señale.

ARTÍCULO 59. La acción penal que originan las infracciones a esta Ley, es pública en todos los casos y se iniciará de oficio.

ARTÍCULO 60. Las asociaciones de gestión colectiva de derechos y derechos conexos reconocidos en la Ley 23 de 1982, podrán demandar ante la jurisdicción civil o penal en representación de sus asociados, el resarcimiento de los perjuicios causados en los hechos punibles.

## ANEXO F ESTUDIO DE COSTOS

Teniendo en cuenta los costos que debe afrontar una empresa proveedora de servicios de telecomunicaciones a la hora de instalar enlaces de datos, se realizó la siguiente relación de gastos, basada en unos valores reales para el diseño de una red de fibra óptica metropolitana, cuya fuente es una empresa de telecomunicaciones reconocida en el país (confidencial). Se resalta el porcentaje con el que influye el sistema de Gestión de red, en la relación de gastos:

RELACIÓN DE COSTOS		
Descripción	Costo	Porcentaje
Equipos activos	US\$ 1,615.026	70,23%
* Sistema de gestión	207.790	9,03%
Instalación y tendido de fibra	529.528	23,02%
Personal	137.377	5,97%
Dotación y herramientas	9.362	0,40%
Administración	8,127	0,35%
<b>TOTAL</b>	<b>US\$ 2,299.417</b>	<b>100%</b>

Como se puede observar en la tabla de costos anterior, el sistema de gestión de red tendría un valor aproximado de US\$ 207.790, un 9.3 % del valor total del costo del enlace. Obviamente se debe tener en cuenta el sistema de gestión que se va a utilizar, pues no cuesta lo mismo tener un enlace bajo un sistema de gestión HP OPENVIEW a un enlace bajo un sistema de gestión MERCURY. Además del costo del sistema de gestión de red, se deben tener en cuenta otros costos que lleva implícitos la elección del aplicativo que se va a utilizar, como son la capacitación del personal para que sea competente a la hora de utilizar el programa y este sea aprovechado al máximo, y los equipos que deben adquirirse para que estos aplicativos puedan desempeñar su función como es debido, teniendo en cuenta que en muchos casos estos equipos de cómputo necesitan ser muy robustos y por ende muy costosos. Estos altos gastos se deben al hecho que muchas veces los aplicativos que adquieren las empresas de telecomunicaciones, cuentan con demasiadas herramientas, algunas de las cuales la empresa que utiliza el aplicativo realmente no necesita y en cambio carece de algunas que la empresa desearía tener y el software no incluye.

Este sería el costo que la empresa tendría que asumir para instalar un enlace, sin tener en cuenta el margen de ganancia que debe considerarse al fijar el precio al usuario final. Citando la misma fuente anterior, para el mismo enlace se tiene que el precio cobrado al usuario final es de **US \$2.859.975**, o sea **US \$560.558** más de lo que costo el enlace, obteniendo un margen de ganancia del 19.6 %. Esto afecta

directamente al usuario final, causando que muchas veces algunas empresas se limiten en cuanto a la adquisición de nuevas tecnologías debido a que su costo es inasequible. Este proyecto tiene como uno de sus objetivos precisamente el hecho de disminuir los costos tanto a la empresa proveedora de comunicaciones como al usuario final, disminuyendo la inversión necesaria en cuanto a los sistemas de gestión de red se refiere.

De esto se podría concluir que si estos desarrollos de software se hicieran en este país de una forma mas personalizada, teniendo en cuenta que las necesidades de las empresas de telecomunicaciones propias difieren de las necesidades de las empresas de telecomunicaciones de otros países, los costos que tendrían que asumir las empresas de telecomunicaciones en el tema de gestión de red disminuirían considerablemente, no solo en la adquisición de las licencias y el soporte técnico que respalda al aplicativo, si no además en la capacitación del personal para que se explote al máximo la herramienta adquirida. Este objetivo podría alcanzarse si los estudiantes se interesaran y se prepararan mejor en estos temas prácticos que les permitan no estar sujetos a la búsqueda de un empleo y a engrosar las filas de desempleados en este país, si no que salieran directamente con la idea de aportarle algo al desarrollo de las empresas de este país.

Para tener el panorama claro, de cuanto es el costo de operación de algunos de los sistemas de gestión para 250 nodos existentes en el mercado, se realizó una consulta que nos arrojó los siguientes resultados:

Fabricante	Aplicativos de gestion de redes	Precio
Cisco	CiscoWorks2000 LMS 2.2 WIN/SOL	US \$19995
IBM	Enterprise Tivoli	US \$9600
HP	Openview NNM SE 250 Nd Pk 7.01 LTU	US \$5550
HP	Openview O/T Manager Upg LTU from NNM/Solaris	US \$59000
IPSWITCH	Whatsup gold Premium	US \$6995

**ANEXO G  
CHECKLIST**



## CHECKLIST (TELEFONICA TELECOM)

El siguiente documento se realiza como parte de la fase de investigación del proyecto de grado como requisito para optar por el Título de Ingenieros Electrónicos de la Universidad De San Buenaventura, titulado, "DESARROLLO DE UN APLICATIVO PARA MONITOREO DE ENRUTADORES CISCO Y/O HUAWEI".

### ENTREVISTADO: VICTOR MORALES

1- Que cargo tiene usted en TELECOM?

Victor Morales: Soy jefe de soporte y mantenimiento del área conmutación, trabajo desde el año 1995 en gestión de red, enfocado a la parte de telefonía.

2- Que aplicativos de gestión de red se utilizaban en esa época?

VM: El producto adquirido por TELECOM en esa época para el ámbito de gestión de redes fue NETMINDER, el cual fue adquirido a AT&T y era un sistema orientado a la gestión de la red de telefonía.

3- Actualmente que aplicativos se manejan en TELECOM?

VM: En la actualidad el sistema ya fue reemplazado y tenemos herramientas propietarias desarrolladas por TELEFONICA I+D en España que nos permiten hacer la gestión de desempeño en telefonía y gestión de alarmas, los cuales son sistemas puestos en funcionamiento a partir de este año. Para la parte de gestión de tráfico el aplicativo utilizado es ECGT y para la gestión de alarmas el aplicativo es EOC (Entorno de observación y conservación). El primero toma información de las centrales telefónicas, el desempeño basado en observaciones sobre muestras tomadas cada 5 minutos, y el segundo toma la información de alarmas de las centrales. En la actualidad son 40 la centrales conectadas al sistema, las cuales entregan información de desempeño cada 5 minutos, y de alarma espontáneamente. El cubrimiento que se espera tener para el siguiente año es de 127 centrales y el sistema que se tiene actualmente puede soportar esa cantidad de centrales y mas. En cuanto al core de transmisión de fibra óptica que tiene TELECOM, a partir del año 95 tiene sistemas propietarios de NEC, el sistema ISDH de fibra óptica se llama INC 100B y maneja todo el cubrimiento de los dos anillos de fibra óptica que tiene TELECOM a nivel nacional. Posteriormente hace tres años se hace una adquisición a través de HUAWEI para el monitoreo de los enlaces de fibra, el TC 2000.

Posteriormente TELECOM entra a se parte del plan de telefonía social, en el plan bianual<sup>1</sup> que es el primer plan de convergencia que existe instalada en el país a través de ERICSSON. Los elementos de red en este plan de convergencia tienen como software de gestión de red a NETCOOL para el soporte de las 112 localidades instaladas. A través de NETCOOL se gestionan las alarmas de energía, de transmisión, y de conmutación y el backbone que comunica todas estas localidades también. A través de IMPACT de NETCOOL se monitorean mediante mapas las fallas y afectaciones que se presentan ,e esto para la parte de conmutación. Para la parte de monitoreo en la red de energía se utiliza la herramienta NETBOSS, la cual es un sistema propietario de HARRIS y adicionalmente se utiliza la herramienta POWEMANAGER para llevar a cabo acciones sobre los eventos presentados, como arranque de plantas, realización de conmutación en la parte de inversores.

4- En la parte de gestión de datos, que otros aplicativos se utilizan aparte de la herramienta NETCOOL??

VM: Mi área tiene mas que ver con a conmutación, pero en la red de datos se utilizan sistemas como NETCOOL, PRTG, MRTG, WHATSUP y HP OPENVIEW.

5- Mediante que interface de usuario grafica se realiza el monitoreo a escala grupal?

VM: Se cuenta con 5 pantallas de proyección gigantes, 3 monitores de plasma, y mas de 30 monitores de ordenadores de escritorio.

6- Que tipo de GUI utilizan los aplicativos utilizados para el monitoreo de red?

VM: Se utilizan tipos de GUI diversas como son GUI orientada a interfaz WEB y abierta a cualquier tipo de navegador, orientada a interfaz WEB utilizada con un solo tipo de navegador, orientada a interfaz WINDOWS sobre sistema operativo WINDOWS, orientada a interfaz Windows sobre sistema operativo UNIX y orientada a interfaz tipo consola DOS.

7- Considera que con los aplicativos que cuenta en su centro de gestión de red existe lo suficiente para atender las fallas o eventos de red oportunamente y además existe lo necesario para poder minimizar el tiempo de atención?

VM: No.

8- De forma global, cuanto podría ser el costo aproximado de los sistemas de gestión de red anteriormente mencionados?

VM: Los sistemas de conmutación superan aproximadamente los 10 millones de dólares.

## **CHECKLIST (Banco Caja Social BCSC)**

### **ENTREVISTADO: HENRY PACHECO**

El siguiente documento se realiza como parte de la fase de investigación del proyecto de grado como requisito para optar por el Título de Ingenieros Electrónicos de la Universidad De San Buenaventura, titulado, "DESARROLLO DE UN APLICATIVO PARA MONITOREO DE ENRUTADORES CISCO Y/O HUAWEI".

1- Con que aplicativos se realizan las tareas respecto a monitoreo de elementos de red ?

R/: En el banco tenemos OPENVIEW y MERCURI para hacer el monitoreo de las redes.

2- Mediante que interface de usuario grafica "Graphic User Interface" **GUI** se realiza el monitoreo a escala grupal?

R/: Mediante los monitores de cada ordenador, y mediante pantallas gigantes de plasma, donde hay monitores pendientes de lo que ocurre en la red.

Indique que tipo de GUI utilizan los aplicativos utilizados para el monitoreo de red:

R/: Utilizamos una GUI propia de UNIX que es donde tenemos montada la parte de OPENVIEW, aunque también utilizamos GUI sobre Browser.

3- ¿Considera que con los aplicativos con que se cuenta en su centro de gestión de red existe lo suficiente para atender las fallas o eventos de red oportunamente y además existe lo necesario para poder minimizar el tiempo de atención?

R/: En la parte básica los aplicativos actuales muestran muchas de las fallas que se presentan, pero obviamente hacen falta cosas que uno tiene que ir a consultar a diferentes sitios para poder atender las fallas oportunamente. Por ejemplo uno en estos esquemas no tiene una base de datos de los contactos, si bien la herramienta indica los eventos, no nos da la facilidad de tener a la mano la información de los encargados a quienes se debe contactar para que tomen acciones de forma oportuna.

4- Consideraría ventajoso el contar con una herramienta que le avisara cuando existe una falla o evento de red únicamente cuando sea necesario sin necesidad de estar pendiente de la revisión continua del aplicativo de gestión y que a su vez la o la GUI desplegaran las fallas relevantes de una forma más amigable?

R/: Esa es una de las grandes desventajas que tienen las herramientas actuales en el mercado, que dan muchísima información, entonces toca analizarla y eso toma tiempo. Si la herramienta avisara únicamente lo importante, ahorraría una cantidad enorme de trabajo. Las herramientas actuales vienen con la capacidad de hacer muchas cosas, entonces el trabajo que se debe hacer para personalizarla y llevarla a un punto que sea útil es muy largo y muy dispendioso a veces, además tiene un tiempo de aprendizaje, lo cual es una ventaja que veo en la aplicación que ustedes están desarrollando, ya que ustedes han plasmado allí el conocimiento que tienen sobre la red, entonces solo se están reportando en su aplicación únicamente cosas importante y puntuales.

CHECKLIST  
(Banco Caja Social BCSC)

El siguiente documento se realiza como parte de la fase de investigación del proyecto de grado como requisito para optar por el Título de Ingenieros Electrónicos de la Universidad De Sanbuenaventura, titulado, "DESARROLLO DE UN APLICATIVO PARA MONITOREO DE ENRUTADORES CISCO Y/O HUAWEI".

1- Con que aplicativos se realizan las tareas respecto a monitoreo de elementos de red

Nombre del Aplicativo	SI	NO
HP Opnview	✓	
Cisco Works		
PRTG		
Netcool		
MRTG		
Whatsup		
Tivoli		
Otro	✓	

Nota: En caso de responder Otro, especificar cual o cuales son abajo:

Nombre del Aplicativo
Se utilizan sistemas propietarios como:
- 3com Network director - equipos 3com
- Netsight Atlas - Equipos Enterasy.
Estos sistemas para gestión en las 3 primeras capas del OSI, para las capas superiores se utiliza:
- Mercury.



2- Mediante que interface de usuario grafica "Graphic User Interface" GUI se realiza el monitoreo a escala grupal:

Interface de usuario grafica	SI	NO
Pantalla gigante con proyector		
Computadores de escritorio	✓	
Pantalla de plasma	✓	
Pantalla tipo Publik		
Otro		

**Nota:** En caso de responder Otro, especificar cual o cuales son abajo:

Nombre del Aplicativo



3- Indique que tipo de GUI utilizan los aplicativos utilizados para el monitoreo de red:

Tipo de GUI	SI	NO
Orientada a interface web y abierta a cualquier tipo de navegador	✓	
Orientada a interface web utilizada con un solo tipo de navegador		
Orientada a interface windows sobre sistema operativo windows	✓	
Orientada a interface windows sobre sistema operativo tipo UNIX	✓	
Orientada a interface tipo consola DOS		
Propietaria	✓	
Otra		

**Nota:** En caso de responder Otra, especificar cual o cuales son abajo:

Tipo de GUI



4- ¿Considera que con los aplicativos con que se cuenta en su centro de gestión de red existe lo suficiente para atender las fallas o eventos de red oportunamente y además existe lo necesario para poder minimizar el tiempo de atención?

Si	<input type="checkbox"/>
No	<input checked="" type="checkbox"/>

**Nota:** En caso de responder No, indique en la siguiente tabla con que herramientas o aplicativos se podría minimizar el tiempo de atención y detección de fallas o mediante que recurso de software y hardware se podría facilitar el monitoreo de red:

Tipo hardware o software
<i>Sería ideal en nuestro caso contar con un Centro de gestión de red, adaptando herramientas ya existentes como HP-Openview.</i>

5- ¿Consideraría ventajoso el contar con una herramienta que le avisara cuando existe una falla o evento de red únicamente cuando sea necesario sin necesidad de estar pendiente de la revisión continua del aplicativo de gestión y que a su vez la o las GUI desplegaran las fallas relevantes y de una forma mas amigable?

Si	<input checked="" type="checkbox"/>
No	<input type="checkbox"/>





**Nota:** En caso de responder Si, indique en la siguiente tabla mediante que forma quisiera que los aplicativos le avisaran acerca de eventos o fallas en la red y como desearia que la información se desplegara:

Respuesta obtenida por el encuestado
Pop-ups, emails, beepers e llamadas a celular
son elementos de alerta interesantes, desde
que estas alertas sean pertinentes y no
perjudiquen al usuario enviando alertas sobre
eventos relevantes para algunos departamentos
e irrelevantes para otros.

Entrevistado: Ing. German Vinas



**CHECKLIST**  
(Banco Caja Social BCSC)

El siguiente documento se realiza como parte de la fase de investigación del proyecto de grado como requisito para optar por el Título de Ingenieros Electrónicos de la Universidad De Sanbuenaventura, titulado, "DESARROLLO DE UN APLICATIVO PARA MONITOREO DE ENRUTADORES CISCO Y/O HUawei".

1- Con que aplicativos se realizan las tareas respecto a monitoreo de elementos de red

Nombre del Aplicativo	SI	NO
HP Openview	✓	
Cisco Works		
PRTG		
Netcool		
MRTG		
Whatsup		
Tivoli		
Otro	✓	

**Nota:** En caso de responder Otro, especificar cual o cuales son abajo:

Nombre del Aplicativo
<i>Mercury - Hp.</i>
<i>Snmp Manager</i>

*51.700.024*

2- Mediante que interface de usuario grafica "Graphic User Interface" GUI se realiza el monitoreo a escala grupal:

Interface de usuario grafica	SI	NO
Pantalla gigante con proyector		
Computadores de escritorio	✓	
Pantalla de plasma		
Pantalla tipo Publik	✓	
Otro		

Nota: En caso de responder Otro, especificar cual o cuales son abajo:

Nombre del Aplicativo

3- Indique que tipo de GUI utilizan los aplicativos utilizados para el monitoreo de red:

Tipo de GUI	SI	NO
Orientada a interface web y abierta a cualquier tipo de navegador		
Orientada a interface web utilizada con un solo tipo de navegador		
Orientada a interface windows sobre sistema operativo windows	✓	
Orientada a interface windows sobre sistema operativo tipo UNIX	✓	
Orientada a interface tipo consola DOS		
Propietaria		
Otra		

Nota: En caso de responder Otra, especificar cual o cuales son abajo:

Tipo de GUI

4- ¿Considera que con los aplicativos con que se cuenta en su centro de gestion de red existe lo suficiente para atender las fallas o eventos de red oportunamente y además existe lo necesario para poder minimizar el tiempo de atención?

Si	<input type="checkbox"/>
No	<input checked="" type="checkbox"/>

**Nota:** En caso de responder No, indique en la siguiente tabla con que herramientas o aplicativos se podría minimizar el tiempo de atención y detección de fallas o mediante que recurso de software y hardware se podría facilitar el monitoreo de red:

Tipo hardware o software
<i>Wlan sup</i>
<i>Managers - thousei</i>

5- ¿Consideraría ventajoso el contar con una herramienta que le avisara cuando existe una falla o evento de red únicamente cuando sea necesario sin necesidad de estar pendiente de la revisión continua del aplicativo de gestión y que a su vez la o las GUI desplegaran las fallas relevantes y de una forma mas amigable?

Si	<input checked="" type="checkbox"/>
No	<input type="checkbox"/>

**Nota:** En caso de responder Si, indique en la siguiente tabla mediante que forma quisiera que los aplicativos le avisaran acerca de eventos o fallas en la red y como desearia que la información se desplegara:

Respuesta obtenida por el encuestado
- Pop up.
- a-mail.

Entrevistada : Mg. Luz Marina Torres



## **ANEXO F SUGERENCIAS DEL JURADO**

A petición de los jurados de este proyecto, sustentado el día 15 de noviembre del 2007, se anexan los siguientes ítems, a medida de complementación del presente documento:

### **Detalles significativos acerca de la pantalla tipo Publik utilizado en este proyecto**

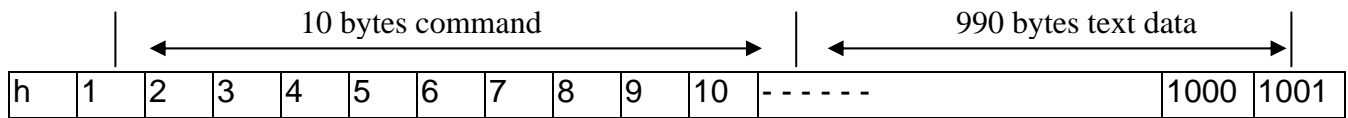
Se utilizo una pantalla tipo Publik de color negro, compuesta por 16 matrices de diodos LED, cada una de 5 columnas X 7 filas de LEDs, lo que indica que en total, todo el Publik esta compuesto por 80 columnas y 7 filas de LEDs. Se compone también de dos ranuras de conexión, una que permite la alimentación de corriente del Publik, y la otra, que permite la comunicación con el computador. Esta última ranura sirve como conexión de un cable, el cual tiene dos terminaciones diferentes, por un lado tiene un conector serial, y por el otro un conector RJ 11.

La configuración del Publik es algo compleja, y para ello se siguieron los siguientes pasos; primero se configuró la conexión del Publik con el computador, lo cual se logró mediante la utilización de un osciloscopio. El Publik trabaja a una frecuencia desconocida, por lo que para poderlo sincronizar se debió buscar la velocidad de transmisión con la que trabaja el Publik, para lo cual se utilizó un osciloscopio. La velocidad resultante fue de 2400 baudios, con la cual se sincronizó el Publik con el computador y ahí se pudo empezar la comunicación entre ambas partes. Seguidamente se buscó capturar la trama utilizada por el Publik para recibir datos, el modelo de la trama se anexó posteriormente. La trama contiene un total de 1000 bytes, de los cuales se necesita un byte de preámbulo y uno de finalización, pero en el protocolo anexado no se cuenta con esta información. Para poder conocer la trama en su totalidad, se necesitó capturar la trama por medio de un Sniffer, con el cual se capturaron algunas tramas para conocer los datos de preámbulo y de finalización. Una vez se estableció completamente la comunicación entre el Publik y el computador, se procedió a configurar el Php para que desde este se pudiera trabajar directamente sobre el puerto serial. La configuración del puerto serial mediante Php se logró mediante la instalación de la librería Php\_ser.dll.

### **Structure of Protocol:**

#### **Text Data**

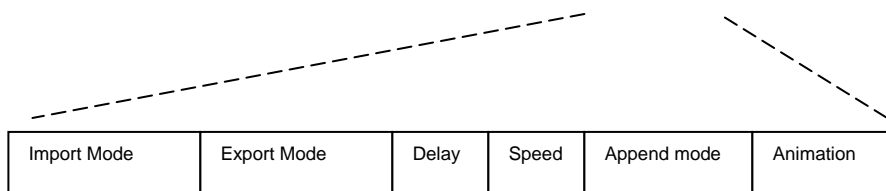
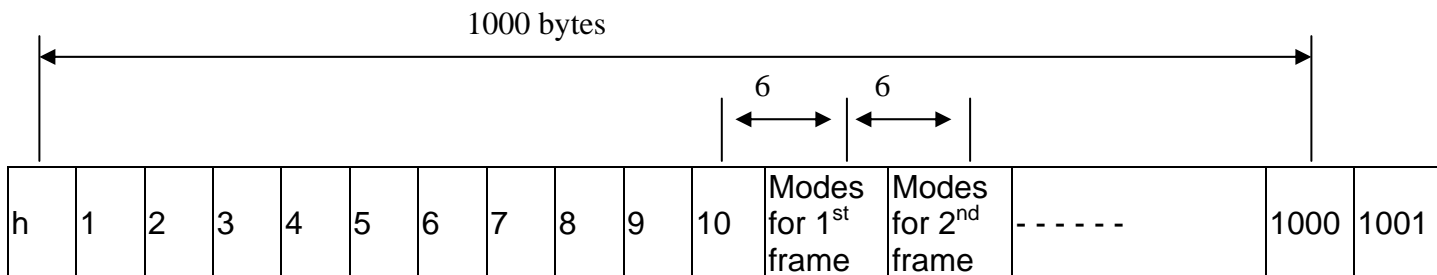
This is the actual part of the message that includes the message itself and information on the colors, the fonts, the sizes.



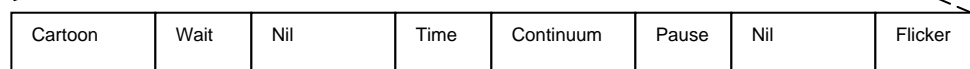
H	Packet header also serves as destination Sign identifier
1	Data Code for LED pixels <ul style="list-style-type: none"> <li>✓ 7FH: the header for red (for the first frame only)</li> <li>✓ 6FH: the header for green (for the first frame only)</li> <li>✓ 7EH: the header for red (for the middle frames, 0-N frames)</li> <li>✓ 6EH: the header for green (for the middle frames, 0-N frames)</li> <li>✓ 7DH: the header for red (for the last frame only)</li> <li>✓ 6DH: the header for green (for the last frame only)</li> </ul>
2	Nil
3 – 10	Nil
11 – 1000	Text data
1001	Packet end for checking

### Command Data

This is the actual part of the message that includes the functions such as scroll up, scroll down, Time, Animation etc.



1 byte



1 bit



H	Packet header also serves as destination Sign identifier
1	Command code (5FH)
2	The total no. of frames for uploading
3	Nil
4	The 1 <sup>st</sup> frame (default=0)
5	The last frame
6	The length of the sign ( = the pixel wide / 8 )
7	The height of the sign ( = the pixel height / 8 )
8	Color (1: single color; 2: tricolor)
9	The max. frames for the sign
10	D0=0
11 --	Modes for each frame, each frame contains 6 bytes
1001	Pocket end for checking

**Import Mode:**

- 0: Move from right
- 1: Move from left
- 2: Scroll up
- 3: Scroll bottom
- 4: Jump from right
- 5: Open from left
- 6: Open from right
- 7: Open from bottom
- 8: Open from up
- 9: Open from center
- 10: Open from both sides
- 11: Cover from center
- 12: Cover from both sides
- 13: Immediate
- 14: Ready
- 15: Random

**Export Mode:**

- 0: Move from right
- 1: Move from left
- 2: Scroll up
- 3: Scroll bottom
- 4: Jump from right
- 5: Open from left
- 6: Open from right
- 7: Open from bottom
- 8: Open from up

- 9: Open from center
- 10: Open from both sides
- 11: Cover from center
- 12: Cover from both sides
- 13: Immediate
- 14: Ready
- 15: Random

**Delay:** 0 – 19 seconds

**Speed:** 0 – 7 moving speeds; 0=fastest

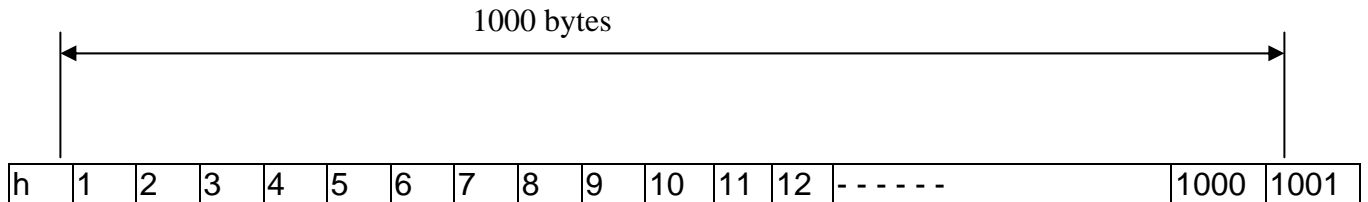
**Append Mode:**

1<sup>st</sup> bit: Cartoon; 2<sup>nd</sup> bit: Wait; 3<sup>rd</sup> bit: Nil; 4<sup>th</sup> bit: Time; 5<sup>th</sup> bit: Continuum; 6<sup>th</sup> bit: Pause; 7<sup>th</sup> bit: Nil; 8<sup>th</sup> bit: Flicker

**Animation:**

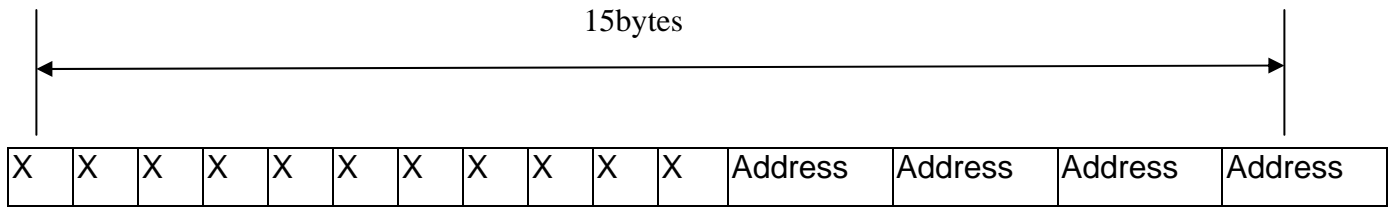
(0: Eat bean; 1: Toxophily; 2: Weight lifting; 3: Lion; 4: Horse)

**Clock Data**

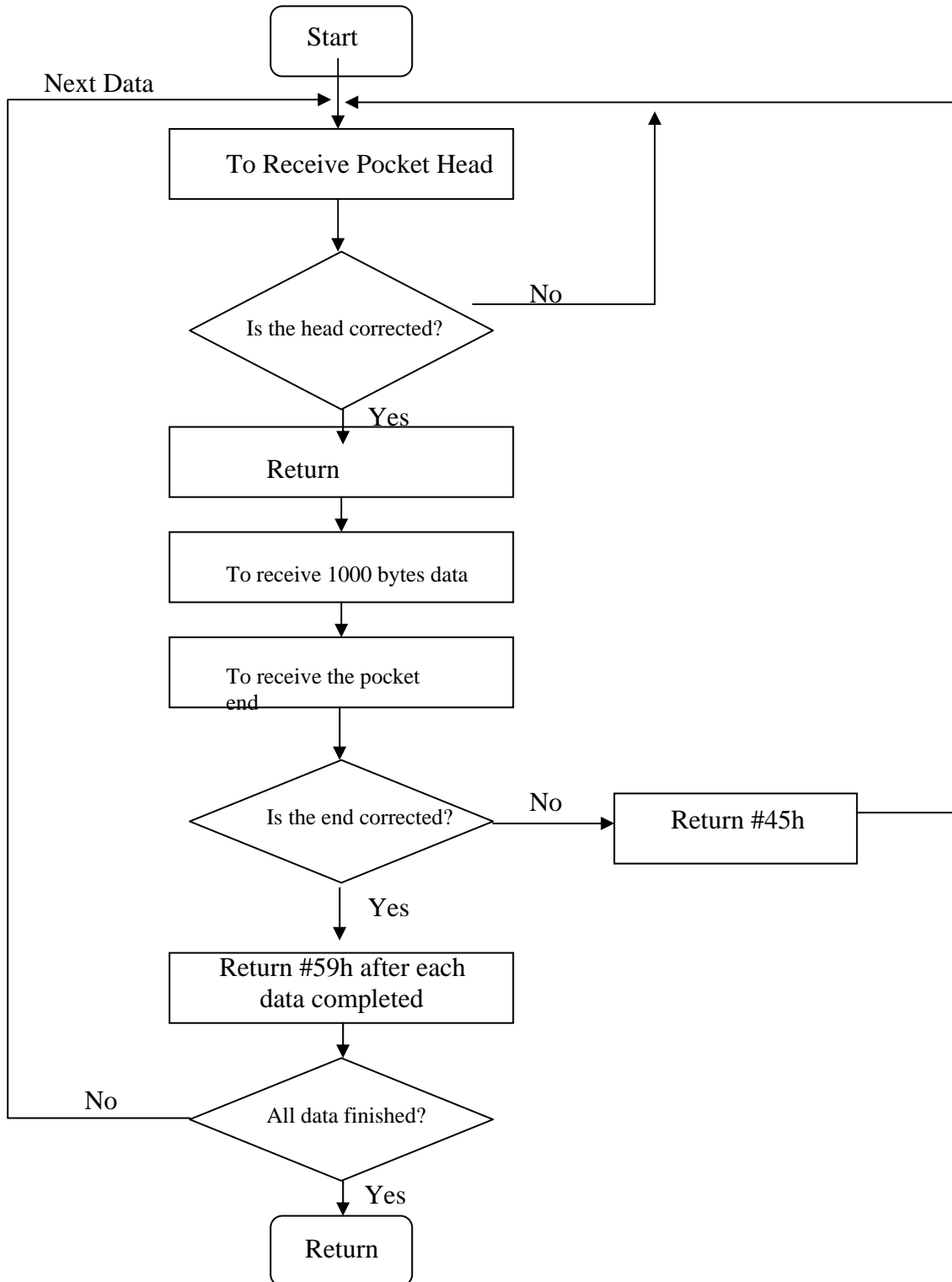


H	Packet header also serves as destination Sign identifier
1	Clock code (4FH)
2	The first two digits. E.g: 20XX (Year, month, day, week, month, minute, second to be BCD code)
3	The last two digits. E.g: XX03
4	Month
5	Day
6	Week
7	Tour
8	Minute
9	Second
10	the position to be displayed: X-axis ( unit: bytes)
11	the position to be displayed: Y-axis ( unit: bytes)
12	D0=0, to display with second D0=1, to display without second
13	Nil

**Structure of the Pocket Head, "h"**



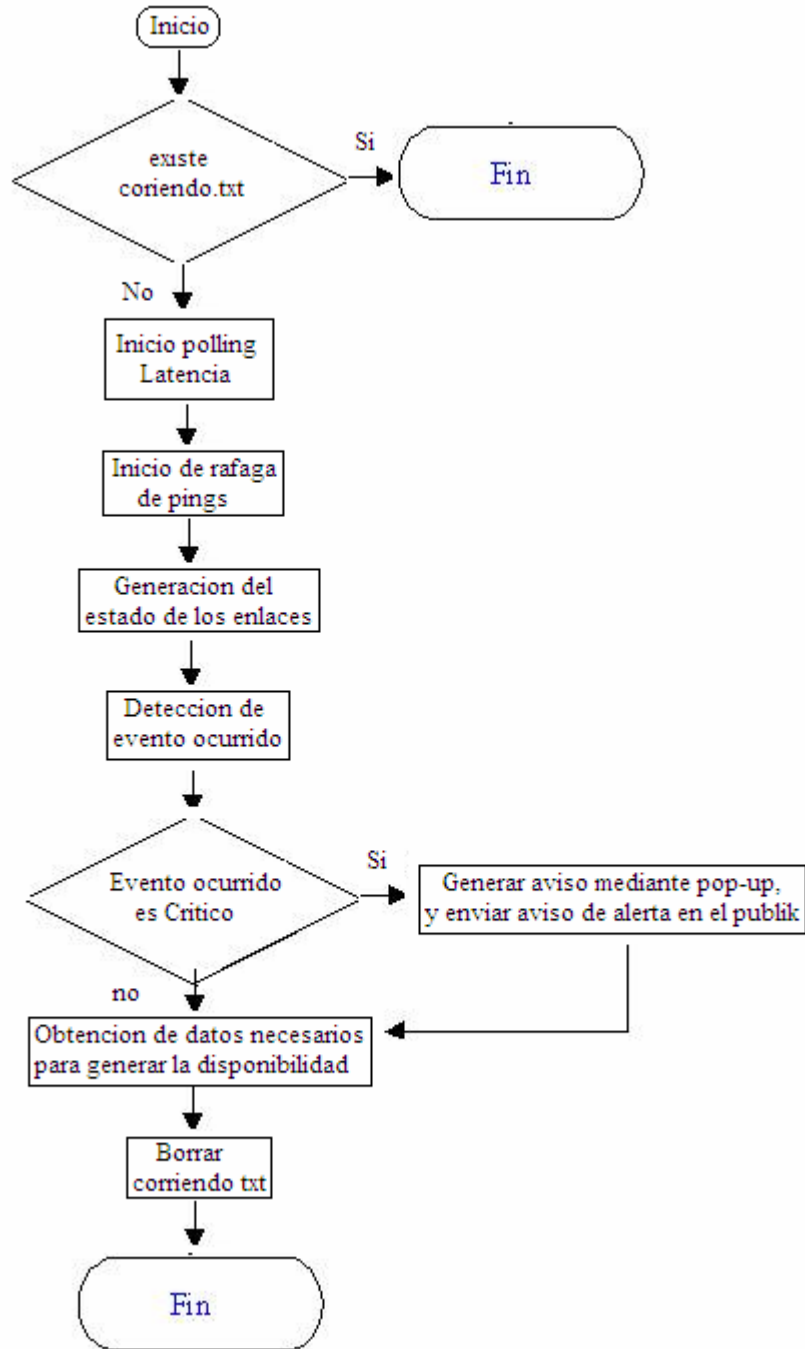
## Communication Parameters



## Diagrama de flujo de los scripts basicos utilizados en el aplicativo.

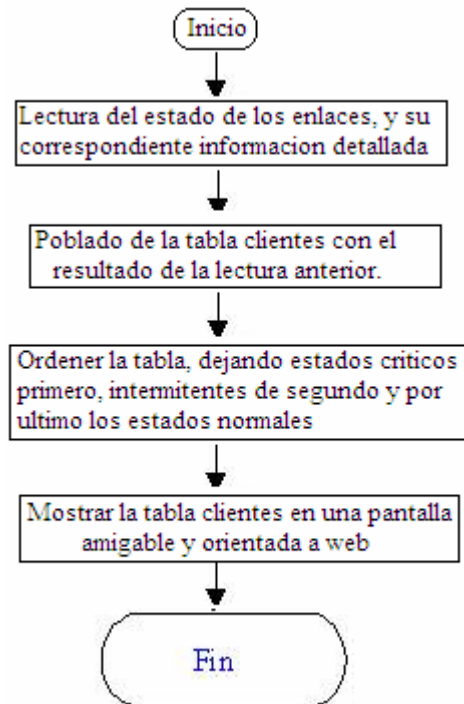
### Principal.bat

Figura. Muestra el diagrama de flujo para el script principal.bat

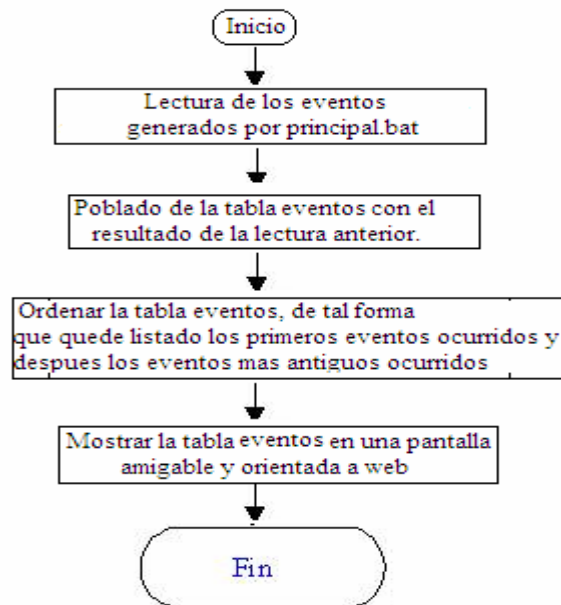


Como se puede observar en la figura anterior, este script como su nombre lo indica es el script principal, el cual esta corriendo en background para asi generar en archivos de texto las informaciones necesarias de la red, para posteriormente mostrarla de manera amigable via web mediante php.

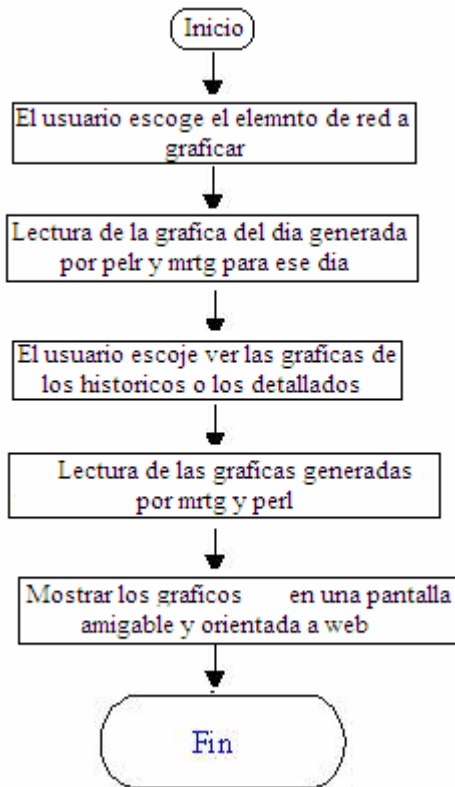
### Faultmanagment.php



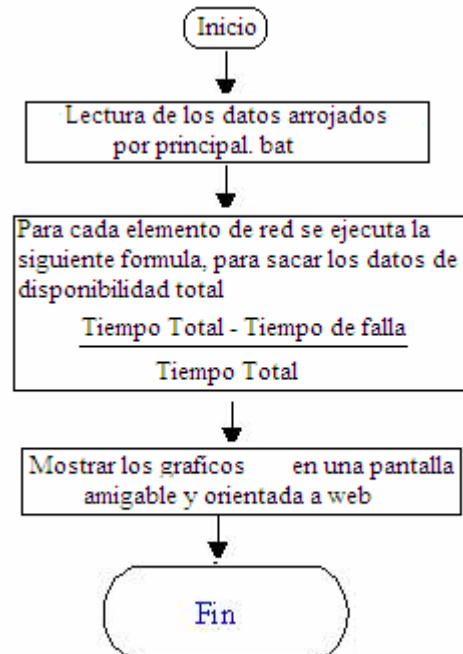
### Eventos.php



### Trafico1.php



### Disponibilidad3.php



## Latencia.php

