

**UNIVERSIDAD TÉCNICA DE AMBATO**

**FACULTAD DE INGENIERÍA EN SISTEMAS**

**“GESTIÓN DE REDES DE UN CENTRO DE COMPUTO UTILIZANDO  
PROTOCOLO SNMP/RMON”**

**Autores: Edith Susana Acuña García**

**Verónica Matilde Caicedo Urresta**

**Director: Ing. Msc. Hernando Buenaño**

**Tesis de grado, previa a la obtención del título de Ingeniero en Sistemas**

**Ambato – Ecuador**

**Junio/2005**

## **DEDICATORIA**

### **Edith**

Dedico esta investigación con todo mi amor a mi hijo Mateo, quien es mi fuente de inspiración y razón de vivir. Al que deseo sea un ejemplo para tantos logros que él pueda realizar.

Y a mis padres Francisco y Susana. Gracias por haber inculcado en mí siempre un espíritu de superación.

### **Verónica**

Hago un reconocimiento muy especial y dedico esta tesis a todas aquellas personas que de alguna forma estuvieron a mi lado con su apoyo, comprensión y amor.

A mis padres, quienes compartieron sus vidas conmigo forjando mi educación con valores y conocimientos. Nunca podré pagar tanta riqueza recibida a lo largo de mi vida y siempre estaré profundamente agradecida.

## **AGRADECIMIENTOS**

### **Verónica**

En primer lugar quiero agradecer a mi compañera de Tesis Edith, por toda la coordinación en equipo para las incontables horas de trabajo Gracias por tu amistad y ayuda que no tiene precio.

Todo esto nunca hubiese sido posible sin el amparo incondicional de mi familia, mis padres y mis hermanos Esto es también vuestro premio.

### **Edith**

A ti amiga por haber tenido el privilegio de realizar esta tesis y culminar juntas nuestra carrera.

A mi Jefatura Ing. Preslav Amores por el apoyo incondicional y por su amistad.

### **Nuestro**

Un sincero agradecimiento a nuestro Director Ing. Hernando Buenaño y a nuestro Asesor Ing. David Guevara, por todo el tiempo que nos han dedicado, por el respaldo y la amistad. Además no podríamos olvidar a nuestra querida Facultad, Ingeniería en Sistemas, a todo su personal académico y administrativo, gracias por compartir sus conocimientos y enseñanzas.

Debemos un especial reconocimiento a las empresas en la cuales trabajamos, su apoyo fue incondicional para poder realizar las prácticas necesarias

## **DECLARACIÓN, AUTENTICIDAD Y RESPONSABILIDAD**

Nosotros, Edith Susana Acuña García con C.I. 1803012762 - 7, y Verónica Matilde Caicedo Urresta con C.I. 010305408-6 declaramos que:

La investigación enmarcada en el desarrollo de la presente Tesis de Grado, es absolutamente original, auténtica y personal. En tal virtud, declaramos que el contenido, efectos legales y académicos que se desprenden del trabajo son y serán de nuestra exclusiva responsabilidad legal y académica.

-----  
**Edith S. Acuña G.**

-----  
**Verónica M. Caicedo U.**

## INDICE

|                                                            |    |
|------------------------------------------------------------|----|
| DEDICATORIA .....                                          | 2  |
| AGRADECIMIENTOS .....                                      | 3  |
| DECLARACIÓN, AUTENTICIDAD Y RESPONSABILIDAD .....          | 4  |
| INDICE .....                                               | 5  |
| 1.1 PLANTEAMIENTO DEL PROBLEMA .....                       | 22 |
| 1.2 JUSTIFICACIÓN .....                                    | 24 |
| 1.3 OBJETIVOS .....                                        | 26 |
| 1.3.1 Objetivos General.....                               | 26 |
| 1.3.2 Objetivos Específicos.....                           | 26 |
| 1.4 HIPÓTESIS.....                                         | 26 |
| 1.5 MÉTODOS Y TÉCNICAS.....                                | 27 |
| 1.6 RECURSOS.....                                          | 27 |
| 2 CAPITULO II: INTRODUCCIÓN A LOS ESTÁNDARES DE GESTIÓN DE |    |
| REDES EN CENTROS DE CÓMPUTO.....                           | 29 |
| 2.1 CENTRO DE CÓMPUTO.....                                 | 29 |
| 2.2 OBJETIVO.....                                          | 29 |
| 2.3 NIVELES DE PLANEACION .....                            | 30 |
| 2.4 POLITICAS .....                                        | 30 |
| 2.5 EMPRESAS QUE UTILIZAN GESTION EN REDES EN CENTROS      |    |
| DE COMPUTO.....                                            | 33 |
| 2.6 PROBLEMAS FRECUENTES EN LA GESTION DE REDES.....       | 36 |
| 2.7 ESTADÍSTICAS Y NIVELES DE SERVICIOS .....              | 39 |
| 2.7.1 EMPRESA DE CARRIER COMUNICACIONES .....              | 40 |
| 2.7.2 EMPRESA FINANCIERA .....                             | 42 |
| 2.7.3 EMPRESA DE IMPORTACIÓN Y EXPORTACIÓN.....            | 44 |
| 2.8 DEFINICIÓN DE GESTIÓN DE REDES .....                   | 47 |
| 2.9 INTRODUCCIÓN A LA GESTIÓN DE REDES.....                | 47 |

|          |                                                                                                       |    |
|----------|-------------------------------------------------------------------------------------------------------|----|
| 2.10     | EVOLUCIÓN DE LA GESTIÓN DE REDES.....                                                                 | 49 |
| 2.11     | OBJETIVOS DE LA GESTIÓN DE RED .....                                                                  | 51 |
| 2.12     | FUNCIONES DE GESTIÓN DE RED. ....                                                                     | 51 |
| 2.12.1   | Monitorización. ....                                                                                  | 51 |
| 2.12.1.1 | Objetivos de la Monitorización de red .....                                                           | 51 |
| 2.12.1.2 | Arquitectura funcional de monitorización. ....                                                        | 52 |
| 2.12.2   | Control. ....                                                                                         | 52 |
| 2.13     | ESTÁNDARES DE GESTIÓN DE REDES. ....                                                                  | 53 |
| 2.13.1   | SNMP (Simple Network Management Protocol, Protocolo Simple de Gestión de Red).....                    | 53 |
| 2.13.2   | CMIP (Common Management Information Protocol, Protocolo Común de Gestión de Información).....         | 54 |
| 2.13.2.1 | Protocolos de Aplicación en CMIP.....                                                                 | 56 |
| 2.14     | MODELOS DE GESTIÓN DE RED.....                                                                        | 58 |
| 2.14.1   | Modelo Gestión en Internet.....                                                                       | 59 |
| 2.14.2   | Modelo de Gestión de red OSI.....                                                                     | 60 |
| 2.14.2.1 | Gestión de Fallos.....                                                                                | 60 |
| 2.14.2.2 | Gestión de costes.....                                                                                | 61 |
| 2.14.2.3 | Gestión de Configuración. ....                                                                        | 61 |
| 2.14.2.4 | Gestión de prestaciones.....                                                                          | 62 |
| 2.14.2.5 | Gestión de seguridad. ....                                                                            | 63 |
| 2.14.3   | Arquitectura TMN (Telecommunications Management Network, Redes de Gestión de Telecomunicaciones)..... | 64 |
| 2.15     | SISTEMAS DE GESTIÓN DE RED.....                                                                       | 66 |
| 2.16     | PLATAFORMAS DE GESTIÓN DE RED.....                                                                    | 66 |
| 2.17     | MIB ( Management Information Base, Base de Gestión de Información).                                   | 68 |

|           |                                                                                                                  |    |
|-----------|------------------------------------------------------------------------------------------------------------------|----|
| 3         | CAPITULO III: PROTOCOLO SNMP (Simple Network Managenement Protocol,<br>Protocolo Simple de Gestión de Red) ..... | 74 |
| 3.1       | SNMP CONCEPTO .....                                                                                              | 74 |
| 3.2       | INTRODUCCIÓN .....                                                                                               | 74 |
| 3.3       | EVOLUCIÓN .....                                                                                                  | 78 |
| 3.3.1     | SNMPv1 .....                                                                                                     | 78 |
| 3.3.1.1   | Información de Gestión Estructurada.....                                                                         | 79 |
| 3.3.1.1.1 | SNMPv1 y tipos de datos ASN.1 .....                                                                              | 80 |
| 3.3.1.1.2 | SNMPv1 y tipos de datos SMI Específicos .....                                                                    | 80 |
| 3.3.1.1.3 | Tablas del MIB del SNMP .....                                                                                    | 81 |
| 3.3.1.2   | Operaciones Del Protocolo SNMPv1.....                                                                            | 82 |
| 3.3.2     | SNMPv2 .....                                                                                                     | 83 |
| 3.3.2.1   | Mejoras en SNMPv2 .....                                                                                          | 83 |
| 3.3.3     | SNMPv3.....                                                                                                      | 84 |
| 3.4       | FUNCIONAMIENTO SNMP.....                                                                                         | 85 |
| 3.5       | COMPONENTES BÁSICOS DEL SNMP.....                                                                                | 87 |
| 3.6       | COMANDOS BÁSICOS DEL SNMP .....                                                                                  | 89 |
| 3.7       | CONSTRUCCIÓN DEL MENSAJE DEL SNMP .....                                                                          | 90 |
| 3.8       | ARQUITECTURA.....                                                                                                | 92 |
| 3.9       | ELEMENTOS DE LA ARQUITECTURA SNMP .....                                                                          | 95 |
| 3.10      | BASE CON INFORMACIÓN DE GESTIÓN .....                                                                            | 95 |
| 3.10.1    | Nodos administrados.....                                                                                         | 96 |
| 3.10.2    | Agente Apoderado (o proxy) .....                                                                                 | 96 |
| 3.10.3    | Consola de administración .....                                                                                  | 97 |
| 3.11      | PRIMITIVAS .....                                                                                                 | 98 |
| 3.11.1    | Get Request .....                                                                                                | 98 |
| 3.11.2    | Get Next Request .....                                                                                           | 99 |
| 3.11.3    | Get Bulk Request .....                                                                                           | 99 |

|        |                                                                     |     |
|--------|---------------------------------------------------------------------|-----|
| 3.11.4 | Set Request.....                                                    | 99  |
| 3.11.5 | Set next request .....                                              | 99  |
| 3.11.6 | Get Response.....                                                   | 100 |
| 3.11.7 | Trap .....                                                          | 100 |
| 3.11.8 | Inform Request.....                                                 | 100 |
| 3.12   | MONITORIZACIÓN INTELIGENTE.....                                     | 100 |
| 3.13   | SNMP Y CONGESTIÓN .....                                             | 101 |
| 3.14   | VENTAJA PRINCIPAL DE SNMP .....                                     | 101 |
| 4      | CAPITULO VI: RMON (Remote Network Monitor, Monitor de Red Remoto) . | 103 |
| 4.1    | CONCEPTO.....                                                       | 103 |
| 4.2    | INTRODUCCION .....                                                  | 103 |
| 4.3    | EVOLUCIÓN. ....                                                     | 106 |
| 4.4    | RMON1.....                                                          | 107 |
| 4.4.1  | Características .....                                               | 107 |
| 4.4.2  | Configuración.....                                                  | 109 |
| 4.4.3  | Ventajas dominantes .....                                           | 110 |
| 4.4.4  | Ejecución de Comandos Mediante la MIB RMON .....                    | 110 |
| 4.4.5  | Gestores Múltiples .....                                            | 111 |
| 4.5    | RMON 2.....                                                         | 113 |
| 4.5.1  | Beneficios.....                                                     | 113 |
| 4.5.2  | Visibilidad de la capa de red mediante RMON2 .....                  | 114 |
| 4.5.3  | Visibilidad de la capa de aplicación mediante RMON2 .....           | 115 |

|         |                                                                        |     |
|---------|------------------------------------------------------------------------|-----|
| 4.5.4   | Características .....                                                  | 115 |
| 4.5.5   | Una desventaja de las puntas de prueba de RMON1 .....                  | 116 |
| 4.6     | RMON MIB .....                                                         | 117 |
| 4.6.1   | Características. ....                                                  | 118 |
| 4.7     | CARACTERISTICAS GENERALES .....                                        | 119 |
| 4.8     | ADMINISTRACIÓN DE RED CON RMON .....                                   | 120 |
| 4.9     | ESCENARIOS PARA MONITOREO REMOTO DE REDES.....                         | 121 |
| 4.10    | RMON PARA ETHETNET.....                                                | 122 |
| 4.11    | RMON PARA TOKEN RING (RFC 1513) –GRUPO TOKENRING.....                  | 124 |
| 4.12    | GRUPOS DE RMON.....                                                    | 125 |
| 4.13    | COMO TRABAJA RMON? .....                                               | 126 |
| 5       | CAPITULO IV: SELECCIÓN Y APRENDIZAJE DE LA MEJOR                       |     |
|         | HERRAMIENTA DE MONITOREO .....                                         | 129 |
| 5.1     | PATROL EXPRESS .....                                                   | 129 |
| 5.1.1   | Introducción .....                                                     | 129 |
| 5.1.2   | Ventajas principales .....                                             | 129 |
| 5.1.3   | Características BMC software.....                                      | 130 |
| 5.1.4   | Beneficios de Patrol Express.....                                      | 130 |
| 5.1.4.1 | Monitoreo remoto de los elementos de la infraestructura.....           | 130 |
| 5.1.4.2 | Umbral de alertas y políticas de notificación.....                     | 131 |
| 5.1.4.3 | Medir los objetivos de nivel de servicio definidos por el usuario..... | 131 |
| 5.1.4.4 | Monitoreo de transacciones Web.....                                    | 131 |
| 5.1.4.5 | Acceso Web centralizado a toda la organización.....                    | 132 |
| 5.2     | SGA - SISTEMA DE GESTIÓN DE ALARMAS .....                              | 133 |
| 5.2.1   | Introducción .....                                                     | 133 |
| 5.2.2   | Arquitectura.....                                                      | 133 |
| 5.2.3   | Arquitectura del traductor de alarmas .....                            | 135 |

|         |                                               |     |
|---------|-----------------------------------------------|-----|
| 5.3     | ENTERASYS NETWORKS- NETSIGHT MANAGER .....    | 136 |
| 5.3.1   | Introducción .....                            | 136 |
| 5.3.2   | Características .....                         | 137 |
| 5.3.3   | Arquitectura.....                             | 139 |
| 5.4     | OBSERVER.....                                 | 140 |
| 5.4.1   | Concepto .....                                | 140 |
| 5.4.2   | Introducción .....                            | 140 |
| 5.4.3   | Versiones.....                                | 141 |
| 5.4.3.1 | Observer .....                                | 141 |
| 5.4.3.2 | Expert Observer .....                         | 141 |
| 5.4.3.3 | Observer Suite.....                           | 142 |
| 5.4.3.4 | Examinadores (Probes) .....                   | 142 |
| 5.4.4   | Introducción Observer.....                    | 142 |
| 5.4.5   | Examinadores (Probes) / Advanced Y Rmon ..... | 144 |
| 5.4.6   | Requerimientos .....                          | 145 |
| 5.4.6.1 | Sistemas operativos.....                      | 145 |
| 5.4.6.2 | Protocolo de red .....                        | 146 |
| 5.4.6.3 | Requisitos del hardware .....                 | 146 |
| 5.5     | HP OPENVIEW.....                              | 146 |
| 5.5.1   | Concepto .....                                | 146 |
| 5.5.2   | Características .....                         | 147 |
| 5.5.3   | Personalización .....                         | 152 |
| 5.5.4   | Configuración.....                            | 153 |

|           |                                                                                                          |     |
|-----------|----------------------------------------------------------------------------------------------------------|-----|
| 5.5.5     | Conclusiones .....                                                                                       | 155 |
| 5.6       | SOLARWINDS .....                                                                                         | 156 |
| 5.6.1     | Introducción .....                                                                                       | 156 |
| 5.6.2     | Características .....                                                                                    | 156 |
| 5.7       | PATROL DASHBOARD .....                                                                                   | 158 |
| 6         | CAPITULO VI: HERRAMIENTAS DE MONITOREO.....                                                              | 160 |
| 6.1       | SOLARWINDS .....                                                                                         | 160 |
| 6.1.1     | Introducción .....                                                                                       | 160 |
| 6.1.2     | Descripción .....                                                                                        | 161 |
| 6.1.3     | Requerimientos del Sistema.....                                                                          | 162 |
| 6.1.4     | Versiones y Costos.....                                                                                  | 162 |
| 6.1.5     | Características .....                                                                                    | 163 |
| 6.1.5.1   | Network Performance Monitoring Tools (Herramientas para<br>Supervisar el Funcionamiento de la Red) ..... | 163 |
| 6.1.5.1.1 | Network Performance Monitor (Monitor del Funcionamiento de la<br>red) .....                              | 164 |
| 6.1.5.1.2 | SNMP Graph (Gráfico SNMP ) .....                                                                         | 167 |
| 6.1.5.1.3 | Advanced CPU Load (Carga Avanzada del CPU).....                                                          | 168 |
| 6.1.5.1.4 | CPU Gauges (Medidor del CPU).....                                                                        | 168 |
| 6.1.5.2   | Network Discovery Tools (Descubrimiento de la Red).....                                                  | 169 |
| 6.1.5.2.1 | Switch Port Mapper (Mapeo del Puerto del Interruptor) .....                                              | 170 |
| 6.1.5.2.2 | IP Network Browser ( Buscador de Red IP) .....                                                           | 170 |
| 6.1.5.3   | Tools For Cisco Routers (Herramientas para Redes Cisco) .....                                            | 176 |
| 6.1.5.3.1 | Advanced Router CPU Load (Carga Avanzada del CPU Router)<br>.....                                        | 177 |
| 6.1.5.3.2 | Config Downloaded (Descarga de Configuración).....                                                       | 179 |
| 6.1.5.3.3 | Config Uploader (Carga de Configuración).....                                                            | 179 |
| 6.1.5.3.4 | Config Editor/Viewer (Vista/Edición Configuración).....                                                  | 180 |
| 6.1.5.3.5 | Compare Running vs Startup Configs (Comparación de<br>Configuración Inicial vs Ejecución).....           | 182 |

|           |                                                                                                                                                                                                             |     |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 6.1.5.3.6 | Proxy Ping (Apoderado Ping ) .....                                                                                                                                                                          | 182 |
| 6.1.5.3.7 | Router Password Decryption (Desencriptar Clave del router)....                                                                                                                                              | 184 |
| 6.1.5.3.8 | CPU Gauge (Medidas CPU) .....                                                                                                                                                                               | 184 |
| 6.1.5.3.9 | Router Security Check (Chequeo Seguridad Router) .....                                                                                                                                                      | 185 |
| 6.1.5.4   | Fault Monitoring Tools (Herramienta que Supervisa Fallas) .....                                                                                                                                             | 186 |
| 6.1.5.4.1 | Network Monitor (Monitor de Red).....                                                                                                                                                                       | 187 |
| 6.1.5.4.2 | SysLog Server (Servidor SysLog) .....                                                                                                                                                                       | 188 |
| 6.1.5.4.3 | Watch it; (Miralo;).....                                                                                                                                                                                    | 189 |
| 6.1.5.5   | MIB Browser Tools (Herramientas MIB).....                                                                                                                                                                   | 190 |
| 6.1.5.5.1 | MIB Browser (Buscador MIB) .....                                                                                                                                                                            | 190 |
| 6.1.5.5.2 | MIB Viewer (Vista MIB).....                                                                                                                                                                                 | 191 |
| 6.1.5.5.3 | MIB Walk (Camino MIB).....                                                                                                                                                                                  | 192 |
| 6.1.5.5.4 | Update System MIB's (Actualización de Sistemas MIB).....                                                                                                                                                    | 193 |
| 6.1.5.6   | Security And Attack Tools (Herramientas de Seguridad y Ataque).194                                                                                                                                          |     |
| 6.1.5.6.1 | SNMP Brute Force Attack (Ataque SNMP) .....                                                                                                                                                                 | 194 |
| 6.1.5.6.2 | SNMP Dictionary Attack (Ataque Diccionario SNMP).....                                                                                                                                                       | 195 |
| 6.1.5.6.3 | Remote TCP Reset (Reseteo TCP Remoto).....                                                                                                                                                                  | 196 |
| 6.1.5.7   | Ping And Diagnostic Tools (Herramientas para Diagnostico y Ping )                                                                                                                                           | 198 |
| 6.1.5.7.1 | Trace Route (Router Ruta).....                                                                                                                                                                              | 198 |
| 6.1.5.7.2 | TFTP Server (Trivial File Transfer Protocol , Servidor Versión FTP)                                                                                                                                         | 199 |
| 6.1.5.7.3 | Wake – On-LAN (Encender en LAN) .....                                                                                                                                                                       | 200 |
| 6.1.5.7.4 | PING .....                                                                                                                                                                                                  | 200 |
| 6.1.5.7.5 | WAN Killer (Asesino LAN) .....                                                                                                                                                                              | 201 |
| 6.1.5.8   | IP Address Management Tools (Herramientas de Gestión de Direcciones) .....                                                                                                                                  | 202 |
| 6.1.5.8.1 | IP Address Management ( Gestión de Dirección IP).....                                                                                                                                                       | 202 |
| 6.1.5.8.2 | DHCP Scope Monitor (Monitor DHCP).....                                                                                                                                                                      | 203 |
| 6.1.5.8.3 | Advanced Subnet Calculador (Calculador de Sub Red Avanzado)                                                                                                                                                 | 204 |
| 6.1.5.8.4 | DNS Audit. (Auditoria DNS).....                                                                                                                                                                             | 205 |
| 6.1.5.8.5 | DNS/ Who Is Resolver (Cómo Resolver DNS).....                                                                                                                                                               | 205 |
|           | DNS Resolver busca y crea un informe detallado en el Nombre del Dominio, URL, IP Address, Dirección de la Red o Dirección del correo electrónico. Incluso puede definir su propio quién es el servidor..... | 205 |
| 6.1.5.9   | Miscellaneous Tools (Herramientas Misceláneas).....                                                                                                                                                         | 206 |
| 6.1.5.9.1 | TFTP Server (Servidor TFTP) .....                                                                                                                                                                           | 207 |
| 6.1.5.9.2 | Update System MIB's (Actualización de Sistemas MIB).....                                                                                                                                                    | 207 |
| 6.2       | PATROL DASHBOARD .....                                                                                                                                                                                      | 208 |
| 6.2.1     | Introducción .....                                                                                                                                                                                          | 208 |
| 6.2.2     | Arquitectura.....                                                                                                                                                                                           | 208 |

|          |                                                  |     |
|----------|--------------------------------------------------|-----|
| 6.2.3    | Características Dominantes.....                  | 210 |
| 6.2.4    | Conexión para un cliente Patrol Dashboard.....   | 211 |
| 6.2.4.1  | Conexión para un servidor Patrol Dashboard ..... | 211 |
| 6.2.5    | Descripción de la Herramienta.....               | 212 |
| 6.2.6    | Estructura del Árbol .....                       | 212 |
| 6.2.7    | PROPIEDADES GLOBALES.....                        | 214 |
| 6.2.7.1  | Device (Dispositivo) .....                       | 215 |
| 6.2.7.2  | Interface (Interface).....                       | 215 |
| 6.2.7.3  | DLCI .....                                       | 216 |
| 6.2.7.4  | VP (Path Virtual) .....                          | 216 |
| 6.2.7.5  | VC (Canal Virtual).....                          | 216 |
| 6.2.7.6  | E1 Channel (Canal).....                          | 216 |
| 6.2.7.7  | CoS (Clase de Servicio) .....                    | 216 |
| 6.2.7.8  | ToS (Tipo de Servicio).....                      | 217 |
| 6.2.7.9  | Peer (Par).....                                  | 217 |
| 6.2.7.10 | Protocol Root (Raíz de protocolo) .....          | 217 |
| 6.2.8    | Propiedades del Dispositivo.....                 | 217 |
| 6.2.9    | Tipos de Indicadores d Límites (Thresholds)..... | 221 |
| 6.2.10   | Estableciendo Limites .....                      | 222 |
| 6.2.11   | Intervalos de Tiempo del Dispositivo .....       | 223 |
| 6.2.12   | Protocolos.....                                  | 224 |
| 6.2.13   | Perfiles.....                                    | 225 |
| 6.2.14   | Usuarios .....                                   | 226 |

|        |                                                       |     |
|--------|-------------------------------------------------------|-----|
| 6.2.15 | Reportes.....                                         | 227 |
| 6.2.16 | Network (Red).....                                    | 228 |
| 6.2.17 | Alertas y Notificaciones .....                        | 229 |
| 6.2.18 | Tiempo Real .....                                     | 231 |
| 6.2.19 | Alertas Escalables y Temporizador.....                | 234 |
| 6.3    | Cuadro Comparativo Patrol DashBoard y Solar Win ..... | 235 |
| 7      | CAPITULO VII .....                                    | 236 |
|        | CONCLUSIONES Y RECOMENDACIONES.....                   | 236 |
| 7.1    | Conclusiones .....                                    | 236 |
| 7.2    | Recomendaciones.....                                  | 237 |
| 8      | GLOSARIO DE TÉRMINOS.....                             | 239 |
|        | BIBLIOGRAFÍA .....                                    | 269 |
|        | ANEXOS .....                                          | 273 |

## INDICE DE GÁFICOS

|                                                        |     |
|--------------------------------------------------------|-----|
| Gráfico 1. Modelos de Gestión de Red.....              | 46  |
| Gráfico 2. Solicitud de la Estación al Agente.....     | 73  |
| Gráfico 3 Esquema de una Red Gestionada con SNMP.....  | 75  |
| Gráfico 4 Componentes de la Arquitectura de Red.....   | 82  |
| Gráfico 5. RMON1 y RMON 2 en capas del Modelo OSI..... | 95  |
| Gráfico 6. Estaciones de Administración y RMON.....    | 108 |
| Gráfico 7 Objetos RMON.....                            | 111 |
| Gráfico 8. Red de Consolas RMON.....                   | 115 |
| Gráfico 9. Funcionamiento del RMON.....                | 116 |
| Gráfico 10. Esquema de Patrol Express.....             | 120 |
| Gráfico 11. Interfaz de SGA .....                      | 122 |
| Gráfico 12. Arquitectura SGA.....                      | 123 |
| Gráfico 13. Consola de Monitoreo NetSight Manager..... | 126 |
| Gráfico 14. Tipos de Redes.....                        | 128 |
| Gráfico 15. Pantalla Principal Observer.....           | 131 |

|                                                                                   |     |
|-----------------------------------------------------------------------------------|-----|
| Gráfico 16. Instrumentos de Red Avanzados.....                                    | 132 |
| Gráfico 17. Instrumentos de Red ROMON.....                                        | 133 |
| Gráfico 18. Pantalla Principal de HP Open View.....                               | 135 |
| Gráfico 19. Categorías de Alarmas.....                                            | 137 |
| Gráfico 20. Buscador de Alarmas.....                                              | 137 |
| Gráfico 21. Vista de todas las Subredes conectadas al servidor.....               | 138 |
| Gráfico 22. Pantalla del segmento de Red.....                                     | 139 |
| Gráfico 23. Pantalla de Sub-mapas.....                                            | 140 |
| Gráfico 24 Pantalla de Interfaces.....                                            | 141 |
| Gráfico 25 Pantalla para Crear Objetos de la Red.....                             | 143 |
| Gráfico 26 Pantalla para Adicional Objetos.....                                   | 144 |
| Gráfico 27. Pantalla del Monitor de Funcionamiento de la Red .....                | 150 |
| Gráfico 28. Pantalla para Seleccionar una Interfase y Mostrar la Estadística..... | 151 |
| Gráfico 29. Pantalla del Gráfico SNMP (SMNP Graph).....                           | 152 |
| Gráfico 30. Pantalla de la Carga Avanzada del CPU.....                            | 153 |
| Gráfico 31. Pantalla Mediciones CPU (CPU Gauges).....                             | 154 |

|                                                                                 |     |
|---------------------------------------------------------------------------------|-----|
| Gráfico 32. Pantalla del Mapeo del Puerto Switch.....                           | 155 |
| Gráfico 33. Pantalla del Buscador de Red IP.....                                | 156 |
| Gráfico 34. Monitoreo de una Sub Red con el Sonar.....                          | 157 |
| Gráfico 35. Pantalla para Obtener la Dirección MAC.....                         | 158 |
| Gráfico 36. Auditoria DNS.....                                                  | 159 |
| Gráfico 37. Barrido SNMP.....                                                   | 163 |
| Gráfico 38. Lista de Subred.....                                                | 164 |
| Gráfico 39. Carga Avanzada del CPU Router1.....                                 | 165 |
| Gráfico 40. Carga Avanzada del CPU Router2.....                                 | 165 |
| Gráfico 41. Muestra de Impresión por Pantalla de la Carga del CPU Avanzada..... | 166 |
| Gráfico 42. Descarga de la Configuración.....                                   | 167 |
| Gráfico 43. Carga de la Configuración.....                                      | 168 |
| Gráfico 44. Pantalla Vista Edición y Configuración.....                         | 169 |
| Gráfico 45. Pantalla de Comparación de Configuración Inicial vs Ejecución.....  | 170 |
| Gráfico 46. Ping Apoderado.....                                                 | 171 |
| Gráfico 47. Icono Proxy Ping.....                                               | 171 |

|                                            |     |
|--------------------------------------------|-----|
| Gráfico 48. Desencriptar Clave Router..... | 172 |
| Gráfico 49. Medidas CPU.....               | 173 |
| Gráfico 50. Chequeo Seguridad Router.....  | 174 |
| Gráfico 51. Monitor de Red.....            | 176 |
| Gráfico 52. Pantalla Servidor SysLog.....  | 177 |
| Gráfico 53. Pantalla Miralol.....          | 178 |
| Gráfico 54. Buscador MIB.....              | 179 |
| Gráfico 55. Vista MIB.....                 | 180 |
| Gráfico 56. Camino MIB.....                | 181 |
| Gráfico 57. Actualización MIB.....         | 182 |
| Gráfico 58. Ataque SNMP.....               | 183 |
| Gráfico 59. Ataque Diccionario SNMP.....   | 184 |
| Gráfico 60. Reseteo TCP Remoto.....        | 185 |
| Gráfico 61. Pantalla Ruta del Router.....  | 187 |
| Gráfico 62. Encendido LAN.....             | 188 |
| Gráfico 63. Ping.....                      | 189 |

|                                                                   |     |
|-------------------------------------------------------------------|-----|
| Gráfico 64. Asesino LAN.....                                      | 190 |
| Gráfico 65. Gestión de Direcciones IP.....                        | 191 |
| Gráfico 66. Monitor DHCP.....                                     | 192 |
| Gráfico 67. Calculador Sub Red Avanzado.....                      | 193 |
| Gráfico 68. Calculador Sub red Avanzado y Clasificado.....        | 194 |
| Gráfico 69. Cómo resolver DNS.....                                | 195 |
| Gráfico 70. Servidor TFTP.....                                    | 196 |
| Gráfico 71. SNMP Data Collect and Export to a CIM Repository..... | 200 |
| Gráfico 72. Pantalla Principal PATROL Dashboard.....              | 203 |
| Gráfico 73. Estructura del árbol.....                             | 203 |
| Gráfico 74. Propiedades Globales (Global Properties).....         | 205 |
| Gráfico 75. Propiedades globales de un dispositivo.....           | 209 |
| Gráfico 76. Tipos de Indicadores.....                             | 212 |
| Gráfico 77. Indicadores de limites para Workload.....             | 213 |
| Gráfico 78. Intervalos de tiempo de dispositivos.....             | 215 |
| Gráfico 79. Protocolos que utiliza Patrol.....                    | 216 |

|                                                       |     |
|-------------------------------------------------------|-----|
| Gráfico 80. Perfiles de usuario.....                  | 217 |
| Gráfico 81. Usuarios de Patrol DashBoard.....         | 218 |
| Gráfico 82. Reportes de Alarmas.....                  | 219 |
| Gráfico 83. Red de Monitoreo.....                     | 220 |
| Gráfico 84. Ejemplo de Alertas y notificaciones.....  | 222 |
| Gráfico 85. Ejemplo de un informe en tiempo real..... | 223 |
| Gráfico 86. Ejemplo de dispositivos de una red.....   | 224 |

## INDICE DE TABLAS

|                                                                              |     |
|------------------------------------------------------------------------------|-----|
| Tabla 1.- Empresas que utilizan herramientas de monitoreo de red.....        | 35  |
| Tabla 2. Descripción de Problemas mas frecuentes en el monitoreo de red..... | 37  |
| Tabla 3.- Uptime mensual de nivel de servicio.....                           | 39  |
| Tabla 4.-Estadístico de niveles de servicio.....                             | 41  |
| Tabla 5. Funciones de los Grupos RMON.....                                   | 114 |
| Tabla 6. Requerimientos del Sistema1.....                                    | 150 |
| Tabla 7. Versiones SolarWinds vs. Costos.....                                | 151 |
| Tabla 8. Descripción de componentes principales.....                         | 203 |
| Tabla 9. Descripción de las propiedades de un dispositivo.....               | 209 |
| Tabla 10. Descripción de otras propiedades de un dispositivo.....            | 210 |
| Tabla 11. Descripción de Indicadores de límites para Workload.....           | 213 |

## **CAPITULO I: INTRODUCCION**

### **1.1 PLANTEAMIENTO DEL PROBLEMA**

Brindar servicios de excelencia para satisfacer las expectativas de los usuarios con relación a las tecnologías de la información y de telecomunicaciones, es una de las principales necesidades del mercado de hoy en día, desde ese punto de vista nos hemos enfocado para plantear la necesidad en la obtención de información de los servicios que oferta cada empresa; para establecer niveles de servicio óptimos.

Nuestro planteamiento esta dirigido a un grupo indispensable para la obtención de dicha información que son los centros de cómputo y la gestión de redes de los mismos.

Cada vez es más usual la implantación de una red (WAN) en las pequeñas y grandes empresas, de ahí la necesidad de solucionar y prevenir muchos de los problemas que pueden presentarse en la administración de la misma: cuellos de botella, sobrecarga de usuarios, intrusiones, caídas, etc.

El reto de mantener niveles de servicio óptimos demanda de las empresas un radical e inmediato cambio en la manera de monitorear sus servicios.

Por lo tanto es importante estar siempre informado de los datos que circulan por nuestro sistema mediante un estudio profundo en el conocimiento de las redes de ordenadores, especialmente en los aspectos de planificación, organización, gestión y seguridad.

Es importante para las empresas de la nueva era ofrecer una visión amplia y comprensible de las tecnologías y los estándares de gestión de red, así como permitir un conocimiento actualizado de esta área tecnológica.

La gestión de redes vista como el conjunto de estrategias, procesos, funciones y herramientas definidos para facilitar el aprovisionamiento, la operación, el mantenimiento y la administración de los servicios y redes de telecomunicaciones, se convierte en el mejor aliado para elevar el grado de satisfacción de los clientes y la rentabilidad de su negocio.

Es importante proporcionar una solución rápida y eficiente de cada uno de los enlaces monitoreados; en la cual se determine en forma interactiva el tipo de error, su localización exacta, y su causal para una pronta y eficaz solución.

Con lo planteado se pretende buscar un modelo de gestión de redes a través del protocolo SMNP (Simple Network Management Protocol, Protocolo Simple de Gestión de Red) y RMON (Remote Network Monitor, Monitor de Red Remota); que permita administrar y gestionar sistemas de redes informáticas llegando a afrontar cualquier tipo de problema con garantías de éxito.

## **1.2 JUSTIFICACIÓN**

A la hora de gestionar una red de comunicaciones de medio y gran tamaño, se encuentra la necesidad de contar con herramientas de gestión automatizadas, que permitan llevar un control continuo de todas las redes.

Este proceso consiste en la definición de alarmas e identificación automática de problemas que notifiquen al gestor de manera inmediata las desviaciones del comportamiento habitual de la red. De esta forma, se puede aislar el problema y actuar en consecuencia.

Por tanto en una red, es necesaria la monitorización precisa del tráfico en los periodos de congestión, que es cuando las herramientas sobre SNMP(Simple Network Management Protocol, Protocolo Simple de Gestión de Red) y RMON(Remote Network Monitor) muestran su vulnerabilidad por la posibilidad de pérdida de datos, esto significará proporcionar al usuario calidad y seguridad para un mejor rendimiento de la red en su trabajo diario.

Cuando hay problemas con la red, la única forma de identificar el problema era ejecutando comandos muy simples como el ping, el cual no brinda suficiente información para resolver rápidamente dichos problemas. SNMP, muestra una manera de administrar y supervisar las redes de cómputo para identificar y resolver problemas, así como para planear su crecimiento. Se encuentra implementado en la capa de aplicación y pertenece al grupo de protocolos de TCP/IP.

El diseño de SNMP es simple por lo que su implementación es sencilla en grandes redes y la información de gestión que se necesita intercambiar ocupa pocos recursos de la red. Además, permite al usuario elegir las variables que desea monitorizar.

SNMP en la actualidad es el sistema más extendido. La popularidad la ha conseguido al ser el único protocolo que existió en un principio y por ello casi todos los fabricantes de dispositivos como puentes y encaminadores diseñan sus productos para soportar SNMP.

RMON es otro estándar que define objetos actuales e históricos de control, permitiendo capturar la información en tiempo real a través de la red entera.

Se puede utilizar RMON para analizar y para vigilar datos del tráfico de la red dentro de segmentos alejados de la LAN. Esto permite que detecte, aíse, diagnostique, y señale problemas potenciales y reales de la red antes de que se extiendan a las situaciones de crisis.

RMON permite instalar las historias automáticamente, que el agente de RMON recoge durante todo el tiempo, proporcionando datos en la estadística básica.

RMON automatiza esta colección de datos y proporciona a otros datos del proceso las hojas de operación (planning), el proceso es más fácil y el resultado más exacto.

## **1.3 OBJETIVOS**

### **1.3.1 Objetivos General**

- Estudiar las alternativas tecnológicas disponibles para la gestión de redes, enfocado al protocolo SNMP/RMON hasta el estudio de las herramientas existentes para implementar en la práctica las ideas de los mismos.

### **1.3.2 Objetivos Específicos**

- Estudiar el protocolo SNMP (Simple Network Management Protocol)
- Estudiar al RMON (Remote Network Monitor, Monitor de Red Remota)
- Desarrollar un caso de estudio en el que se aplique la óptima utilización del protocolo SNMP y RMON

## **1.4 HIPÓTESIS**

El estudio de SNMP/RMON proporcionará la mejor alternativa tecnológica para el monitoreo de una red.

## **1.5 MÉTODOS Y TÉCNICAS**

Los diferentes métodos y técnicas que se van a utilizar son parte de la investigación para el desarrollo del estudio planteado, además se utilizará la investigación bibliográfica, experimental y de campo.

La metodología bibliográfica se basa fundamentalmente en libros y documentación obtenida mediante Internet, documentación de las empresas evaluadas.

Para la experimental nos hemos ayudado de la instalación de las herramientas evaluadas en centros de cómputo de una institución financiera y una importadora y de técnicas de observación y experimentación.

La de campo la hemos hecho a través de varias entrevistas y encuestas informales que se han podido establecer a las jefaturas de las áreas de sistemas y centro de cómputo evaluados.

Es importante señalar la necesidad de recopilar información a través de la metodología de trabajo.

## **1.6 RECURSOS**

Ha sido necesario obtener Demos de las herramientas evaluadas así como nuevas licencias para ampliaciones de los triales.

Internet para establecer empresas proveedoras de software de monitoreo en Ecuador así como las ultimas tendencias y requerimientos del mercado en la gestión de red de los centros de computo.

## **2 CAPITULO II: INTRODUCCIÓN A LOS ESTÁNDARES DE GESTIÓN DE REDES EN CENTROS DE CÓMPUTO**

### **2.1 CENTRO DE CÓMPUTO**

Es el encargado de generar un soporte técnico en la operación de hardware y software, administrar recursos tecnológicos y físicos, solucionar solicitudes de los usuarios sobre problemas de hardware y software, operación de equipos, información y monitoreo.

Un centro de cómputo en su esencia es el departamento desde el cual se manejan el procesamiento de información así como el control y monitoreo de cada uno de los servicios que presta la institución.

También el implementar la mejor opción en la adquisición de nuevo hardware y software que se adapte a las necesidades y crecimiento de la empresa sin necesidad de gastar más dinero del necesario y presupuestado.

La administración de un centro de cómputo se define como el proceso de crear, diseñar y mantener un ambiente en el que las personas al laborar o trabajar en grupos, alcancen con eficiencia metas seleccionadas.

### **2.2 OBJETIVO**

Los principales objetivos de un centro de cómputo son:

- Concentrar el procesamiento de datos e información de una manera sistematizada y automática. Así como verificar que el software y hardware, funcionen correctamente, a través de un monitoreo y emitir soluciones técnicas y operacionales para su mejor rendimiento.
- Prestar servicios a diferentes áreas de una organización ya sea dentro de la misma empresa, tales como: producción, control de operaciones, captura de datos, programación, dibujo, biblioteca, etc. Los diversos servicios que puede prestar un centro de cómputo, pueden dividirse en departamentos o áreas específicas de trabajo.

### **2.3 NIVELES DE PLANEACION**

La planeación operativa de un centro de cómputo es muy importante; pues consiste en realizar un detallado análisis de necesidades de la empresa y definir en base a estas necesidades una plataforma tecnológica con una infraestructura en hardware, software, personal operativo, etc. que soporte las operaciones de la empresa y se utilice como el medio de procesamiento de información.

### **2.4 POLITICAS**

Para establecer las políticas de un centro de cómputo, dependerá del tipo de empresa en la cual este funcionando, sin embargo se mencionan a continuación algunas políticas aplicadas a la mayoría:

El espacio físico disponible, debe ser el adecuado con sus respectivas instalaciones de suministro eléctrico, acondicionamiento térmico, elementos de seguridad disponibles, la altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc,

El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y evitar la incidencia directa del sol sobre los equipos.

Los equipos de aire acondicionado deben cumplir con las normas y estándares de medición que se determinan según el espacio y # de equipos que posea el centro de computo.

El sistema contra incendios es muy importante, teniendo en cuenta que los materiales sean incombustibles (pintura de las paredes, suelo, techo, mesas, estanterías, etc.). También se toma en cuenta la protección contra inundaciones y otros peligros físicos que puedan afectar a la instalación.

El suministro eléctrico a un Centro de Cómputo, y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias, con elementos de

protección y seguridad específicos y en muchos casos con sistemas de alimentación ininterrumpida (equipos electrógenos, instalación de baterías, etc.).

Mantener documentada toda la información solicitada al centro de cómputo que fundamente la realización de cualquier procedimiento.

La seguridad es sin duda una de las principales normativas a cumplirse, en cuanto a:

- Restricciones de acceso al área de equipos y operación según políticas internas, estructuras organizacionales y funcionales de la institución.
- El uso de claves de acceso deben estar estructuradas en base a la asignación de tareas y apegarse a las normativas para el uso de las mismas.
- Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la empresa y se usarán exclusivamente para actividades relacionadas con la misma.

Mantener actualizado en un documento activo las normas, políticas y procedimientos que posee el centro de cómputo, para el caso se cambio de personal como ejemplo.

El centro de cómputo no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

Nadie puede ver, copiar, alterar o destruir la información de un usuario sin el consentimiento explícito del afectado.

No se permite interferir o entorpecer las actividades de los demás usuarios por cualquier medio o evento que no haya sido solicitado expresamente por los mismos.

## **2.5 EMPRESAS QUE UTILIZAN GESTION EN REDES EN CENTROS DE COMPUTO**

Para poder determinar a que tipo de empresas estaría dirigida esta investigación las hemos clasificado por grupos de acuerdo al tipo de servicios que brindan y tamaño, a la vez se presentan ejemplos de las mismas y hemos recopilado información estadística para el desarrollo de este capítulo.

Normalmente este departamento solo existe en empresas que manejan gran cantidad de información ó dinero ya que el costo de un departamento de estos es muy alto. La inversión en equipos de cómputo, software y servicios; demandan sacar el mayor beneficio a fin de hacer rentable la infraestructura.

Los administradores requieren conocer todos los aspectos del entorno técnico-administrativo, mantener actualizados sus conocimientos en los nuevos desarrollos tecnológicos disponibles en el mercado, así como adquirir una visión de la tendencia al futuro de dichos centros, de ahí la necesidad de información a través de herramientas que monitoreen la calidad de servicio.

Por ello determinaríamos en primer lugar que principalmente la tendrían:

- Empresas globales
- Medianas empresas
- Instituciones gubernamentales.
- Empresas que requieren ejecutar transacciones más rápidas de base de datos o soportar una mayor cantidad de usuarios.
- Clientes que necesitan un rápido rendimiento
- Segmentos industriales con grandes requerimientos de cómputo para crear aplicaciones.

En conclusión toda empresa que posea más de una conexión WAN necesitara herramientas de monitoreo para la red. Más aún empresas que provean servicios de comunicación como se detalla en la tabla siguiente:

|                     |                                  |
|---------------------|----------------------------------|
| <b>Dirigidas a:</b> | <b>Empresas de nuestro medio</b> |
|---------------------|----------------------------------|

|                                                    |                                                                                  |
|----------------------------------------------------|----------------------------------------------------------------------------------|
| Carrier Comunicaciones                             | Telconet<br>Suratel<br>Impsat<br>Megadatos                                       |
| Telefonía Móvil – Fija                             | Movistar<br>Porta<br>Andinatel                                                   |
| Instituciones Gubernamentales                      | SRI<br>Banco Central                                                             |
| Instituciones Financieras                          | Bancos<br>Cooperativas                                                           |
| Importadoras Exportadoras<br>Comercio Distribución | El Rosado<br>Tecnomega<br>Química Suiza<br>Nestle<br>Quifatex<br>Almacenes Japón |

**Tabla 1.- Empresas que utilizan herramientas de monitoreo de red.**

El principal objetivo de usar gestión de redes en un centro de cómputo es Diseñar, implementar y optimizar las redes de datos, mediante un análisis minucioso de sus dispositivos de red Hubs, Switch o Routers configurándolos de la mejor forma para que proporcionen al máximo rendimiento en la red.

La obtención de información es el primer requisito para cumplir el objetivo, y esto no puede ser sino mediante el uso de herramientas de monitoreo que proporcionan los datos estadísticos e históricos de las principales falencias que posee la red.

En la actualidad la mayoría de herramientas de monitoreo de red utilizan el protocolo SNMP para el monitoreo de las redes, puesto que los equipos de red se han estandarizado y

utilizan el protocolo básico de gestión de red SNMP y RMOM, que permite controlar el acceso y funcionamiento de los dispositivos a la red.

Se tiene que instalar o activar en todos los puestos de la red, y a cambio permite detectar si la conexión de algún equipo está fallando y poder aislar o desconectar aquellos que produzcan errores en la red.

## **2.6 PROBLEMAS FRECUENTES EN LA GESTION DE REDES**

Para cada tipo de empresa mencionada en la tabla 2 se pudieron establecer los siguientes problemas más frecuentes presentados en su red; para lo cual utilizan un software de gestión de redes que detecta dicha fallas.

Cabe mencionar que la información obtenida fue muy restringida por políticas de seguridad que tienen las instituciones razón por la cual no se mencionan nombres específicos.

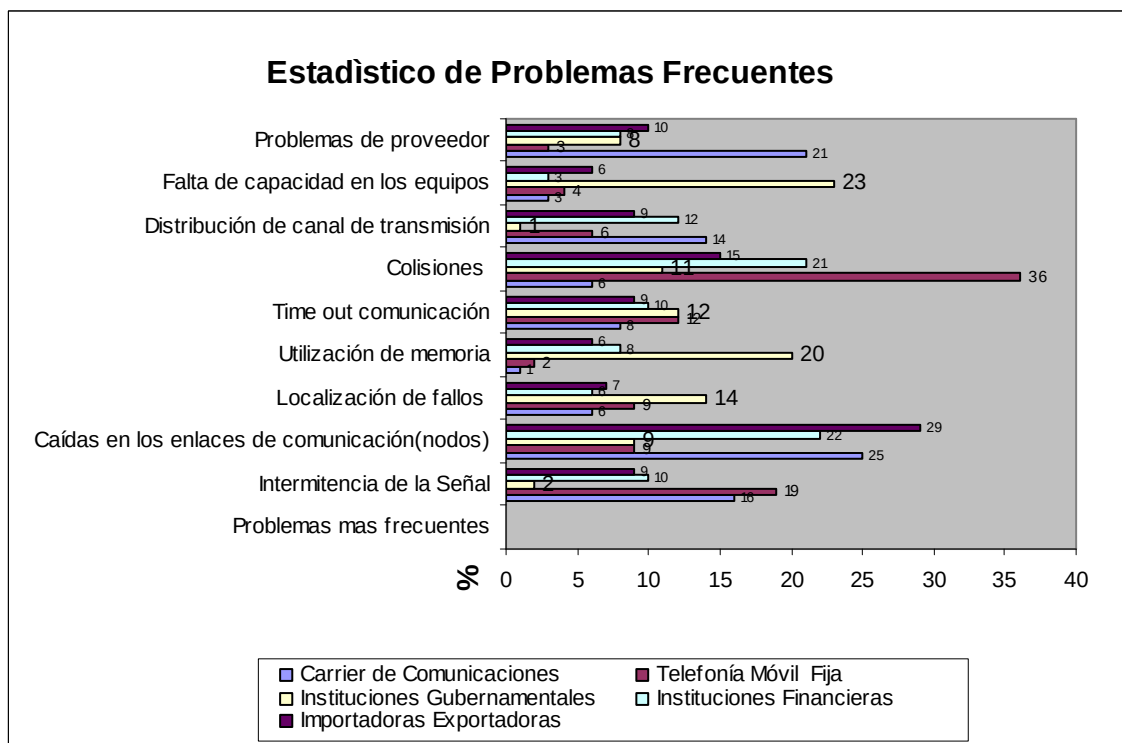
Entre los principales problemas de red para el personal de monitoreo y comunicación fueron:

| <b>Problemas mas frecuentes</b>              | <b>Descripción</b>                                                                                                                                                                                                                 |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Intermitencia de la Señal                    | Este es un problema para la comunicación, debido a que el retraso en la conmutación dura unos cuantos cientos de milisegundos, lo cual no se nota, pero en la transmisión de información puede hacer estragos.                     |
| Caídas en los enlaces de comunicación(nodos) | La falta de comunicación de un enlace ocasiona pérdida de servicios en horarios hábiles. El poder determinar que nodo de la red y que tipo de falla esta específicamente ligado es indispensable para la solución.                 |
| Localización de fallos                       | Nos es muy difícil diagnosticar tanto la existencia de fallos en la continuidad o empalmes defectuosos que originen serios problemas de comunicación en la red.                                                                    |
| Carga de trabajo                             | Este es uno de los problemas más frecuentes, el poder determinar a que tipo de problema esta ligado la falta de sistema, ocasiona perdidas económicas por la falta de atención a clientes.                                         |
| Utilización de memoria                       | Es uno de las consecuencias de lentitud en la red y por ende en el sistema de transmisión de datos                                                                                                                                 |
| Time out comunicación                        | En los tiempos de respuesta altos es otro de los problemas más comunes, pueden estar ligados a una perdida de señal o como a una carga de trabajo alta.                                                                            |
| Colisiones                                   | La falta de información de los usuarios para la utilización del canal de transmisión hace que tengamos colisiones de sistema.                                                                                                      |
| Distribución de canal de transmisión         | El poder distribuir el canal para determinado tipo de información y evitar los cuellos de botella se ha vuelto imprescindible pero a la vez el poder determinar los rangos que requieren ser actualizados es aun más imperante.    |
| Falta de capacidad en los equipos            | El aumento en la transaccionalidad no solo necesita una actualización o distribución de información sino que también el poder determinar que equipos se saturan y deben ser reemplazados o a sus ves actualizadas en su capacidad. |
| Problemas de proveedor                       | La perdida de comunicación de un nodo lleva a la perdida de los que se encuentra ligados a el y el soporte de backup establecido no responde sería un ejemplo de error en el proveedor de enlace                                   |

**Tabla 2. Descripción de Problemas mas frecuentes en el monitoreo de red.**

Para los problemas antes mencionados se realizaron una encuesta (véase en anexos ) que arrojo los siguientes datos estadísticos.

| <b>Problemas mas frecuentes</b>                     | <b>Carrier de Comunicaciones</b> | <b>Telefonía Móvil Fija</b> | <b>Instituciones Gubernamentales</b> | <b>Instituciones Financieras</b> | <b>Importadoras Exportadoras</b> |
|-----------------------------------------------------|----------------------------------|-----------------------------|--------------------------------------|----------------------------------|----------------------------------|
| <b>Intermitencia de la Señal</b>                    | 16                               | 19                          | 2                                    | 10                               | 9                                |
| <b>Caídas en los enlaces de comunicación(nodos)</b> | 25                               | 9                           | 9                                    | 22                               | 29                               |
| <b>Localización de fallos</b>                       | 6                                | 9                           | 14                                   | 6                                | 7                                |
| <b>Utilización de memoria</b>                       | 1                                | 2                           | 20                                   | 8                                | 6                                |
| <b>Time out comunicación</b>                        | 8                                | 12                          | 12                                   | 10                               | 9                                |
| <b>Colisiones</b>                                   | 6                                | 36                          | 11                                   | 21                               | 15                               |
| <b>Distribución de canal de transmisión</b>         | 14                               | 6                           | 1                                    | 12                               | 9                                |
| <b>Falta de capacidad en los equipos</b>            | 3                                | 4                           | 23                                   | 3                                | 6                                |
| <b>Problemas de proveedor</b>                       | 21                               | 3                           | 8                                    | 8                                | 10                               |



**Grafica 2.- Estadístico de problemas frecuentes**

## 2.7 ESTADÍSTICAS Y NIVELES DE SERVICIOS

En las empresas investigadas se pudo obtener los datos estadísticos de los índices de servicio que se establecen en base a las variables de frecuencia de problemas comunes en la gestión de redes de cada uno de sus centros de cómputo.

También se establecen que herramientas y técnicas de monitoreo se utilizaron para la obtención de estos datos y el período de frecuencia a ser examinados. Principalmente revisa los cambios en la obtención y análisis de datos que han ocurrido últimamente y resalta algunos de los beneficios que están disponibles en las herramientas de monitoreo.

Concluye que los desarrollos tecnológicos que permiten obtener datos de alta calidad desde todos los niveles del sistema de distribución a una frecuencia que no se pudo lograr antes de las herramientas de monitoreo han permitido niveles de eficiencia y estabilidad muy altos; ya que actualmente las empresas exigen un 99.99% de disponibilidad en sus servicios.

### **2.7.1 EMPRESA DE CARRIER COMUNICACIONES**

Una empresa proveedora de Carrier de comunicaciones se basa fundamentalmente en el nivel de servicio que brinda, para ello utilizan MRTG una herramienta de monitoreo basada en plataforma Solaris (Linux), mediante la cual pueden establecer el tipo de incidencias y fallas que se han presentado en un periodo determinado para un cliente específico. Lo más importante de esto es el poder determinar cuales de ellas fueron provocadas por la empresa proveedora y cuales por parte del cliente.

Por ejemplo en la tabla 3 muestran una estadística que la empresa de Carrier entrega a uno de sus clientes en un mes de servicio. Y la relación del porcentaje obtenido y el cumplimiento del porcentaje de uptime contratado.

| <b>Tipo</b>               | <b>% Uptime</b> |
|---------------------------|-----------------|
| Problemas de ultima milla | 94              |
| Problemas de nodo         | 96              |
| Problemas de radio base   | 95              |
| SLDA                      | 95              |

**Tabla 3.- Uptime mensual de nivel de servicio**

El grafico1 muestra un estadístico para 6 meses de servicios brindado a un cliente, fundamentados en los reportes emitidos por parte de la empresa Carrier y la proyección que este tendría en el siguiente mes.

| <b>Tipo</b>               | <b>Enero<br/>%</b> | <b>Febrero<br/>%</b> | <b>Marzo<br/>%</b> | <b>Abril<br/>%</b> | <b>Mayo<br/>%</b> | <b>Junio<br/>%</b> |
|---------------------------|--------------------|----------------------|--------------------|--------------------|-------------------|--------------------|
| Problemas de ultima milla | 94                 | 96                   | 93                 | 95                 | 96                | 94.8               |
| Problemas de nodo         | 96                 | 96                   | 95                 | 95                 | 94                | 95.2               |
| Problemas de radio base   | 95                 | 98                   | 97                 | 96                 | 98                | 96.8               |
| SLDA                      | 95                 | 96.667               | 95                 | 95.3               | 96                | <b>95.6</b>        |

**Tabla 4.-Estadístico de niveles de servicio**

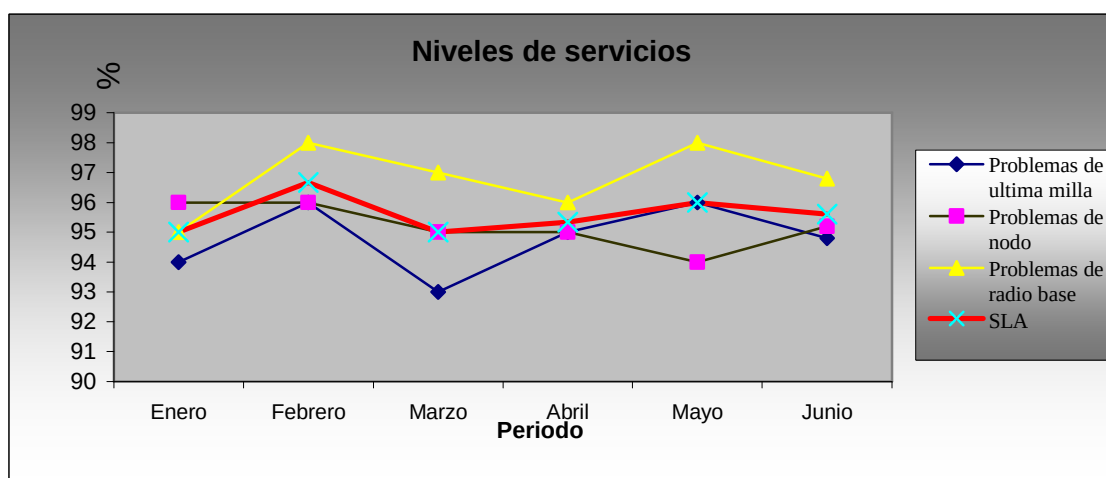


**Gráfico 1: Niveles de servicio en los 6 últimos meses.**

El establecer estos informes mensuales a cada uno de los clientes de las empresas de Carrier es fundamental para mostrar el nivel de servicio que provee, garantizando de esta manera una correcta y eficiente monitorización de su red.

### **2.7.2 EMPRESA FINANCIERA**

El nivel de transaccionalidad de una entidad financiera es uno de los puntos que más resalta en una empresa de este tipo, de tal forma el nivel de servicio estará medido en gran parte por la rapidez y eficiencia de cada una de las transacciones que realiza día a día.

La entidad investigada posee actualmente la necesidad de añadir a su centro de cómputo una herramienta que monitoree la red. Posee paquetes de software que permiten parcialmente monitorear los enlaces de comunicación, un ejemplo es NetSightManager que ha sido adquirida como parte del manejo de hardware (ENTERASYS) adquirido por la institución.

La implementación de Patrol DashBoard en la institución, ha sido para medir los niveles de satisfacción en los requerimientos de la institución. Y las estadísticas del nivel de servicio obtenidas están basadas en los informes emitidos por NetSightManager y Patrol Dashboard en el tiempo que duro el Demo.

En la tabla 5 se muestra un Uptime la red para un mes de evaluación; en el no se distinguen cuales fueron provocados por la parte proveedora y cuales por la operativa ya que se trata de medir el nivel de servicio al cliente y para esto los dos casos son transparentes para el usuario.

|                         |         |
|-------------------------|---------|
| Suc.Ambato(Amb)TS       | 97.04%  |
| Suc.Cuenca(Cue)TS       | 100.00% |
| Suc.Esmeraldas(Esm)TH   | 100.00% |
| Suc.Guayaquil(Gye)BP    | 100.00% |
| Suc.Ibarra(Iba)TH       | 99.04%  |
| Suc.Loja(Loj)BP         | 100.00% |
| Suc.Manta(Man)TH        | 100.00% |
| Suc.Quevedo(Que)BP      | 100.00% |
| Suc.Riobamba(Rio)BP     | 100.00% |
| Suc.SantoDomingo(Sto)BP | 100.00% |

**Tabla5.- Uptime de servicio**

Los informes de detallados del porque fueron las bajas en servicio son evaluados por la vicepresidencia de sistemas y jefaturas de sistemas para la aprobación de nuevos equipos y periféricos, contratación de nuevos proveedores y generación de correctivos en el manejo del sistema.

### **2.7.3 EMPRESA DE IMPORTACIÓN Y EXPORTACIÓN**

En las empresas importadoras – exportadoras se ha demostrado que la mayoría de problemas son provocados por fallas en la red y por la falta de control en la gestión de misma, por esta razón se realizó una evaluación exhaustiva de los niveles de servicio que recibían y brindaban generando un nivel de servicio inferior al estandarizado y requerido en el mercado. Por este motivo es muy importante tener un software que permita monitorear toda la red y poder establecer parámetros y llevar un control detallado sobre todo lo que circula en la misma.

A continuación se muestra los porcentajes y problemas más frecuentes en este tipo de empresas:

- El usuario desconecta el cable de red
- Problemas de servidores por fallas de Hardware o Software (sobre demanda de peticiones que causa vulnerabilidades al Sistema Operativo)
- Caídas eléctricas, por fallas o bajas de UPS's, teniendo en cuenta que se debe prever de un generador.
- Fallas de dispositivos de red (switches, routers, hub)
- Deterioro del Cableado
- Fallas de tarjetas de red

En fin, todos estos problemas pueden englobarse como se muestra en la Tabla4:

| <b>Tipo de Problema</b>                                                                                        | <b>%<br/>Porcentaje</b> |
|----------------------------------------------------------------------------------------------------------------|-------------------------|
| Falla en el sistema de red (perdida de comunicación con el software, conflictos con direcciones IP).           | 45                      |
| Fallas de dispositivos de la red ( impresoras, switches, hub, routers), ya sea por configuración o desconexión | 30                      |
| Caídas Eléctricas y o UP's                                                                                     | 15                      |
| Perdida de Comunicación con los dispositivos de las filiales en otros países.                                  | 10                      |

**Tabla 5. Problemas frecuentes**

En la tabla 5 se muestra como baja el porcentaje de los problemas al realizar un monitoreo utilizando un software de gestión.

| <b>Tipo de Problema</b>                                                                                        | <b>%</b> | <b>Solucion</b>                                                                            | <b>%</b> |
|----------------------------------------------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------|----------|
| Falla en el sistema de red (perdida de comunicación con el software, conflictos con direcciones IP).           | 45       | Asignación correcta de direcciones IP, monitoreo de la red para evitar trafico en la misma | 30       |
| Fallas de dispositivos de la red ( impresoras, switches, hub, routers), ya sea por configuración o desconexión | 30       | Monitoreo constante de los Routers y demás dispositivos, para verificar su estado          | 5        |
| Caídas Eléctricas y o UP's                                                                                     | 15       |                                                                                            | 15       |
| Perdida de Comunicación con los dispositivos de las filiales en otros países.                                  | 10       | Monitoreo constante                                                                        | 3        |

**Tabla5. Problemas y soluciones al utilizar software de gestión.**

El grafico2 muestra un estadístico de los problemas mas frecuentes que se presentan en las empresas, los cuales son posibles monitorear si se tiene un software de gestión para

poder solucionar con rapidez, confiabilidad y de esta manera mejorar el rendimiento de la red.

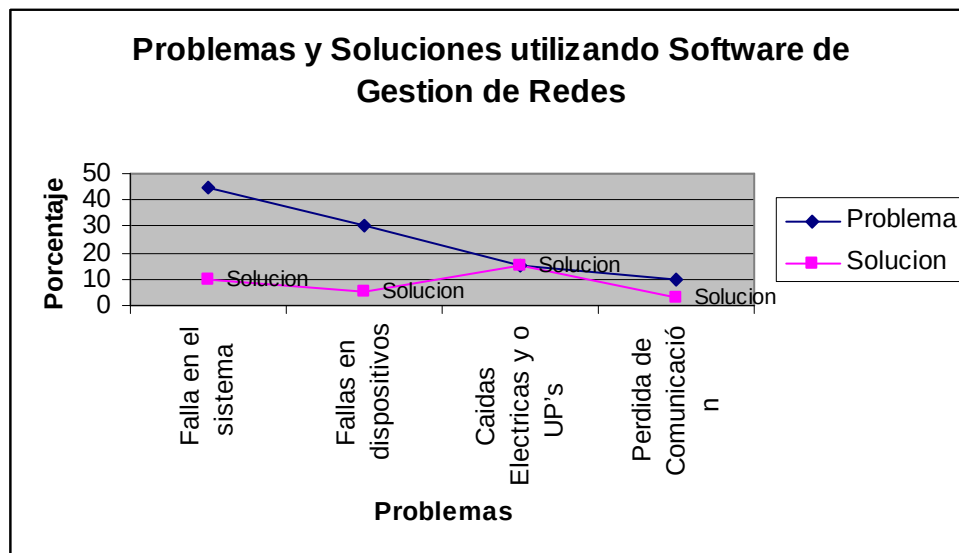


**Grafico 2. Muestra la solución a los problemas de la red utilizando software de Gestión**

En estas empresas es muy importante y fundamental el monitoreo de red, debido al servicio que debe brindar a sus clientes en los despachos y recepción de productos, por tal motivo se ve la necesidad de implementar un centro de computo. En algunos casos no únicamente se tiene el centro de computo centralizado en un solo país, sino también debe estar interconectado con sus múltiples filiales alrededor del mundo y de esta forma el control en la gestión de redes es debe ser mucho mas confiable.

## **2.8 DEFINICIÓN DE GESTIÓN DE REDES**

Se define como el proceso o control de la información compleja que circula por la red para maximizar su eficiencia y productividad.

Provee un conjunto de herramientas que permite una monitorización de las redes antes de la ausencia de fallas y ofrece diagnósticos remotos así como cambios y eventos que el administrador considere necesario.

Las áreas fundamentales en las que actúa son la gestión de fallos, gestión de la configuración, gestión de la seguridad, gestión de la ejecución y gestión de la contabilidad.

## **2.9 INTRODUCCIÓN A LA GESTIÓN DE REDES**

El desarrollo de las telecomunicaciones ha incrementado enormemente, al igual que la complejidad de las redes y la gama de servicios disponibles, lo cual resalta la importancia de la gestión de redes como uno de los componentes esenciales para maximizar la relación costos / prestaciones, mediante la utilización de recursos más poderosos de configuración, supervisión y mantenimiento.

Como complemento de una red de comunicaciones se hace imprescindible un buen sistema de gestión de red que asegure un control completo de todos los elementos implicados en la red de comunicaciones del cliente dentro de un entorno de gestión integrado.

Cualquier red corporativa debe estar correctamente administrada con el objetivo de asegurar a sus usuarios su utilización y garantizar a los clientes de red el correcto funcionamiento de la misma, por otra parte, la monitorización del tráfico nos servirá para evitar problemas, o en el peor de los casos, para ayudarnos a solucionarlos.

La solución a una Gestión de red ineficiente, compleja y cara es tratar de unificar criterios, además hay que monitorizar, saber como interpretar y controlar el proceso de gestión.

Las herramientas de gestión que vienen siendo utilizadas son principalmente los analizadores de protocolos y las plataformas de gestión SNMP (Simple Network Management Protocol, Protocolo Simple de Gestión Red). La aplicación de los analizadores de protocolos o sniffers a la gestión de red se limita al ámbito del segmento local que monitorizan, para conseguir una proactividad y una correcta gestión de la red.

Las herramientas de gestión de red se han desarrollado con el propósito fundamental de ayudar a diagnosticar rápidamente los problemas de conectividad; localizar con precisión los puntos de congestión y cuellos de botella; analizar de un modo extensivo la utilización de la red; y planificar las necesidades futuras de capacidad.

Con el crecimiento en tamaño y complejidad de las redes basadas en TCP/IP (Transmission Control Protocol / Internet Protocol, Protocolo de Control de Transmisión / Protocolo de Internet), la necesidad de mecanismos de gestión de red se

ha vuelto muy importante. En la actualidad, los protocolos que forman el soporte de la gestión de red son:

- a) SMI (Structure of Management Information, Estructura para la Información de Gestión)- Describe cómo se definen los objetos gestionados contenidos en el MIB (Management Information Base, Base de Gestión de Información).
- b) MIB-II - describe los objetos gestionados contenidos en el MIB.
- c) SNMP - define el protocolo usado para gestionar estos objetos.

## **2.10 EVOLUCIÓN DE LA GESTIÓN DE REDES**

A finales de los años 70, las redes de ordenadores experimentaron un crecimiento y empezaron a conectarse entre sí. A estas nuevas redes se les llamó interredes o Internet. Pronto se hicieron muy difíciles de gestionar, y se hizo necesario el desarrollo de un protocolo de gestión.

El primer protocolo que se usó fue el SNMP. Se diseñó como algo provisional hasta que se desarrollara otro protocolo más elaborado.

En los años 80 aparecieron dos nuevos protocolos: por un lado, la segunda versión del SNMP, que incorporaba muchas de las funciones del original (que sigue en uso) e incluía nuevas características que mejoraban sus deficiencias. Por otro, el CMIP (Common Management Information Protocol, Protocolo Común de Gestión de

Información), que estaba mejor organizado y contenía muchas más funciones que las dos versiones del SNMP.

En los comienzos de Internet, se hacía hincapié en la definición e implementación de protocolos que alcanzaran la inter operación.

A medida que crecía la red aparecieron situaciones en las que procedimientos para gestionar la red no eran capaces de crecer con ella.

En 1987 quedó claro que era necesario un protocolo que permitiera que se pudieran gestionar remota y uniformemente los elementos de una red, como los routers. Se propusieron varios protocolos con este propósito, entre ellos: el SNMP, diseñado como su propio nombre indica buscando la simplicidad; HEMS (High Level Management System, Sistema de Gestión de Alto Nivel) un diseño más complejo procedente de la comunidad de investigadores; y CMIP, desarrollado por la comunidad OSI (Open Systems Interconexión, Interconexión de Sistemas Abiertos).

Una serie de investigaciones llevaron a tomar la decisión de desestimar HEMS como candidato para la estandarización, dejando que tanto SNMP como CMIP siguieran adelante con la idea que el primero fuera una solución inmediata mientras que CMIP pasara a ser una aproximación a largo plazo: el mercado podría elegir el que resultara más apropiado. Hoy SNMP se usa casi universalmente para la gestión de red.

## **2.11 OBJETIVOS DE LA GESTIÓN DE RED**

Tiene como objeto proveer soluciones para ayudar al personal de operación y mantenimiento de redes a cumplir la misión de garantizar la disponibilidad de los servicios de las redes en todo lo momento.

Además de reducir los riesgos y costos asociados con las operaciones de las empresas, y mantener la red en servicio con el requisito de que los costes de gestión sean razonables, alcanzando un compromiso entre la calidad del servicio ofrecido y el coste de la gestión de la red.

## **2.12 FUNCIONES DE GESTIÓN DE RED.**

Se pueden agrupar en dos grandes categorías: monitorización y control.

### **2.12.1 Monitorización.**

Son funciones de lectura, encargadas de observar y analizar el estado y comportamiento de la configuración de red y sus componentes. Abarca prestaciones, fallos y costes.

#### **2.12.1.1 Objetivos de la Monitorización de red**

Tiene tres objetivos fundamentales:

- Identificar la información a monitorizar.
- Diseñar los mecanismos de monitorización.

- Utilizar la información.

#### **2.12.1.2 Arquitectura funcional de monitorización.**

Los cuatro elementos principales que intervienen en la monitorización son:

- a) Aplicación de monitorización: gestiona las funciones de monitorización que son visibles al usuario, tal como gestión de prestaciones, fallos y costes.
- b) Gestor: el módulo de la red que recoge la información del resto de los elementos de la red.
- c) Agente: recoge y almacena información de uno o varios elementos de la red y los envía al gestor.
- d) Objetos gestionados: información de gestión que representa recursos y su actividad.

Además podemos añadir un quinto elemento funcional relacionado con la información estadística:

- d) Agente de monitorización: módulo que genera sumarios y análisis estadísticos de la información de gestión. Si este módulo es remoto al gestor, actúa como un agente y comunica la información estadística que genera ha dicho gestor.

#### **2.12.2 Control.**

Son Funciones de escritura, utilizados para alterar parámetros de los componentes de la red. Abarca: configuración y seguridad.

## **2.13 ESTÁNDARES DE GESTIÓN DE REDES.**

Para ilustrar en qué consiste un protocolo de gestión de red, y cuál es la problemática en la definición de la información gestionada, se presentan dos estándares concretos, SNMP, orientado a la gestión de redes TCP/IP y CMIP, orientado a la gestión de redes de telecomunicación.

### **2.13.1 SNMP (Simple Network Management Protocol, Protocolo Simple de Gestión de Red).**

Es un protocolo estándar de Internet, su estatus es recomendado y su especificación actual se encuentra en el RFC 1157.

El RFC 1157, titulado como Protocolo Simple de Administración de redes SNMP, es un documento donde se define el funcionamiento de un protocolo para la administración de redes SNMP.

Definiendo el protocolo SNMP para administrar nodos en la comunidad de Internet y OSI Network Management Framework. La información sería administrada de dos formas, una para definir la estructura de la información administrable SMI (Structure of Management Information), y la otra para definir la Base de Información Administrable (MIB).

Durante el desarrollo de los dos estándares para la administración de redes el OSI Network Management Framework presenta grandes diferencias, así también surge incompatibilidad entre SMI y MIB por lo que es suspendido.

Esto permite que la Administración Operacional de las Redes se base en SNMP, para responder a las nuevas necesidades operacionales en Internet.

#### **2.13.2 CMIP (Common Management Information Protocol, Protocolo Común de Gestión de Información)**

Especifica los procesos de transmisión de información de gestión, las reglas de codificación de la gestión común de información y los procesos para la correcta interpretación de la información de control del protocolo.

CMIP y CMIS (Common Management Information Services, Servicio Común de Gestión de Información) se definen según los estándares ISO/IEC 9595 y 9596.

Tras la aparición de SNMP como protocolo de gestión de red, a finales de los 80, plantearon el Protocolo Común de Gestión de Información CMIP, que se pensó que podría llegar a ser una realidad debido al alto presupuesto con que contaba. En cambio, problemas de implementación han retrasado su expansión de modo que solo está disponible actualmente de forma limitada y para desarrolladores.

CMIP fue diseñado teniendo en cuenta a SNMP solucionando los errores y fallos que tenía SNMP y volviéndose un gestor de red mayor y más detallada. Su diseño es similar a SNMP por lo que se usan PDUs como variables para monitorizar 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 gestión de red que se implementa sobre el modelo de Interconexión de Redes Abiertas OSI que ha sido normalizado por la ISO en sus grupos de trabajo. Además existe una variante del mismo llamado CMOT (CMIS/CMIP Over TCP/IP, CMIS/CMIP SOBRE TCP/IP) que se implementa sobre un modelo de red TCP/IP.

En pocas palabras, CMIP es una arquitectura de gestión de red que provee un modo de que la información de control y de mantenimiento pueda ser intercambiada entre un gestor y un elemento remoto de red. En efecto, los procesos de aplicación llamados gestores residen en las estaciones de gestión mientras que los procesos de aplicación llamados agentes residen en los elementos de red.

CMIP define una relación igual a igual entre el gestor y el agente incluyendo lo que se refiere al establecimiento y cierre de conexión, y a la dirección de la información de gestión. Las operaciones CMIS se pueden originar tanto en gestores como en agentes, permitiendo relaciones simétricas o asimétricas entre los procesos de gestión. Sin embargo, la mayor parte de los dispositivos contienen las aplicaciones que sólo le permiten hacer de agente.

Un sistema CMIP debe implementar una serie de protocolos de los cuales el CMISE (Common Management Information Services Element, Elemento de Servicio de Gestión de Información), es el que trabaja mano a mano con CMIP: todas las operaciones de gestión de red que crea CMISE, el CMIP las mapea en una operación en el CMIP remoto.

#### **2.13.2.1 Protocolos de Aplicación en CMIP.**

Para comunicarse entre sí dos entidades de aplicación pares del gestor y del agente se utilizan APDU's (Application Protocol Data Units, Unidad de datos de Protocolos de Aplicación). Como hemos visto, CMIP está compuesto de los protocolos OSI que siguen:

- ACSE (Association Control Service Element - Asociación de Control de Servicios y Elementos) se utiliza para establecer y liberar asociaciones entre entidades de aplicación. El establecimiento lo puede realizar el agente o el gestor, 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.

- CMISE: proporciona los servicios básicos de gestión confirmados y no confirmados para reportar eventos y manipular datos de gestión.
- CMOT es un protocolo propuesto como estándar de Internet. Su estatus es electivo. Su especificación actual se encuentra en el RFC 1189.

Es un protocolo de gestión de red que se implementa sobre un modelo de red TCP/IP. El objetivo de CMOT era extender la gestión OSI del mundo de las telecomunicaciones al mundo de Internet, pero la mayoría de vendedores adoptaron SNMP.

- MIB-II Es un protocolo estándar de Internet. Su estatus es recomendado. Su especificación actual se encuentra en el RFC 1213

A partir de que se creó el RFC 1155, donde se definió el primer MIB, ha habido algunos cambios en cuanto a la información administrable, por lo tanto surgió un nuevo MIB, definido en el RFC 1213.

El RFC 1213 está titulado como Base de Información Administrable para redes basadas en TCP/IP y es comúnmente conocido como MIB II. En este RFC se describen los cambios que han surgido para cada objeto definido en el RFC 1155, así también se describen los nuevos objetos que han sido definidos.

## **2.14 MODELOS DE GESTIÓN DE RED.**

La gestión de redes y servicio ha sido un campo en el que tradicionalmente se han impuesto soluciones y mecanismos propietarios de distintos fabricantes, que exigían que la gestión de sus equipos y servicios solo pudieran realizar con el gestor del propio fabricante, por esta razón surgieron los denominados modelos de gestión de red integrada, que definían un protocolo y unos modelos de información de gestión estándares que rompían la propiedad en el acceso de gestión remota, permitiendo en teoría la interoperabilidad entre gestores y elementos gestionados de múltiples fabricantes.

Debido a diversas razones, fueron dos los modelos propuestos: el de gestión de red de Internet conocido como SNMP y el modelo de gestión de red OSI conocido también con el nombre de su protocolo CMIP, estos modelos son incompatibles entre si lo que ha hecho que al cabo de los años cada modelo tenga su ámbito de aplicación distinto; mientras que la gestión OSI se utiliza sobre todo para la gestión de equipos y servicios en redes de telecomunicación, la gestión Internet esta mas orientada a la gestión de equipos y servicios sobre redes de datos. No obstante existen diversos entornos en los que ambos modelos deben coexistir con la problemática que ello conlleva.

- Gestión Internet: definido por la Internet Society, Sociedad Internet, para gestionar redes TCP/IP.
- Gestión de red OSI: definido por ISO, para gestionar los recursos según el modelo de referencia OSI

- Arquitectura TMN (Telecommunications Management Network, Redes de Gestión de Telecomunicaciones): definida por la ITU-T, se basa en los modelos anteriores e incluye el acceso a los recursos de telecomunicaciones.

En el Gráfico 1 se indica los modelos de Gestión de Red.

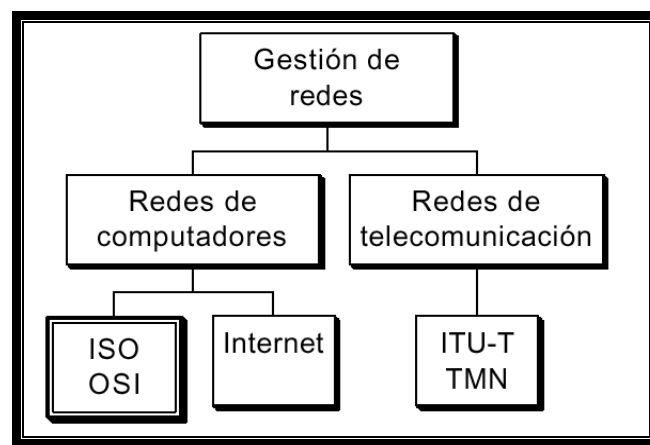


**Gráfico 1. Modelos de Gestión de Red**

#### **2.14.1 Modelo Gestión en Internet.**

Es un Conjunto de estándares que incluyen:

- Un protocolo para especificar el intercambio de datos entre agentes y gestores (SNMP)
- Se refiere a:
  - o La especificación de una estructura de base de datos (SMI: Structure of Management Information – Estructura de Gestión de Información)

- o Un conjunto de objetos de datos (MIBs).
  - o Complemento: Extensión para administración de LANs.
  - o RMON (Remote Network Monitoring, Monitoreo Remoto de Red)
- Incluye aspectos de seguridad
  - Define una arquitectura para ampliaciones futuras

#### **2.14.2 Modelo de Gestión de red OSI.**

Se definen por OSI cinco áreas funcionales para la gestión de redes:

##### **2.14.2.1 Gestión de Fallos.**

Incluye monitorización de alarmas de los equipos, averías, responsable de detectar, aislar y controlar comportamientos no deseables de la red.

- Mantiene funcionando correctamente la red como un todo y cada uno de sus elementos individualmente.
- Cuando algo falla, es importante, tan rápido como sea posible:
  - o Determinar exactamente cual era el fallo.
  - o Aislar el resto de la red del fallo para que continúe funcionando sin interferencias.

- o Reconfigurar o modificar la red de manera que se minimice el impacto del fallo en las operaciones de la organización.
- o Reparar o sustituir los componentes que han fallado.
- o Hay que distinguir entre fallo y error los errores son normales y la mayoría de las veces se corrigen solos.

#### **2.14.2.2 Gestión de costes.**

- En muchas organizaciones, diferentes divisiones, centros de gasto o proyectos, son facturados por el uso de los servicios de red.
- Aun cuando esto no ocurra, es necesario mantener información sobre el uso de los recursos de red por usuarios o tipos de usuarios:
- Determinados usuarios pueden estar abusando de sus privilegios de acceso y cargar la red afectando a los demás usuarios.
- Los usuarios pueden hacer un uso ineficiente de la red, y el gestor puede ayudar a cambiar procedimientos para aumentar la efectividad.
- Conocer en detalle las actividades de los usuarios será muy útil para planificar el crecimiento adecuado de la red.

#### **2.14.2.3 Gestión de Configuración.**

Responsable de realizar un seguimiento de la configuración inicial y los posibles cambios con el tiempo, así como el control centralizado de los cambios.

- Los modernos elementos físicos y lógicos (controlador de dispositivos de un S.O.) de una red se pueden configurar para realizar diversas tareas. Un dispositivo se puede configurar por ejemplo para ser un nodo final, un router o ambas cosas.
- Una vez elegido el papel de cada dispositivo el gestor debe elegir el software adecuado y los atributos y valores para ese dispositivo.
- La configuración también se encarga de inicializar y apagar adecuadamente parte de la red.
- También se encarga de mantener, añadir y actualizar la relación entre los componentes y su estado durante la operación de la red.
- Automatización de tareas (encendido/apagado de interfaces, etc.).
- Identificación de elementos (gestión de identificación).

#### **2.14.2.4 Gestión de prestaciones.**

- Las redes modernas están compuestas de muchos componentes que se comunican y comparten datos y recursos.
- La efectividad de una aplicación depende cada vez más de unas prestaciones adecuadas de la red.
- Abarca dos grandes categorías funcionales:
  - Monitorización: Seguimiento de la actividad de la red.

- o Control: Realización de ajustes para mejorar las prestaciones.
- Para esta gestión hay que identificar los valores relevantes a monitorizar de la red y definir las métricas adecuadas. Esto permitirá obtener estadísticas que ayuden a mantener las prestaciones adecuadas (eliminar cuellos de botella reconfigurando rutas o ampliando líneas, etc.).

#### **2.14.2.5 Gestión de seguridad.**

Proteger la red, los elementos y la gestión de los equipos de accesos no deseados, obtención de datos privados y daños.

- Generación, distribución y almacenamiento de claves cifradas.
- Mantenimiento y distribución de passwords y otras autorizaciones o controles de acceso a la información.
- Monitorización y control del acceso a los ordenadores de la red y a parte o toda la información de la información de gestión de los nodos de la red.
- Registros (logs): recolección, almacenamiento y procesamiento de registros de auditoria y seguridad.
- Gestión (definir, lanzar / parar) las facilidades de registro. Gestión de segur. (Requisitos de los usuarios)
- Los usuarios quieren conocer que las políticas de seguridad son las adecuadas y efectivas (otros no pueden acceder a su información, etc.).

- También que las facilidades de seguridad son ellas mismas seguras.

#### **2.14.3 Arquitectura TMN (Telecommunications Management Network, Redes de Gestión de Telecomunicaciones)**

Es un modelo genérico para la gestión de redes, es un conjunto de especificaciones recomendado para estándares, relacionadas con gestión de redes.

Por extensión, también se llama TMN a las redes que poseen arquitectura, interfaces y protocolos estándar.

Usa los estándares de gestión de OSI (Open Systems Interconexión, Interconexión de Sistemas Abiertos) como marco de referencia.

Orientado a objetos, por lo que es capaz de soportar un protocolo de gestión de red CMIP y servicio de información de gestión común CMISE (Common Management Information Services Element).

TMN proporciona una infraestructura para soportar la gestión y el despliegue de los servicios de telecomunicaciones.

TMN es conceptualmente una red separada que interacciona con los componentes de las redes de telecomunicaciones a través de diferentes puntos. Los recursos que la TMN puede gestionar se denominan elementos de red (NE - Network Elements, Elementos de red). TMN define una manera estandarizada para llevar a cabo la gestión en las redes identificando cinco áreas principales para la gestión: gestión de rendimiento, gestión de fallos, gestión de la configuración, gestión de contabilidad y gestión de la seguridad.

TMN emplea interfaces estandarizados para definir la comunicación entre las entidades de gestión en la red arquitectura en capas lógicas de TMN. La ultima versión es de Febrero de 2000 donde aparece el bloque funcional función de transformación.

La arquitectura y las interfaces TMN definidos en ITU-T se basan en varios estándares OSI como: CMIP/ CMIS que definen el protocolo y el servicio para la comunicación entre entidades de gestión; ASN.1 (Abstract Syntax, Sintaxis Abstracta) que describe las reglas sintácticas a utilizar para definir los tipos de datos; y el modelo de referencia OSI que define la pila de protocolos OSI que consta de siete capas.

TMN utiliza un enfoque orientado a objetos donde los recursos gestionados de la red son representados mediante objetos que están compuestos de atributos y operaciones.

El conjunto de estos objetos gestionados constituye la denominada MIB.

En TMN, los procesos que gestionan la información se denominan entidades de gestión. Dichas entidades pueden actuar como gestor o como agente. El gestor envía peticiones al agente para poder acceder a la MIB, y el agente puede emitir notificaciones hacia el gestor. La comunicación entre el gestor y el agente utiliza el protocolo CMIP para enviarlas primitivas del servicio CMIS. CMIP puede implementarse sobre la TMN define los siguientes interfaces estandarizadas que están asociados con los correspondientes puntos de referencia: Interfaz Q, Interfaz F e Interfaz X.

### **2.15 SISTEMAS DE GESTIÓN DE RED.**

Es una Colección de herramientas para monitorización y control. Compuesto por una única interfaz de operador con un completo pero amigable conjunto de comandos para realizar la mayoría de las tareas de gestión.

Está diseñado para ver la red completa como una arquitectura unificada, con direcciones y etiquetas asignadas a cada punto y a los atributos específicos de cada elemento y enlace del sistema.

Un conjunto mínimo de equipamiento separado. La mayoría del software y hardware de gestión está incorporado en el equipamiento existente. El software utilizado en realizar tareas de gestión reside en los ordenadores y procesadores de comunicaciones concentradores, bridges, routers, etc.

Los elementos activos de la red envían regularmente información de estado al centro de control de red.

### **2.16 PLATAFORMAS DE GESTIÓN DE RED.**

Históricamente, la gestión de red se realiza mediante un conjunto de programas aislados, cada uno encargado de gestionar un conjunto específico de componentes ya sean dispositivos o datos de gestión de la red.

Una plataforma de gestión de red es una aplicación software que proporciona la funcionalidad básica de gestión de red para los diferentes componentes de la misma.

El objetivo de la plataforma es proporcionar una funcionalidad genérica para gestionar dispositivos de red diversos.

Las funcionalidades básicas que debe incluir son:

- Interfaz gráfica de usuario (GUI)
- Mapa de la red.
- Sistema gestor de base de datos (SGBD)
- Método estándar de consulta de dispositivos.
- Menús del sistema configurables.
- Registro de eventos
- Seguridad del sistema Plataformas de Gestión existentes hoy en día:
  - o Sun: SunNet Manager
  - o Patrol Dashboard
  - o Solar Winds
  - o HP: Open View
  - o IBM: Netview for AIX

- o Cabletron: Spectrum
- o CISCO: CiscoView (a través de WWW)

### **2.17 MIB ( Management Information Base, Base de Gestión de Información).**

Son bases de datos que contienen un conjunto de variables llamadas objetos, almacenadas y organizadas de manera jerárquica, definido en el documento RFC 1156. En este documento se define la primera versión de la Base de Información Administrable MIB.

Existen otros dos documentos que complementan la definición de una estructura para administrar redes basadas en TCP/IP, que son: el RFC 1155, y el RFC 1157.

En esta especificación del MIB se definen las variables necesarias para el monitoreo y control de varios componentes en redes. No todos los grupos de variables definidas son obligatorios para todos los componentes de redes.

No se puede definir la información que formará parte del MIB arbitrariamente. Para definir dicha información se consideró esencial para ser contenida dentro del MIB. Así que, para verificar que la información era útil, se definieron una serie de criterios que se tomaron en cuenta:

- a) Un objeto necesita ser esencial para identificar una falla o configuración de administración.

- b) Solo se permiten objetos de control que no manejen información confidencial.  
Debido a que el protocolo actual no es lo suficientemente seguro.
- c) Debe existir evidencia de que la información fue requerida por su uso actual y su utilidad.
- d) Se hizo el intento de limitar el número de objetos a 100, para facilitar a los proveedores definir dichos objetos dentro de su software y su hardware.
- e) Para evitar variables redundantes, no se permitió que objetos que pueden ser derivados de otros objetos fueran incluidos.
- f) Fue excluida la implementación de objetos específicos.

Los Objetos dentro del MIB son definidos usando la notación de Sintaxis Abstracta. Cada objeto tiene un nombre (name), una sintaxis (syntax) y un código (encode).

El nombre es un identificador del objeto, y es asignado administrativamente, el cual especifica el tipo de objeto. El tipo de objeto junto con una instancia de objeto sirve únicamente para identificar una instancia específica de un objeto.

La sintaxis de un tipo de objeto que define la estructura de datos abstractos correspondiente al tipo de dato.

Y por último, el código de un tipo de objeto es simplemente el tipo de objeto representado usando la sintaxis de tipo de objeto.

Se definió una lista de objetos que se consideran los esenciales para ser administrados y son los siguientes:

- System (Sistema): Incluye la identidad del vendedor y el tiempo desde la última reinicialización del sistema de gestión.
- Interfaces: Un único o múltiples interfaces, local o remoto, etc.
- ATT (Address Translation Table, Tabla de Direcciones): Contiene la dirección de la red y las equivalencias con las direcciones físicas.
- IP (Internet Protocol, Protocolo de Internet): Proporciona las tablas de rutas, y mantiene estadísticas sobre los datagramas IP recibidos.
- ICMP (Internet Communication Management Protocol, Protocolo de Gestión y Comunicación de Internet): Cuenta el número de mensajes ICMP recibidos y los errores.
- TCP (Transmission Control Protocol, Protocolo de Gestión de Transmisión): Facilita información acerca de las conexiones TCP, retransmisiones, etc.
- UDP (User Datagram Protocol, Protocolo de Datagrama de Usuario): Cuenta el número de datagramas UDP, enviados, recibidos y entregados.
- EGP (Exterior Gateway Protocol, Protocolo de Enlace Exterior): Recoge información sobre el número de mensajes EGP recibidos, generados, etc.

Estos grupos de objetos definen de manera general la información administrable en un equipo, y representan una forma de clasificar dicha información.

Los MIB's son accedidos por protocolos de red como el protocolo SNMP. La comunicación entre el protocolo y el MIB, es a base de consulta-respuesta.

Se definen seis mensajes que pueden enviarse sobre el protocolo SNMP, y son los siguientes:

**Get Request.** Es la Solicitud de un Administrador al Agente SNMP para que envíe los valores contenidos en el MIB de una o más variables.

**Get Next Request.** Es una petición del Administrador al Agente SNMP para que envíe los valores del MIB que se refieren al siguiente objeto del especificado anteriormente.

**Get Response.** Es la respuesta del Agente SNMP a la petición del Administrador.

**Set Request.** Es una petición del Administrador al Agente SNM para que este cambie algún valor contenido en el MIB que se refiera a un objeto determinado.

**Inform-request.** Mensaje de administrador a administrador donde se describe el MIB local.

**Trap.** Es un mensaje espontáneo del Agente SNMP al Administrador, cuando este detecta una condición predeterminada, como la conexión o desconexión de una estación, o la caída de un enlace, etc.

El objeto o variable administrado, es una característica específica de algún elemento administrado. Existen dos tipos de objetos administrados: los escalares y los tabulares. Los escalares definen una sola instancia del objeto y los tabulares definen múltiples instancias de objetos que tienen una relación entre si y están agrupados en el MIB.

Para identificar a cada uno de los objetos administrados se crea un identificador único, este identificador se crea siguiendo el árbol jerárquico del MIB de manera descendente, en la que cada variable u hoja puede representarse de forma simbólica todo el camino o mediante forma numérica.

Entendemos la MIB como el conjunto de valores que componen la base de datos, y trabajaremos con objetos (los registros)

- Objeto:
  - o Nombre.
  - o Permisos (lectura, lectura/escritura, solo escritura, no accesible).
  - o Tipo (Contador, cadena, entero, medidor).
  - o Descripción.
  - o Estado.

Un proveedor también puede definir objetos para introducirlos al MIB y administrar así sus productos. Existe un MIB que define aspectos generales de productos de cualquier empresa, éste es conocido como MIB II, y está definido en el RFC 1213.

En si, es una base de datos donde se guarda toda la información relativa a la gestión de la red. El MIB tiene una estructura en árbol, donde en la parte superior se encuentra la información más general sobre la red, y conforme avanzamos por las ramas se consigue información más específica y detallada. Cada nodo del árbol MIB se conoce como variable, y la parte superior del árbol MIB se denomina Internet. Aunque la ISO ha definido un MIB modelo, cada fabricante de equipos tiene el suyo propio, e el que en general aunque las variables se denominen de diferente manera la información contenida en ellas es la misma.

### **3 CAPITULO III: PROTOCOLO SNMP (Simple Network Managenement Protocol, Protocolo Simple de Gestión de Red)**

#### **3.1 SNMP CONCEPTO**

SNMP es un protocolo de nivel de aplicación para consulta a los diferentes elementos que forma una red, como routers, switches, hubs, hosts, modems, impresoras, etc. También permiten tener datos concretos del tráfico que se produce en la red, así como quien lo produce.

Además como su nombre lo sugiere, SNMP es una herramienta simple de gestión de redes. Esta define una, delimitada y fácil de implementar base de información de gestión MIB (Management Information Base, Base de Información de Gestión), la cual consta de estructuras de datos estándares como variables escalares y tablas de dos dimensiones. SNMP define también un protocolo que permite modificar y recuperar informaciones de las variables MIB, además de habilitar a los agentes a enviar información de gestión no solicitada, la cual se denomina trap.

#### **3.2 INTRODUCCIÓN**

En 1988, el IAB (Internet Activities Board, Comité de Actividades Internet) determinó una estrategia de gestión para TCP/IP (Transmisión Control Protocol, Internet Protocol, Protocolo de control de transmisión, Protocolo de Internet). Esto significó el nacimiento

de dos esfuerzos paralelos: la solución a corto plazo SNMP y la solución eventual a largo plazo, CMOT (CMIP Over TCP/IP, CMIP sobre TCP/IP.).

CMOT pretendía implantar los estándares del modelo de gestión OSI en el entorno TCP/IP. CMOT tuvo que afrontar varios problemas derivados por la demora en la aparición de especificaciones e implementaciones prácticas. Los desarrollos de CMOT se paralizaron en 1992.

SNMP es una extensión del protocolo SGMP (Simple Gateway Management Protocol, Protocolo Sencillo de Supervisión de Pasarelas), que se convirtió en 1989 en el estándar recomendado por Internet. Está dirigido a proporcionar una gestión de red centralizada que permita la observación, el control y la gestión de los recursos gestionables. Utilizando SNMP, un administrador de red puede direccionar preguntas y comandos a los dispositivos de la red.

SNMP se ha convertido desde su aparición en el estándar de gestión de redes.

Todo el equipamiento de redes puede ser gestionado mediante SNMP.

Las funciones principales que permite SNMP son:

- Supervisión del rendimiento de la red y su estado.
- Control de parámetro de operación.
- Obtención de informes de fallos.
- Análisis de fallos.

El SNMP define el formato de los mensajes que viajan entre la computadora del administrador y una entidad supervisada.

Un estándar asociado al SNMP define el conjunto de las variables que una entidad administrada mantiene. El estándar se conoce como Base de Información de Administración (MIB). Las variables MIB se describen utilizando ASN.1, un lenguaje formal que proporciona una forma codificada concisa así como una notación precisa que es posible leer para los usuarios, nombres y objetos.

El protocolo de gestión de red simple o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de gestión entre dispositivos de red. Este protocolo es parte del conjunto de protocolos TCP/IP y, por su amplia utilización en redes empresariales, es considerado el estándar del protocolo CMIP de la familia de protocolos OSI, más utilizado en las grandes redes de las operadoras de telecomunicación.

SNMP permite a los administradores:

- Gestionar el rendimiento, encontrar y solucionar problemas, y planificar el crecimiento futuro de la red.
- Si bien SNMP se diseñó, en un principio, con el propósito de hacer posible supervisar de forma sencilla y resolver problemas, en routers y bridges; con su ampliación, este protocolo puede ser utilizado para supervisar y controlar: routers,

switches, bridges, hubs, servidores y estaciones Windows y Unix, servidores de terminal, etc.

El protocolo SNMP opera sobre varios protocolos de transporte, originalmente y habitualmente sobre UDP (User Datagram Protocol, Protocolo de Datagrama de Usuario), aunque actualmente también soporta, OSI CLNS (Connection Less Network Service, Servicio de Red de Menor Conexión), AppleTalk DDP (Datagram-Delivery Protocol, Protocolo de Datagrama de Entrega), y Novell IPX (Internet Packet Exchange, Intercambio del Paquete de Internet).

Un sistema de gestión de red basado en el protocolo SNMP está compuesto por los siguientes elementos: varios agentes, o nodos gestionados, al menos una estación de gestión (manager), un cierto volumen de información relativa a los dispositivos gestionados y un protocolo para la transmisión de dicha información entre los agentes y las estaciones de gestión.

Los mecanismos utilizados para definir la información relativa a los dispositivos gestionados apenas han sufrido modificaciones desde su aparición a finales de los años 80. Uno de los objetivos principales de su diseño fue la flexibilidad, de modo que la información definida pudiese seguir siendo utilizada posteriormente por protocolos diferentes, o incluso por distintas versiones del mismo protocolo.

Por el contrario el requisito fundamental del diseño del protocolo fue la sencillez, lo que si bien facilitó su expansión en perjuicio de protocolos más complejos, como por ejemplo CMIP, ha hecho necesarias varias revisiones para adaptar el protocolo a las

necesidades actuales, entre las que cabe destacar las exigencias en cuanto a la seguridad del sistema.

### **3.3 EVOLUCIÓN**

Al pasar el tiempo, SNMP ha evolucionado a través de sus diferentes versiones SNMPv1, SNMPv2 y SNMPv3 y las definiciones de cada una de éstas, en cuanto a sus componentes, lo que permitirá grandes mejoras y mayor flexibilidad en cuanto al control de acceso, así como la utilización de mecanismos para conseguir autenticación, integridad de los mensajes y privacidad; sin embargo el principio de la arquitectura ha permanecido consistente.

#### **3.3.1 SNMPv1**

El protocolo Snmpv1 fue diseñado a mediados de los 80 como una solución a los problemas de comunicación entre diferentes tipos de redes.

En un principio, su principal meta era el lograr una solución temporal hasta la llegada de protocolos de gestión de red con mejores diseños y mas completos. Pero esos administradores de red no llegaron y SNMPv1 se convirtió en la única opción para la gestión de red.

El manejo de este protocolo era simple, se basaba en el intercambio de información de red a través de mensajes PDU's (Protocol Data Unit, Unidad de Datos de Protocolos). Además de ser un protocolo fácilmente extensible a toda la red, debido a esto su uso se

estandarizo entre usuarios y empresas que no querían demasiadas complicaciones en la gestión de sus sistemas informáticos dentro de una red.

No obstante este protocolo no era perfecto, además no estaba pensado para poder gestionar la inmensa cantidad de redes que cada día iban apareciendo.

La versión 1 SNMPV1 es la puesta en práctica inicial del protocolo del SNMP. Se describe en el RFC 1157 (Request For Comments, Comentarios para Respuestas) y funciones dentro de lo especificado del SMI (Structure of Management Information, Información de Gestión Estructurada).

SNMPv1 funciona con protocolos excesivos tales como UDP (User Datagram Protocol, Protocolo de Datagramas de Usuario), IP (Internet Protocol, Protocolo de Internet), el servicio de red sin conexión de la OSI (CLNS), el protocolo de la Datagrama-Entrega de Appletalk (DDP), y el intercambio del paquete del Internet de Novell (IPX).

SNMPv1 se utiliza y es extensamente el protocolo de hecho de la red de gestión en la comunidad del Internet.

#### **3.3.1.1 Información de Gestión Estructurada**

El SMI define las reglas para describir la información de la gerencia, usando el ASN.1.

El SMI SNMPv1 se define en RFC 1155.

El SMI hace tres especificaciones dominantes:

- Tipos de datos ASN.1,

- Tipos de datos SMI-específicos y,
- Tablas del MIB del SNMP.

#### **3.3.1.1.1 SNMPv1 y tipos de datos ASN.1**

El SMI SNMPv1 especifica que todos los objetos manejados tienen cierto subconjunto de tipos de datos del ASN.1 asociados a ellos.

Se requieren tres tipos de datos ASN.1: nombre, sintaxis, y codificación:

Los servicios del nombre como el identificador del objeto.

La sintaxis define el tipo de datos del objeto (por ejemplo, número entero o secuencia).

El SMI utiliza un subconjunto de las definiciones de sintaxis ASN.1.

Los datos de codificación describen cómo la información asociada a un objeto manejado se ajusta a formato como serie de artículos de datos para la transmisión sobre la red.

#### **3.3.1.1.2 SNMPv1 y tipos de datos SMI Específicos**

El SMI SNMPV1 especifica el uso de un número de tipos de datos SMI específicos, que se dividen en dos categorías: tipos de datos simples y tipos de datos uso-anchos.

Tres tipos de datos simples se definen en el SMI SNMPV1, que son valores únicos: números enteros, secuencias del octeto, e identificaciones del objeto.

Existen siete tipos de datos en el SMI SNMPv1: direcciones de red, contadores, galgas, señales del tiempo, opaques, números enteros, y enteros sin signo.

Las **direcciones** de red representan una dirección de una familia particular del protocolo. SNMPv1 apoya solamente direcciones 32-BIT del IP.

Los **contadores** son los números enteros no negativos que aumentan hasta que alcanzan un valor máximo y después vuelven a cero. En SNMPv1, se especifica un tamaño contrario 32-BIT.

Las **galgas** son los números enteros no negativos que pueden aumentar o disminuir pero que conserve el valor máximo alcanzado.

Una **señal del tiempo** representa un centésimo de un segundo desde un cierto acontecimiento.

Un **opaco** representa una codificación arbitraria que se utilice para pasar las secuencias arbitrarias de la información que no se conforman con mecanografiar terminante de los datos usado por el SMI.

Un **número entero** representa la información número-valorada firmada. Este tipo de datos redefine el tipo de datos del número entero, que tiene la precisión arbitraria en ASN.1 pero precisión limitada en el SMI.

Un **entero sin signo** representa la información número-valorada sin firmar y es útil cuando los valores son siempre no negativos. Este tipo de datos redefine el tipo de datos del número entero, que tiene la precisión arbitraria en ASN.1 pero precisión limitada en el SMI.

### 3.3.1.1.3 Tablas del MIB del SNMP

El SMI de SNMPv1 define las tablas altamente estructuradas que se utilizan para agrupar los casos de un objeto tabular; es decir, un objeto que contiene variables múltiples. Las tablas se componen de cero o más fila, que se ponen en un índice de una manera que permita que el SNMP recupere o altere una fila entera con un solo GetNext o el comando determinado.

#### **3.3.1.2 Operaciones Del Protocolo SNMPv1**

El SNMP es un protocolo simple de request/response. El sistema de la red-gerencia publica una petición, y respuestas de vuelta manejadas de los dispositivos. Este comportamiento es puesto en ejecución usando una de cuatro operaciones del protocolo:

Consiga, GetNext, sistema, y trampa. La operación del conseguir es utilizada por los nanómetros para recuperar el valor de unos o más casos del objeto de un agente. Si el agente que responde a la operación del conseguir no puede proporcionar los valores para todo el objeto cita como ejemplo en una lista, él no proporciona ningunos valores. La operación de GetNext es utilizada por los nanómetros para recuperar el valor del caso siguiente del objeto en una tabla o una lista dentro de un agente. La operación del sistema es utilizada por los nanómetros para fijar los valores de los casos del objeto dentro de un agente. La operación de la trampa es utilizada por los agentes asincrónicos para informar a los nanómetros un acontecimiento significativo.

### **3.3.2 SNMPv2**

De SNMPv1, para reducir la carga de tráfico adicional para la monitorización con los GetBulk e Informs y solucionar los problemas de monitorización remota o distribuida con las RMON, ha dado paso a una nueva versión v2 en 1993.

Las versiones de SNMP son compatibles, en el sentido que SNMPv2 puede leer SNMPv1.

La versión 2 del SNMP es una evolución de la versión inicial, SNMPv1. originalmente, SNMPv2 fue publicada como sistema de estándares propuestos del Internet en 1993; actualmente, es un estándar de bosquejo. Como con SNMPv1, SNMPv2 funciona dentro de lo especificado del SMI. En teoría, SNMPv2 ofrece un número de mejoras a SNMPv1, incluyendo operaciones adicionales del protocolo.

#### **3.3.2.1 Mejoras en SNMPv2**

- Introducción de mecanismos de seguridad, totalmente ausentes en la versión 1. Estos mecanismos protegen la privacidad de los datos, confieren autenticación a los usuarios y controlan el acceso.
- Mayor detalle en la definición de las variables.
- Operaciones con grandes volúmenes: se incorpora una PDU (Protocol Data Units, Unidad de datos de Protocolos) GetBulkRequest. Esta PDU proporciona a las estaciones administradoras la posibilidad de trabajar con grandes cantidades de datos, de una sola vez, como grandes tablas.

- Comunicación entre administradores: Inform\_Request PDU, facilita la comunicación entre diferentes estaciones administradoras, permitiendo la existencia de jerarquías que son necesarias en sistemas muy complejos.
- Mejoras en las adquisiciones: en versión 1 cuando una de las variables en la lista de un comando GET fallaba, hacia que todo el comando fallara, obligando a eliminar esta variable de la lista y volver a consultar. En SNMPv2 este procesamiento es automático, y el error se indica en el valor de retorno de la variable.
- Mejoras en monitorización remota: en redes que no están conectadas directamente a la estación de administración
- SNMP gestiona dispositivos individuales, pero no permite diagnosticar fallos en una red remota u otro segmento de red. Para ello, el software de monitorización debe trasladarse a cada segmento de red. Esto se puede resolver mediante el uso de agentes en los segmentos remotos de red, utilizando equipos especiales o bien ordenadores de propósito general, llamados sondas RMON

### **3.3.3 SNMPv3.**

SNMPv1 utiliza como mecanismo de autenticación o validación un parámetro llamado comunidad, de forma que si el agente y la estación administradora lo conocen, pueden interactuar. Pero esta protección es muy débil porque el texto va en claro y además puede explotarse en fuerza bruta. Por tanto, para evitar la falta de seguridad en las

transmisiones con cifrado y autenticación, se ha creado una capa o parche complemento a SNMPv1 y v2 llamado versión v3, que añade a los mensajes SNMP (v1 y v2) una cabecera adicional.

Si no se dispone de seguridad suficiente, carácter general es aconsejable deshabilitar la ejecución de comandos SET por temas seguridad.

En 1996 se estandarizó la versión 3. Con dos ventajas principales sobre sus predecesores:

- Añade algunas características de seguridad como privacidad, autenticación y autorización a la versión 2 del protocolo.
- Uso de Lenguajes Orientados a Objetos para la construcción de los elementos propios del protocolo (objetos). Estas técnicas confieren consistencia y llevan implícita la seguridad, por lo que ayudan a los mecanismos de seguridad.

### **3.4 FUNCIONAMIENTO SNMP**

- a) Que la estación administradora envíe una solicitud a un agente, proceso que atiende petición SNMP, pidiéndole información o mandándole actualizar su estado de cierta manera. Este método se conoce como **SONDEO** o **POLLING**. Ver Gráfico 2
- b) La información recibida del agente es la respuesta o la confirmación a la acción solicitada. El problema del sondeo que se incrementa con los nodos administrados y en ocasiones puede llegar a perjudicar el rendimiento de la red. Ver Gráfico 2

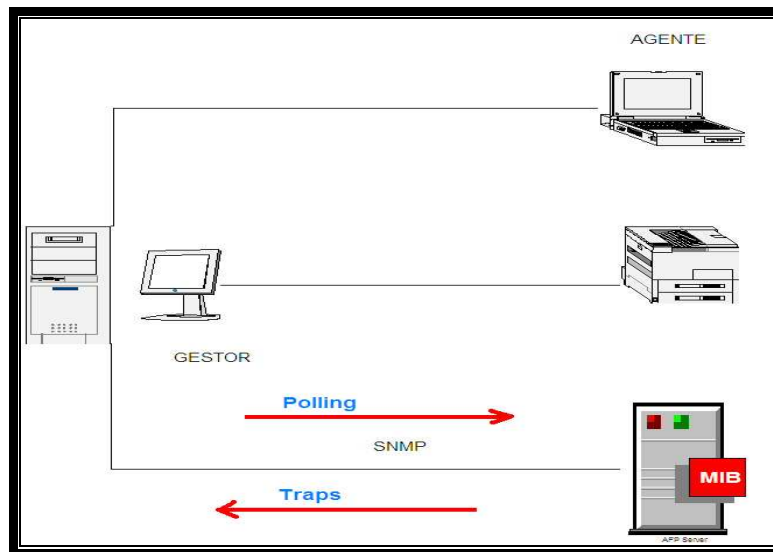


**Gráfico 2. Solicitud de la Estación al Agente**

Es mejor que un agente pueda mandar la información al nodo administrador puntualmente, ante una situación predeterminada, por ejemplo una anomalía detectada en la red. Este método es conocido como **interrupción**.

SNMP es independiente del protocolo (IPX de SPX/IPX de Novell, IP con UDP.), SNMP se puede implementar usando comunicaciones UDP o TCP, pero por norma general, se suelen usar comunicaciones UDP en la mayoría de los casos. Con UDP, el protocolo SNMP se implementa utilizando los puertos 161 y 162. El puerto 161 se utiliza para las transmisiones normales de comando SNMP, mientras que el puerto número 162 se utiliza para los mensajes de tipo TRAP o interrupción.

### **3.5 COMPONENTES BÁSICOS DEL SNMP**

SNMP está formado por cuatro componentes básicos:

- a) Base de datos lógica: SNMP sigue el modelo de una base de datos lógica, en la misma se almacena información referente a la configuración, estado, error y rendimiento.
- b) Agentes: El agente es un software, que permite el acceso a la información. Dicho agente responde a peticiones, realiza actualizaciones e informa los problemas.
- c) Administradores: La estación de administración, contiene un software de administrador, el cual se encarga de enviar y recibir los mensajes SNMP. Además de esto existen otra serie de aplicaciones de administración que se comunican con los sistemas de red mediante el administrador.
- d) Base de información de administración: La base de información de administración, denominada MIB, constituye la descripción lógica de todos los datos de administración de la red. La MIB contiene información de estado y del sistema, estadísticas de rendimiento y parámetros de configuración.

Por consiguiente, el protocolo SNMP tiene una arquitectura cliente servidor distribuida, como se ilustra en el Gráfico 3.

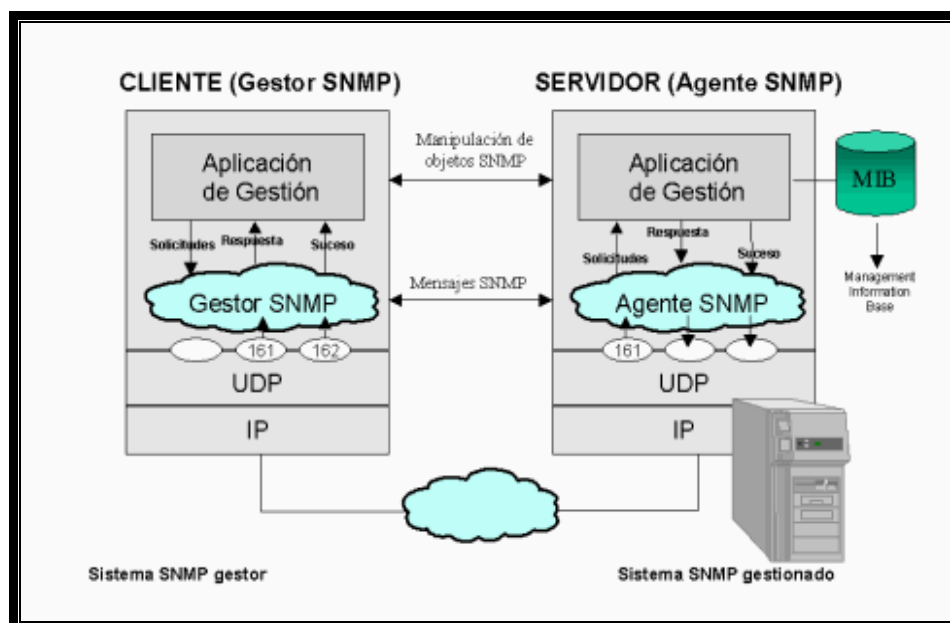


**Gráfico 3 Esquema de una Red Gestionada con SNMP**

La parte servidora de SNMP consiste en un software SNMP gestor, responsable del sondeo de los agentes SNMP para la obtención de información específica y del envío de peticiones a dichos agentes solicitando la modificación de un determinado valor relativo a su configuración.

Es decir, son los elementos del sistema de gestión ubicados en la plataforma de gestión centralizada de red, que interaccionan con los operadores humanos y desencadenan las acciones necesarias para llevar a cabo las tareas por ellos invocadas o programadas.

La parte cliente de SNMP consiste en un software SNMP agente y una base de datos con información de gestión o MIB. Los agentes SNMP reciben peticiones y reportan información a los gestores SNMP para la comunidad a la que pertenecen; siendo una comunidad, un dominio administrativo de agentes y gestores SNMP. Es decir, son los

elementos del sistema de gestión ubicados en cada uno de los dispositivos a gestionar, e invocados por el gestor de la red.

El principio de funcionamiento reside, por consiguiente, en el intercambio de información de gestión entre nodos gestores y nodos gestionados. Habitualmente, los agentes mantienen en cada dispositivo gestionado información acerca de su estado y su configuración.

El gestor pide al agente, a través del protocolo SNMP, que realice determinadas operaciones con estos datos de gestión, gracias a las cuales podrá conocer el estado del recurso y podrá influir en su comportamiento.

Cuando produce alguna situación anómala en un recurso gestionado, los agentes, sin necesidad de ser invocados por el gestor, emiten los denominados eventos o notificaciones que son enviados a un gestor para que el sistema de gestión pueda actuar en consecuencia.

### **3.6 COMANDOS BÁSICOS DEL SNMP**

El gestor SNMP puede lanzar cualquiera de estos tres comandos sobre un agente SNMP:

- **Get.** Una petición por el valor específico de un objeto en la MIB del agente. Este comando es utilizado por el gestor para monitorizar los dispositivos a gestionar.

- **Get-next.** Una petición por un valor en el siguiente objeto en la MIB del agente. Este comando es utilizado para obtener cada valor sucesivo en un subconjunto o rama de la MIB.
- **Set.** Utilizado para cambiar el valor de un objeto en la MIB de un agente, en el caso de que el objeto tenga habilitada la lectura y escritura de su valor.

Debido a la limitada seguridad de SNMP, la mayoría de los objetos de la MIB sólo tienen acceso de lectura. Este comando es utilizado por el gestor para controlar los dispositivos a gestionar.

Por otro lado, un agente SNMP podría también mandar un mensaje a un gestor SNMP sin el envío previo de una solicitud por parte de éste. Este tipo de mensaje es conocido como Trap. Los Traps son generalmente enviados para reportar eventos, como por ejemplo el fallo repentino de una tarjeta del dispositivo gestionado.

El protocolo SNMP debe tener en cuenta y ajustar posibles incompatibilidades entre los dispositivos a gestionar. Los diferentes ordenadores utilizan distintas técnicas de representación de los datos, lo cual puede comprometer la habilidad de SNMP para intercambiar información entre los dispositivos a gestionar. Para evitar este problema, SNMP utiliza un subconjunto de ASN.1 en la comunicación entre los diversos sistemas.

### 3.7 CONSTRUCCIÓN DEL MENSAJE DEL SNMP

Cada mensaje del SNMP tiene el formato:

- a) Número De Versión.
- b) Nombre de la comunidad - clase de una contraseña.
- c) Uno o más SNMP PDUs - autenticación trivial asumida.

Cada PDU del SNMP excepto trampa tiene el formato siguiente:

- a) Identificación de la petición - número de serie de la petición
- b) Estado de error - cero si ningún error de otra manera uno de un sistema pequeño.
- c) El índice del error - si no es cero indica cuál del OIDs en la PDU causó el error<sup>2</sup>
- d) Lista OIDs y valores - los valores son nulos para de consiguen y del consiguen después.

La trampa PDUs tiene el formato siguiente:

- a) Empresa - identifica el tipo de objeto que causa la trampa.
- b) Dirección del agente - IP ADDRESS del agente que envió la trampa.
- c) Identificación genérica de la trampa - las trampas comunes del estándar.
- d) Identificación específica de la trampa - trampa del propietario o de la empresa.
- e) Grupo fecha/hora - cuando hace tictac la trampa ocurrió en tiempo.
- f) Lista de OIDs y de los valores - OIDs que puede ser relevante de enviar a los nanómetros.

### 3.8 ARQUITECTURA

La Arquitectura de Administración de Red se compone de cuatro componentes principales: como se muestra en el Gráfico 4.

- Estación de administración de gestión.
- Agente de administración
- Base de datos de administración de gestión
- Protocolo de administración de gestión de red

a) **Estación de administración:** Ejecuta aplicaciones de administración y monitoreo sobre los elementos administrados. Es la interfase del administrador de red en el sistema. Contiene el software de gestión, y mantiene una base de datos denominada MIB con formato SMI.

Es un dispositivo que sirve como interfase entre la persona encargada de la administración de la red y el sistema de gestión de red.

Esta estación debe tener como mínimo:

- Un conjunto de aplicaciones de gestión para análisis de datos, recuperación de fallas, detección de alarmas, estadísticas, etc.
- Una interfase a través de la cual la persona encargada de la administración de la red pueda monitorear y controlar la red.

- La capacidad de trasladar los requerimientos del administrador a los dispositivos remotos que conforman la red.
- Una base de datos de información de gestión de la red extraída a partir de las bases de datos de todas las entidades gestionadas en la red.

b) **Base de información de administración:** Es cualquier nodo de la red que contiene un agente SNMP, son elementos como: servidores, ruteadores, impresoras, etc., los cuales recopilan información administrable para la estación de Administración, tal que es accesada por medio del protocolo SNMP.

c) **Agente de administración del dispositivo administrado:** Reside en el elemento administrado, el cual toma la información de administración recopilada por este elemento y la traduce para que sea compatible con la estación de administración.

Es el proceso de los dispositivos que están siendo monitorizados. Puentes, Routers, hubs y switches.

Los elementos claves de una plataforma, como: hubs, routers, bridges y hosts pueden estar equipados con un agente de software el cual puede ser manejado desde una estación de gestión. El agente responde a solicitudes de información y de acción que provienen de la estación de gestión, y puede proveer asincrónicamente información importante a la estación de gestión que no ha sido solicitada (alarmas).

d) **Protocolo de administración:** Por medio del cual el elemento administrado proporciona la información de administración a la Estación de Administración.

SNMP facilita la comunicación entre la estación administradora y el agente de un dispositivo de red (o nodo administrado), permitiendo que los agentes transmitan datos estadísticos (variables) a través de la red a la estación de administración.

Protocolo de capa de aplicación diseñado para comunicar entre el Administrador y el Agente. Es el encargado de enlazar la estación de gestión y los agentes.

Cada uno de estos protocolos posee las siguientes capacidades claves:

- **Get:** habilita a la estación de gestión a recuperar el valor de un objeto de un agente.
- **Set:** habilita a la estación de gestión a modificar el valor de los objetos de un agente.
- **Notify:** habilita a un agente a notificar a la estación de gestión acerca de un evento significativo.

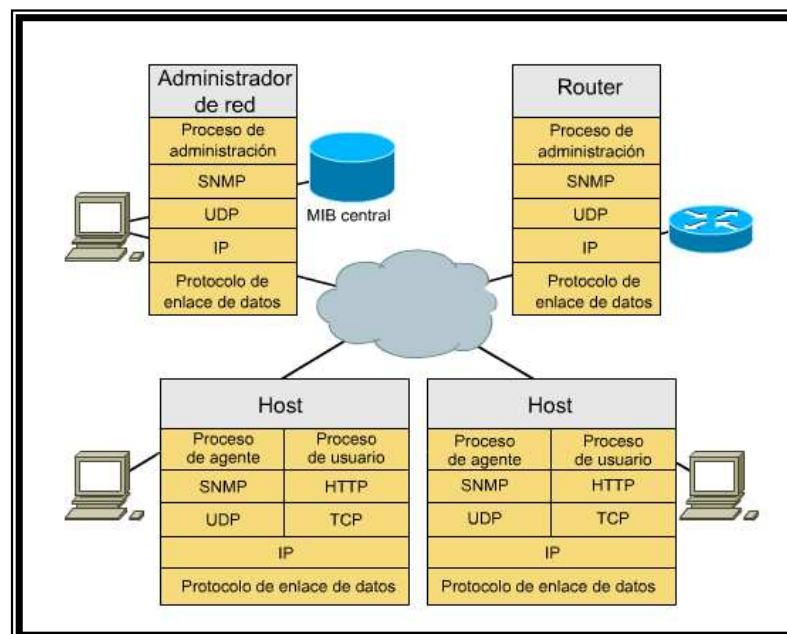


**Gráfico 4 Componentes de la Arquitectura de Red.**

### **3.9 ELEMENTOS DE LA ARQUITECTURA SNMP**

SNMP incorpora elementos presentes en otros estándares como el modelo GESTOR – AGENTE, una estructura para la definición de la información, la existencia de una base de datos con información de la gestión, o el uso de primitivas del tipo PUT y GET para manipular dicha información y el protocolo de comunicaciones SNMP.

A continuación la descripción de estos elementos:

Estructura e identificación de la información sobre la administración (SMI): Una especificación que permite definir las entradas en una MIB.

- a) Agente: equipamiento lógico alojado en un dispositivo gestionable de la red. Almacena datos de gestión y responde a peticiones sobre dichos datos.
- b) Gestor: equipamiento lógico alojado en una estación de gestión de red. Tiene la capacidad de preguntar a los agentes utilizando diferentes comandos SNMP.
- c) MIB: base de datos virtual de los objetos gestionables, accesible por un agente, que puede ser manipulada vía SNMP para realizar la gestión de red.
- d) Protocolo simple para administración de la red (SNMP): El método de comunicación entre los dispositivos administrados y los servidores.

### **3.10 BASE CON INFORMACIÓN DE GESTIÓN**

Las características de los componentes de la red son representadas mediante objetos. Cada objeto es, en esencia, una variable de datos que representa un aspecto del agente

en cuestión. La colección de objetos se define como MIB (Base de Información de Gestión).

La estación de gestión ejecuta las funciones de monitoreo recuperando el valor de los objetos MIB, además, la estación de gestión puede ejecutar una acción que se ejecute en un agente, o puede cambiar la configuración original de un agente modificando el valor de variables específicas.

#### **3.10.1 Nodos administrados**

Los periféricos que tienen integradas las capacidades para SNMP corren un paquete pequeño de software **agente** para administración, generalmente de 64kB, cargado como parte de un ciclo de arranque o guardado en la memoria fija (firmware) del dispositivo.

Estos dispositivos que tienen agentes SNMP se dice que se tratan de dispositivos o nodos administrados. NO TODOS LOS NODOS SON AGENTES, NI PUEDEN SERLO.

#### **3.10.2 Agente Apoderado (o proxy)**

Gestiona los dispositivos que no pueden ejecutar un agente local localización: externo al dispositivo administrado.

Los dispositivos administrados por SNMP (puentes, routers, hubs y switches) se comunican con el software servidor SNMP que está localizado en cualquier parte de la red y les permitan ser controlados por la estación de administración.

El agente de administración responde a la estación de administración de dos maneras:

- **Mediante sondeo o pooling:** la estación de administración requiere datos desde el agente y el agente responde con los datos solicitados
- **Por interrupción:** tal que se establecen umbrales (límites superiores o inferiores) en el dispositivo administrado y si se supera este umbral en el dispositivo, envía un mensaje de alerta a la estación de administración.

En ocasiones se puede combinar ambos métodos, conocido como sondeo dirigido a interrupción.

### 3.10.3 Consola de administración

SNMP es un protocolo de capa de aplicación diseñado para comunicar datos entre la consola de administración y el agente de administración. Los comandos básicos que ejecuta son:

- **OBTENER (GET),** que implica que la consola de administración recupera datos del agente
- **COLOCAR (PUT),** que implica que la consola de administración establece los valores de los objetos en el agente
- **CAPTURAR (TRAP),** que implica que el agente notifica a la consola de administración acerca de los sucesos de importancia por interrupción.

### **3.11 PRIMITIVAS**

El SNMP define ocho mensajes que pueden enviarse:

- get request
- get next request
- get bulk request (en snmp v2)
- set request
- set next request
- get response
- trap
- inform request (en snmp v2)

La implementación de cada uno de estos mensajes lo tenemos en Linux a través de las siguientes funciones: `snmpget`, `snmpgetnext`, `snmpgetbulk` y `snmpset`.

#### **3.11.1 Get Request**

- Solicita uno o más (lista) atributos (valores) de un objeto (o variable).
- Transmitida por el nodo administrador
- Recibida por el agente que contesta

### **3.11.2 Get Next Request**

- Solicita el siguiente atributo de un objeto
- Transmitida por el nodo administrador
- Recibida por el agente que contesta

### **3.11.3 Get Bulk Request**

- Solicita un conjunto amplio de atributos en vez de solicitar uno a uno
- Transmitida por el nodo administrador
- Recibida por el agente

### **3.11.4 Set Request**

- Actualiza uno o varios atributos de un objeto
- Transmitida por el nodo administrador
- Recibida por el agente

### **3.11.5 Set next request**

- actualiza el siguiente atributo de un objeto
- transmitida por el nodo administrador
- recibida por el agente

#### **3.11.6 Get Response**

- Devuelve los atributos solicitados
- Transmitida por el agente
- Recibida por el nodo administrador

#### **3.11.7 Trap**

- Informa fallos como la pérdida de comunicación con un vecino
- Transmitida por el agente
- Recibida por el nodo administrador

#### **3.11.8 Inform Request**

- Describe la base local de información de gestión MIB para intercambiar información nodos de administración entre si.
- Transmitida por el nodo administrador.
- Recibida por otro nodo administrador.

### **3.12 MONITORIZACIÓN INTELIGENTE**

Mediante SNMP, un router puede reportar un incremento de la carga cada 10 %. Si utiliza un sondeo dirigido por interrupción y se conoce la carga del sondeo regular,

puede dar instrucciones al router para enviar una interrupción cuando se experimente un incremento significativo en la carga 10%.

Después de recibir un mensaje de interrupción, el servidor puede seguir sondeando al dispositivo para mayores detalles.

Otro caso de configuración, cuando el router de salida con acceso a Rediris tiene tráfico de salida superior a 34 Mbps, que mande al administrador de la red notificación o alerta.

### **3.13 SNMP Y CONGESTIÓN**

La monitorización se realiza por la propia red, por tanto si la red está congestionada, puede conllevar más problemas.

Si existe una fallo general en cualquier parte de la red, por ejemplo fallo de la corriente eléctrica, cada dispositivo administrado por SNMP tratará de enviar al mismo tiempo, mensajes controlados por interrupción hacia el servidor, para reportar el problema. Esto puede congestionar la red y producir una información errónea en el servidor.

### **3.14 VENTAJA PRINCIPAL DE SNMP**

La principal ventaja de SNMP para los programadores de herramientas de gestión de red, es su sencillez frente a la complejidad inherente a CMIP.

CMIP resuelve la mayor parte de las muchas limitaciones de SNMP, pero por contra, consume mayores recursos (alrededor de 10 veces más que SNMP), por lo cual es poco utilizado en las redes de telecomunicación empresariales.

Puesto que la consulta sistemática de los gestores, es más habitual que la emisión espontánea de datos por parte de los agentes cuando surgen problemas, SNMP es un protocolo que consume un considerable ancho de banda, lo cual limita su utilización en entornos de red muy extendidos. Esto es una desventaja de SNMP respecto a cualquier red manejada.

## **4 CAPITULO VI: RMON (Remote Network Monitor, Monitor de Red Remoto)**

### **4.1 CONCEPTO**

RMON define una MIB que amplía las funcionalidades ofrecidas por MIB-II sin la necesidad de realizar cambios en el protocolo de gestión SNMP. Con la MIB RMON se puede obtener información sobre la red misma, y no sobre los dispositivos conectados a la red como es el caso de MIB-II.

RMON es un protocolo para la monitorización remota de redes. Un agente RMON, denominado también monitor o sonda RMON, recogerá información de gestión, principalmente estadísticas del tráfico, sobre la red entera, y las pone a disposición de las estaciones de gestión.

Las sondas RMON recopilan información y tiene la misma función que un agente SNMP, transmitiendo la información periódicamente. Además, pueden procesar la información a enviar a la estación de administrador.

### **4.2 INTRODUCCION**

Una de las mejoras principales de SNMP se denomina Monitoreo Remoto RMON.

Las extensiones de RMON a SNMP brindan la capacidad para observar la red como un todo, aunque este distribuida, en contraste con el análisis de dispositivos individuales,

declarándose para ello una MIB especial para guardar información de monitorización de un segmento de red diferente. La MIB asociada es 1.3.6.1.2.1.16.

RMON esta localizada en cada segmento de la red y pueden introducirse en un host, en un switch, en un router o en un dispositivo específico para ello. Además, permite añadir redundancia a la administración de la red, ya que RMON permite volcar los datos a varias consolas de administración. Ver Gráfico 5

**RMON1** trabaja en información de capa 1 y 2.

**RMON2** trabaja en información de capa 3 y superiores. Ver Gráfico 5

El software para administración de la red permite al administrador supervisar y controlar los componentes de la misma; por ejemplo, permite que el administrador investigue dispositivos como hosts, enrutadores, conmutadores y puentes para determinar su estado y obtener estadísticas sobre las redes a las que se conectan. Además permite controlar tales dispositivos cambiando las rutas y configurando interfaces de red.

RMON proporciona un nivel más alto de información que SNMP. Cuando un dispositivo lo soporta, RMON se ejecuta continuamente y permite al administrador de la red ver estadísticas, configurar condiciones de alarma que puedan emitir trampas o anotarse en una tabla y marcar ciertos eventos cuando tienen lugar.

SNMP gestiona dispositivos individuales, pero no permite diagnosticar fallos en una red remota u otro segmento de red.

Para ello, el software de monitorización debe trasladarse a cada segmento de red.

Esto se puede resolver mediante el uso de agentes en los segmentos remotos de red, utilizando equipos especiales o bien ordenadores de propósito general, llamados sondas RMON.

RMON se popularizará tan pronto como los nuevos conmutadores y circuitos integrados incorporen soporte para RMON.

La MIB definida para SNMP nos permite obtener información de gestión acerca de un único nodo: el que ejecuta el agente SNMP. Si quisiéramos obtener información acerca de una red como un todo, deberíamos realizar sucesivas consultas individuales a cada nodo conectado en la red. Esto supone un gran consumo de recursos (tiempo de procesamiento en agentes y el gestor, y ancho de banda consumido por las consultas/respuestas SNMP), con esa motivación surge RMON.

El MIB de RMON proporciona un método estándar para vigilar las operaciones básicas de Ethernet. RMON también proporciona un mecanismo para notificarle de cambios en el comportamiento de la red.

Se puede utilizar RMON para analizar y para vigilar datos del tráfico de la red dentro de segmentos alejados de la LAN. Esto permite detectar, aislar, diagnosticar, y señalar problemas potenciales y reales de la red antes de que se extiendan a las situaciones de crisis.

RMON permite instalar las historias automáticas, que el agente de RMON recoge durante todo el tiempo, proporcionando datos en la estadística básica tal como la utilización, colisiones. RMON automatiza esta colección de datos y proporciona a otros datos del proceso las hojas de operación (planning), el proceso es más fácil y el resultado más exacto.

### **4.3 EVOLUCIÓN.**

RMON fue desarrollado originalmente para tratar el problema de manejar segmentos de la LAN y sitios alejados de una localización central. La especificación de RMON, que es una extensión del MIB del SNMP, es una especificación de supervisión estándar. Dentro de RMON una red que supervisa datos es definida por un sistema de estadística y de funciones e intercambiada entre los varios diversos monitores y sistemas de la consola. Los datos resultantes se utilizan para supervisar la utilización, el planeamiento y funcionamiento de la red, así como también diagnosticar la avería de la misma.

Hay 2 versiones de RMON: RMON1 (RMONv1) y RMON2 (RMONv2). RMON1 define 10 grupos del MIB para la red básica que supervisa, que se puede encontrar en la mayoría del hardware moderno de la red.

RMON2 (RMONv2) es una extensión de RMON que se centra en capas más altas de tráfico sobre la capa media del control de acceso (MAC). RMON2 tiene un énfasis en tráfico del IP y tráfico del uso-nivel. RMON2 permite que los usos de la dirección de la

red supervisen los paquetes en todas las capas de red. Ésta es una diferencia de RMON que permite solamente que la red supervise en la capa del MAC o abajo.

Los RMON1 y los RMON2 se enfocan en diversas capas de red, como muestra en el Gráfico 5.

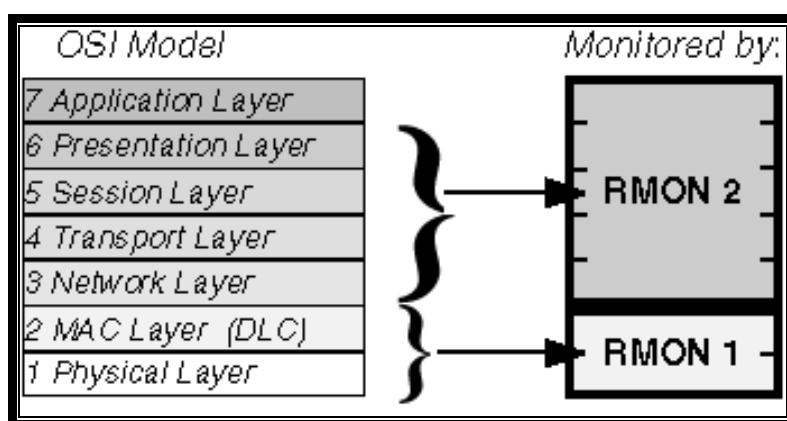


**Gráfico 5. RMON1 y RMON 2 en capas del Modelo OSI.**

#### **4.4 RMON1**

Consiste en el uso de un agente remoto para coleccionar información de gestión bajo demanda. Se diseñó para redes LAN Ethernet (posteriormente para Token Ring) y entregar las funcionalidades de los analizadores de redes y protocolos.

##### **4.4.1 Características**

- a) Operación Fuera de Línea: aún si se ha producido un fallo en la conexión entre el monitor RMON y la estación de gestión de red, el monitor continuará recolectando

información a cerca de la red (funcionamiento, tráfico, etc.). De esta manera, cuando se restaure la conexión con el gestor, el monitor enviará la información requerida por éste. Además, como el monitor recolecta la información estadística sin necesidad de que el gestor envíe constantemente pedidos, se logra reducir el tráfico de interrogación (polling), disminuyendo el ancho de banda necesario para gestión en la red.

- b) Detección y reporte de fallos: El monitoreo preventivo ofrece la posibilidad de detectar un fallo antes de que éste ocurra. Esto se logra mediante el análisis del funcionamiento del tráfico de la red. El monitor RMON puede configurarse para que detecte estos casos automáticamente, y en caso de ocurrir esta condición, la registra y envía un mensaje de notificación al gestor de red.
- c) Datos con valor agregado: El monitor de red puede realizar un análisis de la información recolectada de la subred que gestiona. Por ejemplo, puede reconocer las estaciones que generan mayor cantidad de tráfico, o las que generan mayor cantidad de errores en la red. Esta función no podría ser ejercida por el mismo gestor de red, salvo que se encontrara dentro de la misma subred.
- d) Múltiples Gestores de red: En casos donde la red es muy amplia y consta de muchas subredes puede ser necesario el uso de más de un gestor de red. El monitor de red puede ser configurado para que funcione correctamente con múltiples gestores de red.

Nota: no todos los monitores de red soportan estas características, pero la especificación provee el soporte para el uso de las mismas.

#### **4.4.2 Configuración**

La implementación consiste en una configuración Cliente/Servidor. El cliente es el equipo que presenta la información al usuario de la red de gestión. El servidor es el equipo que en forma remota reúne la información y análisis de paquetes; se lo denomina Probe y desarrolla el programa de software denominado RMON-Agent. El agente-RMON está empapado generalmente en los switchs y routers. El protocolo de comunicación es el SNMP. Los datos son coleccionados y procesados en el servidor remoto de forma que se reduce el tráfico SNMP en la red de datos. De esta forma un segmento de red LAN es gestionable desde cualquier lugar de la red.

La mejora que se ha introducido sobre SNMPv1 se relaciona con la base de datos MIB del RMON. En el MIB se dispone de 9 grupos con las funciones que se indican en el punto **3.12.** , donde cada uno provee funciones específicas para la gestión de la red. Estos grupos pueden implementarse en su totalidad, o sólo un conjunto de éstos.

Pero en el caso de implementar un grupo este debe implementarse en su totalidad. Cada grupo puede constar de una o más tablas de control y una o más tablas de datos. Generalmente las tablas de datos son solamente de lectura (el explorador RMON es el que se encarga de escribir los datos).

Las tablas de control son de lectura-escritura y contienen los parámetros necesarios para configurar los datos que aparecerán en las tablas de datos. Estos parámetros se configuran desde el gestor de red añadiendo filas a la tabla o modificando una fila ya existente. Para modificar un parámetro de la tabla de control debe invalidarse la fila correspondiente y crearse una nueva fila con los valores requeridos. Al invalidarse la fila de la tabla de control se eliminan automáticamente la fila de la tabla de control y las filas asociadas en la tabla de datos.

#### **4.4.3 Ventajas dominantes**

- a) Alta disponibilidad de la red para los usuarios y alta productividad para los administradores de la red.
- b) Un estudio reciente demostró que con la instrumentación de RMON, cuanto más grande es la red, más grande es el aumento en productividad.
- c) El estándar básico de RMON ha sido aceptado ampliamente por la industria de las comunicaciones del establecimiento de una red y de datos debido a las ventajas inmensas que esta tecnología puede entregar a los encargados de red. Sin embargo, especifica solamente la supervisión y el diagnóstico para el tráfico de la misma en la capa del MAC (transmisión de datos).

#### **4.4.4 Ejecución de Comandos Mediante la MIB RMON**

El protocolo SNMP no ofrece la posibilidad de enviar un comando a un agente para que realice una acción determinada, la única posibilidad que ofrece es la lectura y escritura

de objetos definidos dentro de una MIB. Sin embargo, pueden realizarse acciones en el agente mediante el comando Set de SNMP. Para esto se definen objetos que representan un comando en lugar de información. Al cambiar el valor del objeto se ejecuta una acción específica.

En la MIB RMON se definen varios objetos de este tipo. Estos objetos representan estados, y una acción se llevará a cabo cuando el gestor de red cambie el estado de uno de estos objetos.

#### **4.4.5 Gestores Múltiples**

Cuando un explorador RMON es compartido puede ser accedido desde diferentes gestores de red y pueden ocasionarse las siguientes dificultades:

- a) Si se realizan pedidos de varios gestores a la vez donde cada uno necesita cierta cantidad de recursos, y la suma de estos excede la capacidad del explorador RMON, éste no podrá entregar dichos recursos ocasionando que alguno de los pedidos no se lleven a cabo.
- b) Si una estación de gestión retiene recursos del monitor por un período largo de tiempo, puede provocar que otra estación de trabajo no pueda acceder a los datos de gestión por falta de recursos.
- c) Los recursos pueden estar asignados a un gestor que haya sufrido un fallo sin haber liberado estos recursos.

Para evitar este tipo de problemas la MIB RMON tiene para todas las tablas de control definidas una columna que identifica al propietario de la fila correspondiente. Este valor puede ser usado de las siguientes maneras:

- a) Un gestor puede reconocer los recursos que posee y ya no necesita, y de esta forma puede liberarlos.
- b) Un operador de red puede conocer qué gestor está utilizando determinados recursos o funciones y puede negociar por éstos para que sean liberados.
- c) Un operador puede tener la autorización para liberar recursos que otros operadores hayan reservado.
- d) Si un gestor ha sido reinicializado puede detectar los recursos que poseía anteriormente y liberar los que ya no necesitará.

Nota: La especificación de RMON sugiere que en la etiqueta de propietario se coloquen uno o más de los datos siguientes: dirección IP, nombre de la estación de gestión, lugar donde se haya la estación, nombre del administrador de red y el número telefónico.

La etiqueta de propietario no confiere ningún tipo de seguridad sobre los objetos asociados. Estos pueden ser leídos, modificados y borrados por cualquier gestor de red en caso de que los objetos tengan permisos de lectura y escritura.

Para mejorar la eficiencia del sistema en el uso de los recursos, en casos de gestores múltiples, pueden compartirse los valores obtenidos por el explorador RMON. Para que pueda llevarse a cabo esta mejora es necesario que cuando un gestor requiere

información, debe observar antes de solicitar los recursos necesarios por si otro gestor está pidiendo los mismos datos. Si es así, puede leer los datos de las filas de la tabla creadas por el otro gestor, sin gastar más recursos del explorador RMON. La desventaja de compartir recursos se da cuando el propietario de las filas de la tabla ya no necesita más la información y elimina las mismas, sin saber que estaban siendo utilizadas por otro gestor.

## **4.5 RMON 2**

RMON2 es una extensión a la MIB RMON que incluye la decodificación de paquetes pertenecientes a las capas 3 a 7 del modelo OSI.

### **4.5.1 Beneficios.**

- a) Un explorador RMON puede monitorear el tráfico en función de los protocolos y direcciones de capa de red. Esto permite al explorador observar los segmentos de LAN a los que está conectado y ver el tráfico entrante desde los routers.
- b) Como el explorador RMON puede decodificar y monitorear el tráfico a nivel de aplicación, como ser los protocolos de correo electrónico, transferencia de archivos (FTP, File Transfer Protocol, Protocolo de Transferencia de Archivos y WWW, World Wide Web), puede almacenar el tráfico entrante y saliente de los hosts para alguna aplicación en particular.

#### **4.5.2 Visibilidad de la capa de red mediante RMON2**

Con la MIB original de RMON, ahora llamaremos RMON1, se podía analizar el tráfico de una red y obtener las direcciones MAC de todos los hosts conectados al mismo segmento de red. Si en este segmento de Lan se conectaba un router, RMON1 sólo podía observarse el tráfico total, ya sea entrante o saliente del router, pero no podía analizarse el destinatario final de un paquete enviado a través del router o la fuente de un paquete que llega a la LAN a través del router.

Con RMON2, el explorador RMON ahora posee esta capacidad debido a que puede leer el encabezado del protocolo de red utilizado (el protocolo más común es IP). Con esta nueva capacidad del explorador RMON, el gestor de red puede resolver las siguientes cuestiones:

- a) En caso de que se esté recibiendo gran cantidad de tráfico desde el router, se puede determinar desde que red o host se está generando el tráfico.
- b) En caso de que se esté enviando gran cantidad de información a través del router puede determinarse que host local está generando la información y hacia que red se dirige el tráfico.
- c) En caso de detectarse gran cantidad de tráfico entre dos routers conectados al segmento de LAN donde se encuentra el explorador RMON, puede determinarse desde y hacia que red se está transportando la información.

Con esta información recolectada mediante la MIB RMON2 el gestor de red puede mejorar el funcionamiento de la red, reconfigurando la topología de la red y situar en el mismo segmento de red a los servidores y a los clientes que intercambien gran cantidad de tráfico entre sí.

#### **4.5.3 Visibilidad de la capa de aplicación mediante RMON2**

El explorador RMON2 es capaz de leer encabezados de las capas superiores a la capa de red como ser TCP (capa 4) hasta el nivel de capa de aplicación (capa 7). Se debe notar que en la especificación de RMON2 las capas superiores a la capa de red son llamadas en forma general capa de aplicación. Con esta nueva capacidad del explorador puede obtenerse información sobre el tráfico de la red diferenciándolo por protocolo y por aplicación, de esta manera puede controlarse la carga de la red y el funcionamiento de la misma.

#### **4.5.4 Características**

- RMON1 opera sobre LAN (capa 2) y RMON2 opera sobre las capas superiores. Con el incremento de las estadísticas de tráfico la potencia del procesador CPU y la capacidad de la memoria del agente se han incrementado.
- Disponen de dos tipos de soluciones: el tipo A ocupa menos memoria que el tipo B. El tipo A realiza funciones de Statistics/Host/Matrix sobre la capa 3 y Statistic solo en la capa de aplicación; el tipo B realiza las 3 funciones en las capas de red y aplicación.

- Contesta a la necesidad del análisis del tráfico de la red y localizar las averías en las capas más altas. Se construye sobre el principio que no requieren los usuarios y los recursos estar en el mismo segmento físico de la LAN. Cualquier usuario con los privilegios correctos puede tener acceso a cualquier recurso en la red.

#### **4.5.5 Una desventaja de las puntas de prueba de RMON1**

- No puede identificar los anfitriones y las fuentes de la red más allá de la conexión. Hacer así pues, un probe/agent debe ser capaz de identificar tráfico en la capa de red que proporcionará la estadística para todos los anfitriones que tienen acceso a ese segmento, no importa dónde ella se localiza o cómo la red está conectada.

RMON2 define la especificación para supervisar el tráfico de la uso-capa, que permite a administradores supervisar usos de la red tales como notas, telnet, Microsoft envía, Sybase, y otros.

RMON2 agrega lo siguiente:

- a) Tablas del anfitrión y de la matriz de la Red-capa para supervisar tráfico de la capa 3 por el anfitrión, por las conversaciones para los varios protocolos, y para las cualidades estándares de RMON tales como utilización, tarifa del paquete, errores, y otros.
- b) Tablas del anfitrión y de la matriz de la Uso-capa para supervisar tráfico de la capa 7 por el anfitrión, por las conversaciones para los varios usos, y para las cualidades estándares de RMON tales como utilización, tarifa del paquete, y errores.

- c) El Traz de dirección de red para agregar la estadística por la dirección de red tan bien como el MAC address para las redes de Ethernet y del token ring.
- d) Grupos del directorio y de la distribución del protocolo para exhibir protocolos seleccionados y su distribución para cada segmento del LAN.
- e) Historia Usuario-definible, que ahora extiende más allá de estadística del acoplamiento-capa RMON1 para incluir cualquier estadística de RMON1, de RMON2, de MIB-I o de MIB-II.

Incluye la definición de los métodos para remotamente mantener y configurar las puntas de prueba para los mensajes de la trampa, las comunicaciones del módem, y las actualizaciones del software.

#### **4.6 RMON MIB**

Algunos documentos del Management Information Base (MIB) han avanzado más allá de la reunión de los datos para la entrega a una estación de la gerencia. Esta nueva generación de MIBs crea un nuevo nivel de la inteligencia dentro del agente del SNMP. Sin embargo, esta generación del pensador MIBs es mucho más difícil de poner en ejecución correctamente, requiriendo más que las herramientas o los recopiladores del MIB que eran suficientes para la generación primera de MIBs.

Cada MIB se puede utilizar con SNMPv1, SNMPv2c, o los agentes SNMPv3, o los agentes trilingües, los agentes que apoyan las tres versiones.

#### 4.6.1 Características.

a) Apoya a los nueve grupos de RMON:

- Estadística. (statistics), Historia. (history), Alarmar (alarms), Anfitriones (host), Anfitrión N superior. (hostTopN), Matriz del tráfico. (matriz), Filtros. (filter), Captura del paquete. (capture), Acontecimientos. (event)

b) El SNMP de las ayudas consigue, getNext, y las utilidades del getbulk de SNMPv2c para los nueve grupos. Se apoyan, el sistema y la trampa dondequiera que sean útiles.

En la RFC 1513 se definen extensiones en la MIB RMON para la gestión de redes tipo Token Ring. Esta extensión consiste en el agregado de nuevas tablas en los grupos ya existentes, statistics y history, y el agregado de un nuevo grupo: **tokenRing**

Los diez grupos son opcionales para la implementación de RMON. Sin embargo, existen algunas dependencias que se detallan a continuación:

- El grupo alarm necesita la implementación del grupo event.
- El grupo hostTopN necesita la implementación del grupo host.
- El grupo packet capture necesita la implementación del grupo filter.

#### **4.7 CARACTERISTICAS GENERALES**

RMON es un estándar que define objetos actuales e históricos de control, permitiendo capturar la información en tiempo real a través de la red.

- a) RMON es una base de información de gestión MIB desarrollada para proporcionar capacidades de monitorización y análisis de protocolos en redes de área local o segmentos de red. Esta información proporciona a los gestores una mayor capacidad para poder planificar y ejecutar una política preventiva de mantenimiento de red.
- b) El MIB de RMON proporciona un método estándar para vigilar las operaciones básicas de Ethernet. RMON también proporciona un mecanismo para notificar los cambios en el comportamiento de la red.
- c) RMON se puede utilizar para analizar y para vigilar datos del tráfico de la red dentro de segmentos alejados de la LAN. Esto permite detectar, aislar, diagnosticar, y señalar problemas potenciales y reales de la red antes de que
- d) Se extiendan a las situaciones de crisis.

RMON permite instalar las historias automáticas, que el agente de RMON recoge durante todo el tiempo, proporcionando datos en la estadística básica tal como la utilización y colisiones. RMON automatiza esta colección de datos y proporciona a otros datos del proceso las hojas de operación (planning), el proceso es más fácil y el resultado más exacto.

#### 4.8 ADMINISTRACIÓN DE RED CON RMON

Los datos de administración recolectados por un MONITOR DE RED son enviados a las estaciones de administración.

La localización de los monitores de red es dependiente de la implementación: puede colocarse un monitor de red por segmento, por subred, o por red token-ring.

Los monitores remotos de red se ubican en los AGENTES RMON, que proveen funciones tales como soporte de protocolos de comunicación con las estaciones de administración y recuperación de errores, y actúan como INTERMEDIARIOS entre los monitores de red y las estaciones de administración. Para transferir los datos a las estaciones de administración pueden usar protocolos snmpv1 o snmpv2. Ver Gráfico 6

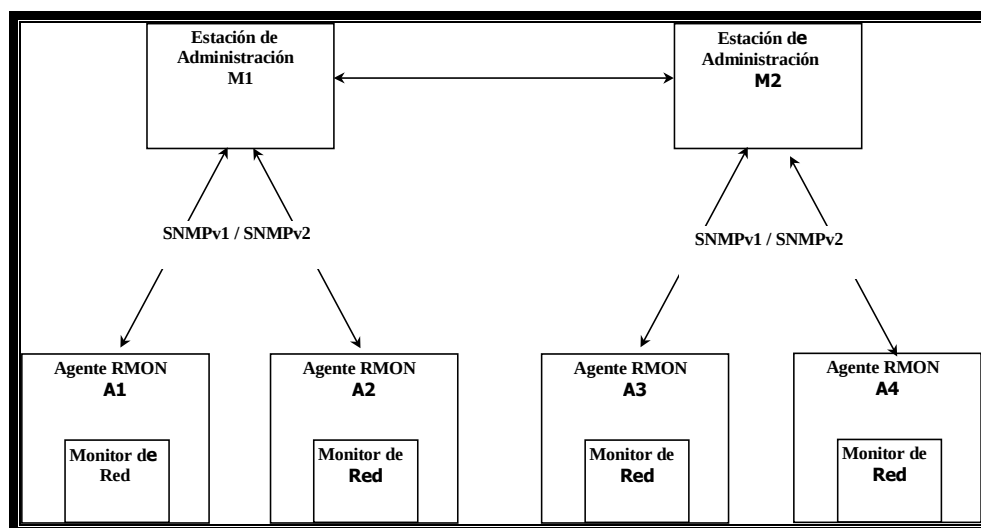


**Gráfico 6. Estaciones de Administración y RMON**

Un agente RMON con un monitor remoto de red puede enviar datos a una o más estaciones de administración; además, pueden ubicarse en hosts, routers y bridges

El tener un monitor exclusivamente para propósitos de administración de red tiene sus ventajas:

- a) El monitor de red puede recolectar datos continuamente y enviarlos selectivamente a las estaciones de administración.
- b) Cuando se cruzan umbrales, se pueden generar eventos y enviar alarmas a las estaciones administrativas.
- c) Puede ayudar a reducir el tráfico de red, ya que los datos recopilados se almacenan en los agentes con monitores de red (en vez de tener que transmitirlos a cada uno); cuando la estación administradora necesita más detalles, puede acceder y recolectar la información desde los agentes con RMONS.

#### **4.9 ESCENARIOS PARA MONITOREO REMOTO DE REDES**

RMON puede usarse en los siguientes escenarios:

Operación Fuera de Línea: se da cuando el monitor de red opera como un dispositivo de monitoreo stand-alone (único, independiente), ya sea por fallas de comunicación con la estación de administración, o para recolección selectiva de datos. El RMON puede operar independientemente de la estación administradora: puede recolectar y almacenar

datos continuamente; la estación de administración puede recuperar los datos almacenados cada vez que lo requiera.

Comunicación con estaciones de administración en base a excepciones: Cuando se observan problemas en la red, debido a que se cruzan umbrales o por fallas, se pueden enviar notificaciones a las estaciones de administración. El RMON puede reunir datos a cerca de la red y almacenarlos en un registro para analizarlos más tarde.

Recopilación de datos relevantes: Un monitor puede concentrarse en hosts de una porción de red (críticos, que tienen mucho tráfico o errores) o en loggear los datos requeridos por la estación administradora.

Múltiples estaciones de administración: Si las estaciones de administración se organizaran en base a las acciones que realizan, podría necesitarse que un monitor trate concurrentemente con más de una estación de administración para reportarse. La descomposición por funciones (contabilidad, configuración, funcionamiento, etc.) puede ayudar a centralizar en una estación administradora los datos requeridos para ciertas funciones de administración.

#### **4.10 RMON PARA ETHETNET**

Los objetos definidos en la MIB RMON son principalmente para el protocolo Ethernet y puede ser expandida para cubrir los protocolos Token-Ring y FDDI.

Los objetos RMON se definen usando los lineamientos provistos en SMI (RFC 1155). Sin embargo, además de los tipos de datos ASN.1 definidos en el SMI, RMON define otros 2 tipos, cuyo objetivo principal es facilitar la compartición (sharing) de recursos:

**Owner String, Secuencia Propia (DisplayString, Secuencia Desplegada):** contiene información usada para identificar los propietarios de un recurso (dirección. IP, nombre de la estación administradora, nombre del administrador de red, número de teléfono, etc.), y ayuda a resolver conflictos cuando más de una estación de administración es propietaria de un recurso.

**Entry Status, Estado de Entrada (INTEGER):** útil cuando un recurso es compartido por más de un propietario, ayuda a determinar cuándo existe una instancia de objeto.

Para RMON se definieron nuevos grupos de objetos, bajo el subárbol {mib-2 16} de la jerarquía de registración. **Ver Gráfico 7**

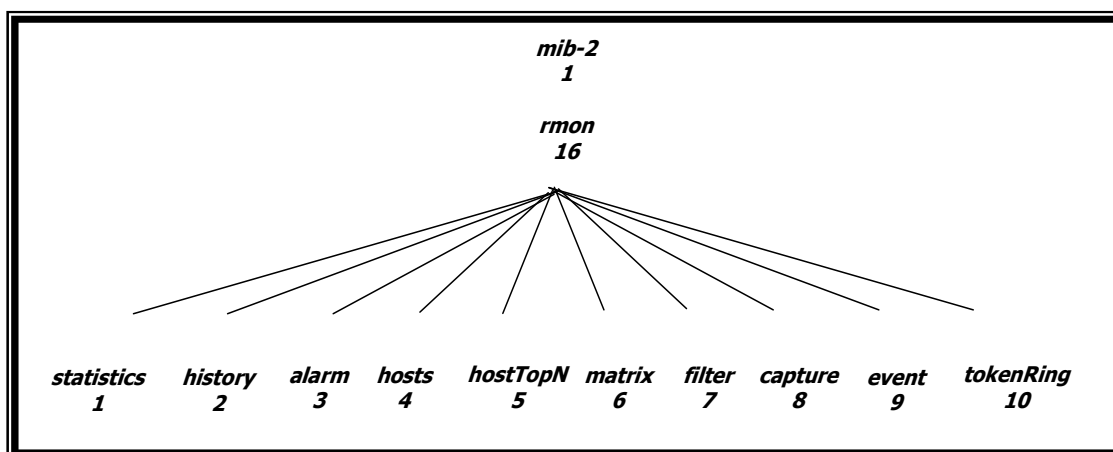


**Gráfico 7 Objetos RMON**

GRUPO STATISTICS (1.3.6.1.2.1.16.1)

GRUPO HISTORY (1.3.6.1.2.1.16.2)

GRUPO ALARM (1.3.6.1.2.1.16.3)

GRUPO HOSTS (1.3.6.1.2.1.16.4)

GRUPO HOSTTOPN (1.3.6.1.2.1.16.5)

GRUPO MATRIX (1.3.6.1.2.1.16.6)

GRUPO FILTER (1.3.6.1.2.1.16.7)

GRUPO PACKET CAPTURE (1.3.6.1.2.1.16.8)

GRUPO EVENT (1.3.6.1.2.1.16.9)

#### **4.11 RMON PARA TOKEN RING (RFC 1513) –GRUPO TOKENRING**

El RFC 1513 extiende la MIB RMON para el protocolo token-ring, mediante el agregado de un nuevo grupo, tokenRing (10), bajo RMON (16), y nuevos subgrupos en los grupos statistics y history, exclusivamente para este protocolo.0

GRUPO TOKENRING (1.3.6.1.2.1.16.10)

Grupo Estadísticas de capa MAC de Token Ring (TOKEN RING MLSATSTABLE  
DEL GRUPO STATISTICS)

Grupo Estadísticas Promiscuas de Token Ring (TOKEN RING PSATSTABLE DEL GRUPO STATISTICS)

Grupo Historia de Capa MAC de Token Ring (TOKEN RING GMLHISTORYTABLE DEL GRUPO HISTORY)

Grupo Historia Promiscua de Token Ring (TOKEN RING PHISTORYTABLE DEL GRUPO HISTORY)

Grupo Ring Satation de Token Ring (del grupo Token Ring)

Grupo RingStationOrder de Token Ring (del Grupo de Token Ring)

Grupo RingStationConfig de Token Ring (Del grupo de Token Ring)

Grupo SourcerOuting de Token Ring (del grupo de Token Ring)

#### **4.12 GRUPOS DE RMON**

RMON entrega la información en nueve grupos, cada grupo es opcional de modo que los vendedores no necesiten apoyar a todos los grupos dentro del Management Information Base (MIB). Los grupos de algún RMON requieren la ayuda de otros grupos de RMON para funcionar correctamente resume a nueve grupos de supervisión especificados en el MIB de Ethernet RMON. Ver Tabla 1

| <b>GRUPO DE RMON</b>       | <b>FUNCION</b>                                                                                                                        |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>Estadística</b>         | Contiene la estadística medida por la punta de prueba para cada interfaz vigilado en este dispositivo.                                |
| <b>Historia</b>            | Registra muestras estadísticas periódicas de una red y las salva para la extracción posterior.                                        |
| <b>Alarmar</b>             | Toma muestras estadísticas de variables en la punta de prueba y las compara periódicamente con los umbrales previamente configurados. |
| <b>Ordenador Principal</b> | Contiene la estadística asociada a cada ordenador principal descubierto en la red.                                                    |
| <b>HostTopN</b>            | Prepara los vectores que describen los ordenadores principal que rematan una lista pedida por una de su estadística.                  |
| <b>Matriz</b>              | Estadística de los almacenes para las conversaciones entre los conjuntos de dos direcciones                                           |
| <b>Filtros</b>             | Permite a los paquetes ser correspondido con por una ecuación del filtro.                                                             |
| <b>Captura del Paquete</b> | Permite a los paquetes ser capturado después de que atraviesen un canal.                                                              |
| <b>Acontecimientos</b>     | Controla la generación y la notificación de acontecimientos de este dispositivo.                                                      |
| <b>Token-ring</b>          | Ayuda del token ring                                                                                                                  |

**Tabla 1. Funciones de los Grupos RMON**

#### **4.13 COMO TRABAJA RMON?**

Una configuración típica de RMON consiste en la dirección de la estación central de la red y un dispositivo que hace un monitoreo remoto, llamado un agente de RMON. La dirección de la estación de la red puede ser el servidor o una PC basada en Windows o

basada en UNIX que ejecuta una aplicación, tal como análisis de efectividad. De esta estación, se puede publicar comandos del SNMP que solicita la información del agente de RMON. El agente de RMON envía la información solicitada a la estación, que procesa y visualiza esta información sobre su consola.

El agente de RMON es un software que reside dentro de la red. Mientras que los paquetes viajan a través de la red, el agente de RMON recoge y analiza datos de Ethernet en tiempo real en un segmento alejado del LAN y salva continuamente los datos localmente en Ethernet DCM según la especificación del MIB de RMON.

Para poder administrar una red de manera correcta también es necesario un buen y potente software. Suele ser una buena elección el software programado por grupos de seguridad conocidos. Ver Gráfico 8 y 9

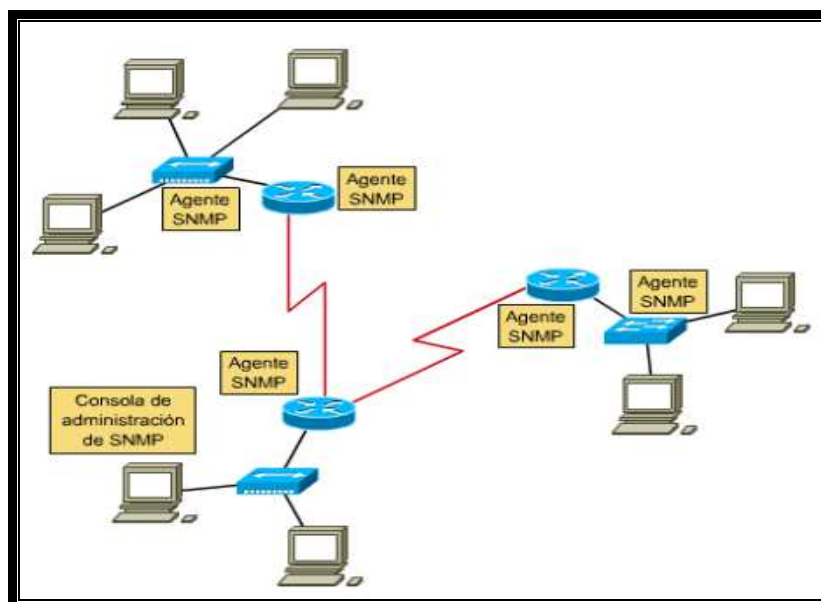


**Gráfico 8. Red de Consolas RMON**

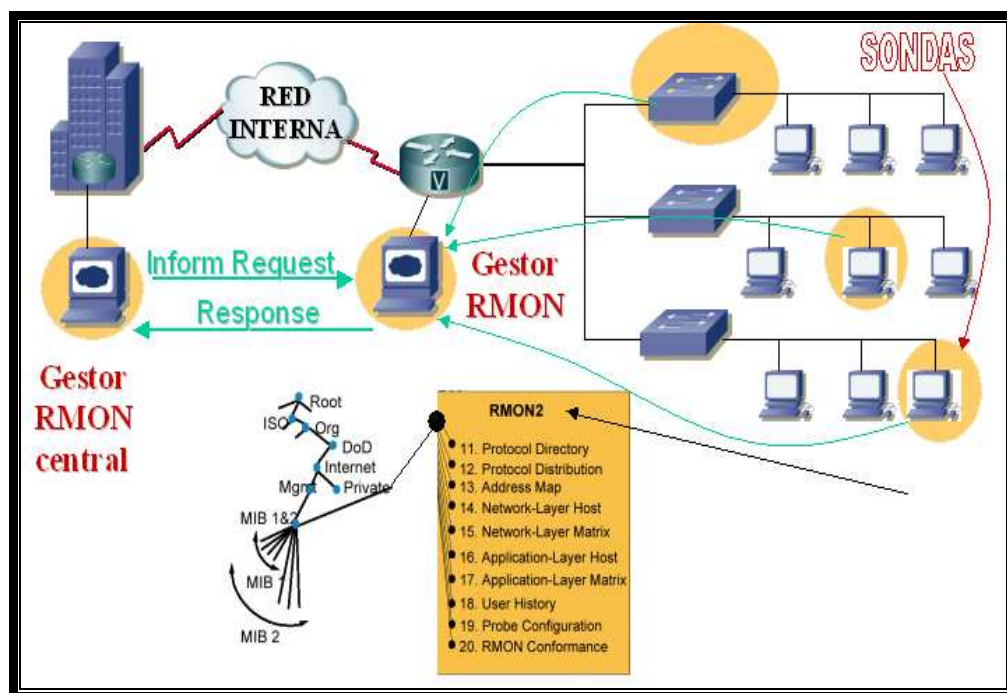


Gráfico 9. Funcionamiento del RMON

## **5 CAPITULO IV: SELECCIÓN Y APRENDIZAJE DE LA MEJOR HERRAMIENTA DE MONITOREO**

### **5.1 PATROL EXPRESS**

#### **5.1.1 Introducción**

La solución ideal es un sistema de administración que pueda ser instalado y configurado rápidamente. Una vez implantado debe realizar el seguimiento de:

- Monitoreo de una variedad de sistemas, aplicaciones almacenamiento y dispositivos de red.
- Permitir a los usuarios añadir monitoreo para nuevos sistemas en pocos minutos.
- Proveer acceso universal a los datos de desempeño para una variedad de usuarios finales, incluyendo administradores de sistemas, ingenieros de redes, gerentes y ejecutivos.

#### **5.1.2 Ventajas principales**

- Infraestructura de monitoreo remoto, tales como sistemas operativos, aplicaciones, almacenamiento y dispositivos de red.
- Monitoreo de transacciones Web bajo la perspectiva de usuario final.
- Medición de los niveles de servicio definidos

- Provee notificación y escalamiento de los problemas en tiempo real.
- Provee un acceso centralizado a todas las partes para obtener reportes a través de un portal Web.

### **5.1.3 Características BMC software**

Patrol Express monitorea el desempeño y disponibilidad de servidores, aplicaciones, almacenamiento y dispositivos de red. El monitoreo se lo hace remotamente (sin agentes), sin software residente en los elementos a ser monitoreados. Patrol Express también monitorea el desempeño y disponibilidad de las transacciones Web.

Monitoreando la infraestructura de las transacciones, permite al IT (Information technology, Tecnología de Información) determinar rápidamente como los problemas de la infraestructura afectan la experiencia del usuario final.

### **5.1.4 Beneficios de Patrol Express**

#### **5.1.4.1 Monitoreo remoto de los elementos de la infraestructura.**

Patrol Express monitorea elementos usando protocolos estándar de la industria tales como PerMon, SNMP, http, rstatd, y Secure Shell (SSH).

Usando estos protocolos permite que los datos sean recolectados remotamente sin tener instalado software en los elementos que están siendo monitoreados.

Toda la recolección de datos es hecha desde el servidor central llamado Remote Service Monitor (RSM, Monitor de Servicio Remoto). El RSM recolecta datos de desempeño y

después los retransmite al Service Integration Portal (SIP), donde el usuario final puede observar los datos de parámetros a través de reportes de niveles de servicio.

#### **5.1.4.2 Umbrales de alertas y políticas de notificación**

Con Patrol Express, los clientes pueden definir físicamente límites para alarmas y advertencias. En algún momento estos límites son excedidos, entonces los clientes reciben en tiempo real alertas vía e-mail, pager o traps de SNMP.

Los clientes pueden especificar diferentes notificaciones y políticas de escalamiento, determinando quien recibe las alertas y que tipo de alertas son enviadas.

#### **5.1.4.3 Medir los objetivos de nivel de servicio definidos por el usuario**

Los clientes podrían medir el desempeño y disponibilidad tanto de transacciones Web y elementos de la infraestructura contar objetivos de niveles de servicio.

Los clientes especifican tanto metas de disponibilidad y tiempo promedio para reparar.

Provee un grupo de gráficos de niveles de servicio que presenta exactamente como estos objetivos están siendo alcanzados.

#### **5.1.4.4 Monitoreo de transacciones Web**

Los clientes configuran las transacciones a monitorear usando un browser.

Este proceso soporta todos los tipos de HTML dinámicos y no hay necesidad de ningún tipo de script.

Adicionalmente todo es hecho en línea y no hay software instalado para guardar la transacción.

#### 5.1.4.5 Acceso Web centralizado a toda la organización.

Todo el reporte y configuración es realizado en línea usando el SIP, el cual es accedido mediante un browser estándar.

Cualquier persona con un Web browser y una conexión de red podría observar los reportes y configurar límites y metas de niveles de servicio.

También, algunos miembros del grupo podrían solo necesitar mirar los reportes, estos pueden acceder a ellos usando solo un login de lectura.

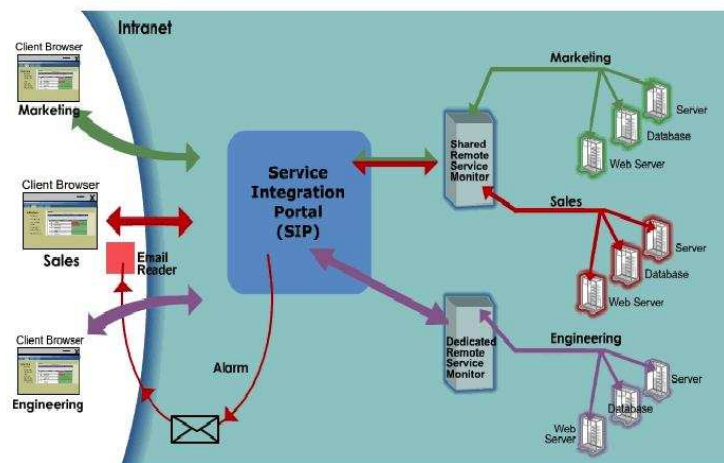


Gráfico 10. Esquema de Patrol Express

## **5.2 SGA - SISTEMA DE GESTIÓN DE ALARMAS**

### **5.2.1 Introducción**

**CESAT** realiza un proyecto de forma conjunta con la empresa **Telefónica Sistemas**, en el que se pretende establecer un marco homogéneo de gestión de alarmas en una red de Telecomunicación.

La idea y definición inicial del proyecto surge como consecuencia de la cooperación entre Telefónica Sistemas y **CESAT** de cara a establecer un marco homogéneo de gestión de alarmas en una red de comunicación. Ha evolucionado hacia la especificación e implementación de una herramienta que permita monitorizar el estado de los componentes de una red mediante las alarmas que éstos emitan. Se busca obtener la información de interés independientemente del protocolo o formato que se utilice para la emisión de las alarmas, de forma que se ofrezca un interfaz homogéneo al operador. Junto con la herramienta principal, se han desarrollado una serie de herramientas complementarias que posibilitan o facilitan la consecución de estos objetivos.

### **5.2.2 Arquitectura**

Como consecuencia de este proyecto se han abierto las siguientes líneas de trabajo:

- Herramientas de gestión de alarmas basadas en plataformas. Solstice Enterprise Manager (SEM). El gráfico<sup>11</sup> muestra la interfaz de la herramienta desarrollada.

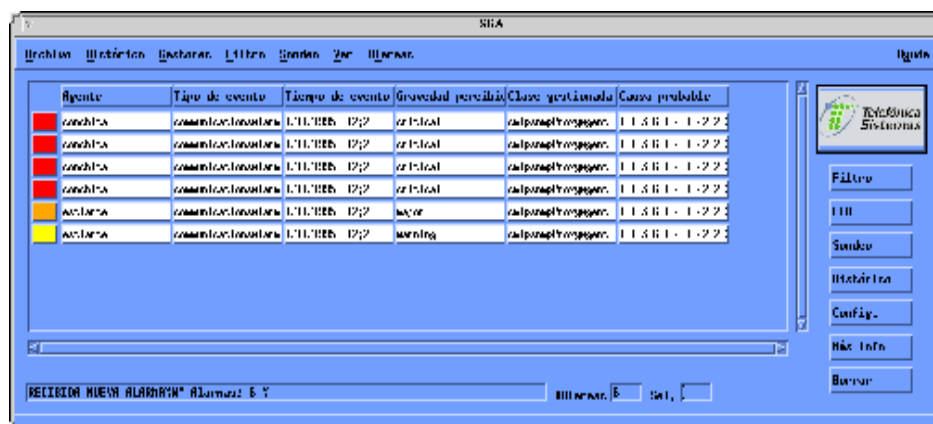


**Gráfico 11. Interfaz de SGA**

- Integración de una base de datos, lo que permitiría manejar toda la información adicional que se necesita para el manejo de alarmas, así como el trabajo en torno a la realización de correlación de eventos.
- Mejora de la interfaz de usuario, optimizando la ya existente e incorporando nuevas características como pueden ser la posibilidad de personalizar el entorno de usuario, tener distintas vistas de la red por categoría de operador, mostrar representaciones gráficas de históricos de alarmas, etc.
- Portabilidad a otras plataformas.
- Ampliación del tratamiento de alarmas, incorporando características adicionales del modelo de gestión OSI que aun no hayan sido contempladas en esta versión.
- Inclusión de capacidades de proceso de informes de históricos que permitan extraer información adicional de los datos recibidos.

- Integración de alarmas SNMP y alarmas CMIP. Dentro de esta línea de investigación se ha desarrollado un traductor de alarmas SNMP a alarmas CMIP sobre la plataforma SEM.

### 5.2.3 Arquitectura del traductor de alarmas

Las arquitecturas distribuidas para gestión de alarmas describen las ideas sobre las que desarrollar una arquitectura distribuida para la gestión de alarmas, y se definen una serie de servicios y elementos funcionales para llevarla a cabo. Hasta ahora el único desarrollo puesto en práctica ha consistido en utilizar el paquete SNMP de CMU para implementar un redirector y un simulador de traps SNMP.

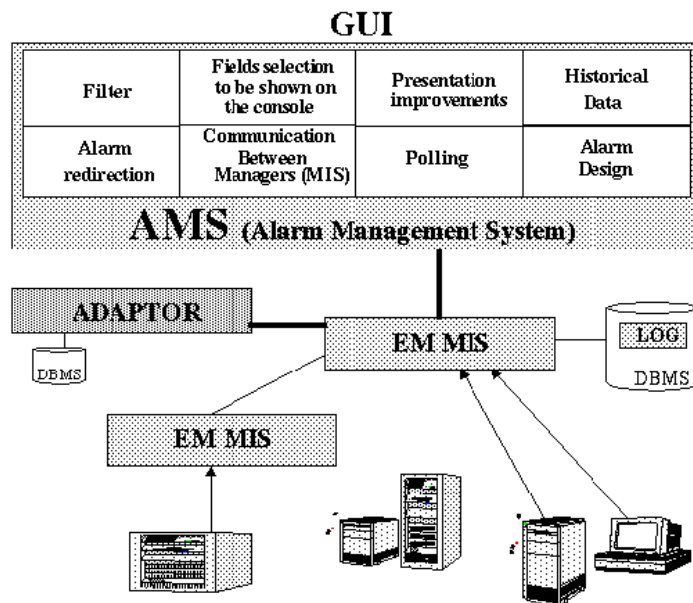


**Gráfico 12. Arquitectura SGA**

### **5.3 ENTERASYS NETWORKS- NETSIGHT MANAGER**

#### **5.3.1 Introducción**

En un continuo esfuerzo por alinear más estrechamente las redes con el proceso diario de los negocios, Enterasys Networks una compañía de Cabletron Systems, lanza NetSight, una amplia solución de administración de redes diseñada para simplificar la administración de las complejas redes empresariales.

Más que un producto de administración de red, NetSight proporciona características avanzadas incluyendo la configuración automática de dispositivos, configuración de VLANs fácil de usar, las últimas aplicaciones de redes y características de seguridad y conectividad basadas en decisiones para convertir la red en una poderosa herramienta de negocios.

La interfase gráfica basada en el Web de NetSight, proporciona flexibilidad en cualquier momento. Lo anterior, crea un centro de comando para simplificar la administración diaria de las redes empresariales y monitorear la seguridad en toda la infraestructura de red.

NetSight está basado en el estándar 802.1Q y trabaja con productos compatibles con ésta norma, e incluye:

Monitoreo del tráfico en la red, descubrimiento de la red, administración de RMON y SNMP, alarmas y administración de eventos, resolución de problemas (troubleshooting) y configuración de dispositivos por niveles en la red.

El NetSight va más allá de la administración tradicional de la red al proveer una herramienta única que protege a la compañía de las amenazas de seguridad internas y externas. Hoy en día la seguridad, QoS y la facilidad de uso son las mayores preocupaciones del personal de IT, hoy es una solución multi-dimensional para reducir la complejidad haciendo la administración de redes más fácil para la empresa.

### **5.3.2 Características**

- Posee una ventana primaria donde se puede navegar entre el Map View, List View, Tree View, and Log Viewl del área de trabajo, para activar ventanas que supervisen y manen la red (tal como ventanas del mapa y ventanas de registro de alarmar). Una barra de menú central proporciona el acceso a la mayoría de las opciones de la gerencia.
- Una interfaz gráfica que deja clasificar, cambiar, y volver a clasificar los nodos según el tamaño exhibiciones de la columna, seleccionar los iconos para los nodos en Map View, List View, and Tree View y modificar la barra de herramientas para requisitos particulares.
- Ayuda en línea completamente equipada, incluyendo wizards para las tareas comunes, ayuda sensible al contexto con un glosario y un índice.
- Los nodos se crean automáticamente en la base de datos central; así como también esta se almacena.

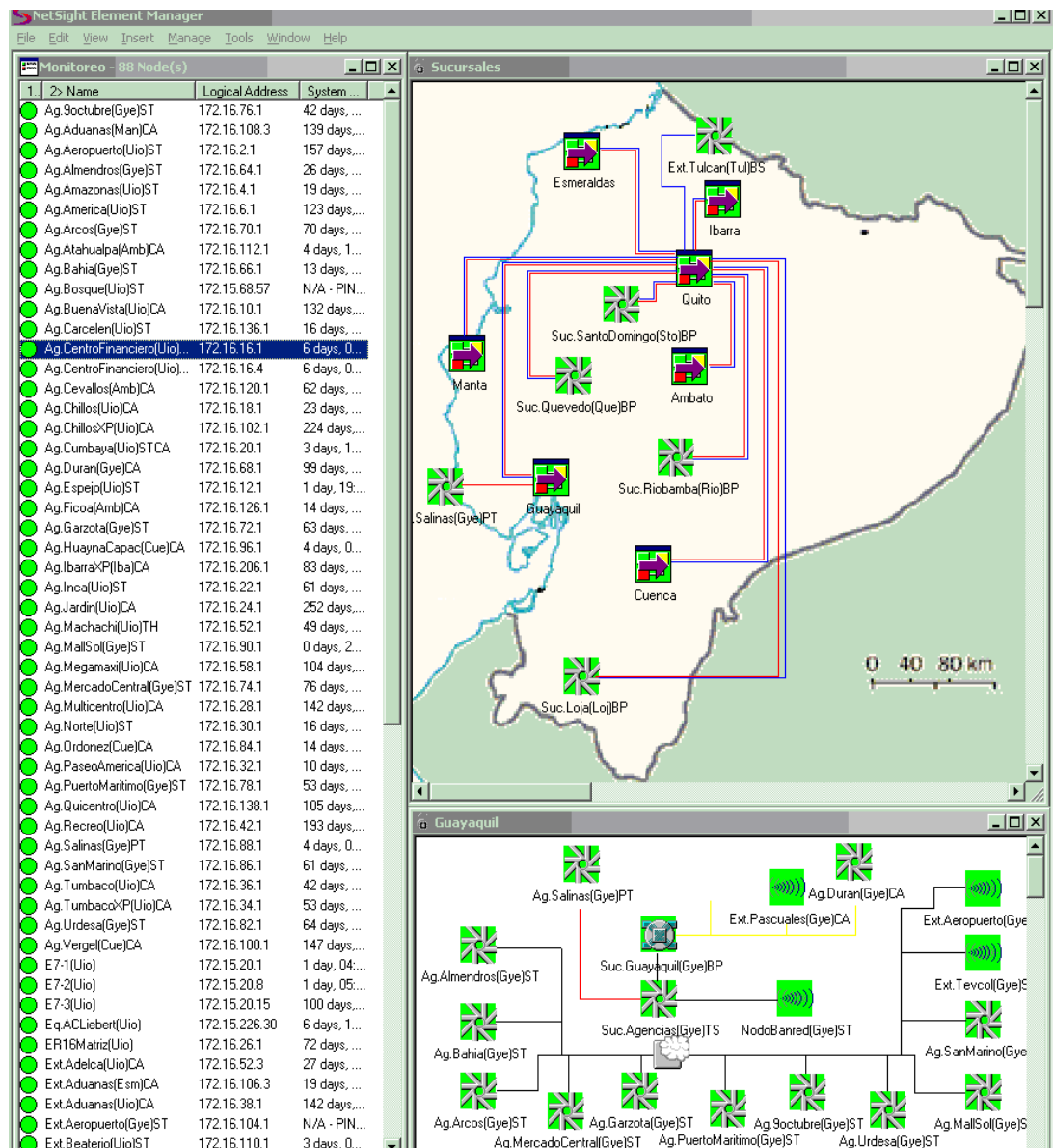


Gráfico 13. Consola de Monitoreo NetSight Manager

### 5.3.3 Arquitectura

- La aplicación **Network Status** (Estado de la Red) es responsable del poleo en los nodos de la base de datos central. Provee un estatus de los dispositivos de la red a través de vistas, árbol de vistas y mapas.
- La aplicación **Event Manager** (Gestión de Eventos) es la responsable de alarmas y eventos administrativos. Este recibe traps desde los nodos de la red y eventos desde otro proceso de NetSight.
- La herramienta **Scheduler** (Planificador) permite almacenar y tener respaldos de los datos, así como también hacer un descubrimiento de la red automáticamente a una hora y día establecido.
- La herramienta de **Administración Remota** permite fácilmente realizar tareas de la gerencia (tales como transferencias directas de TFTP, configuración de la tabla de la trampa, o interrogación de la estadística del MIB de la creación o transferencias directas del MIB) en un dispositivo individual o grupos de dispositivos. Una herramienta del localizador del MAC address también permite que buscar unos o más dispositivos para el puerto a través de el cual un MAC address seleccionado se está comunicando.

## 5.4 OBSERVER.

### 5.4.1 Concepto

La empresa Network Instruments es líder en la manufactura de herramientas para el análisis, monitoreo y resolución de problemas de redes, ofrece Observer, un analizador de protocolos, rico en características especiales, flexibles y fáciles de usar.

Observer y sus examinadores (probes) analiza y monitorea: Ethernet, Wireless 802.11, Gigabit Ethernet, WAN, FDDI y Token Ring

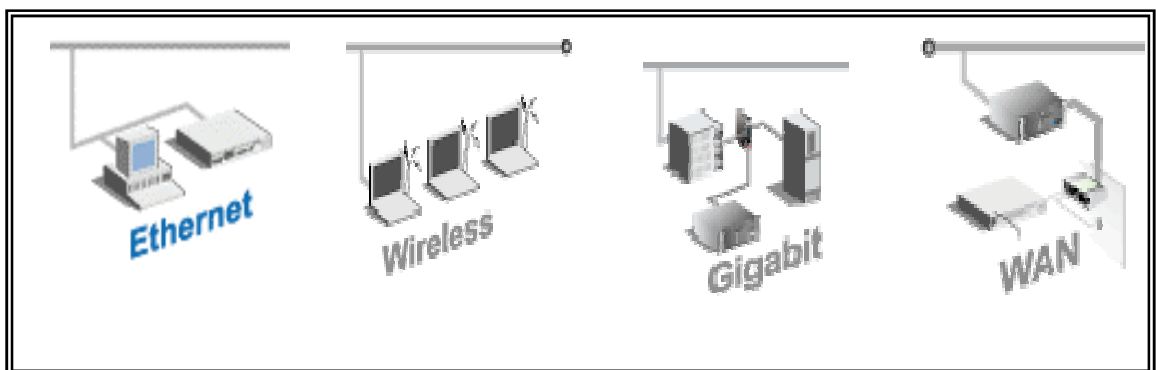


**Gráfico 14. Tipos de Redes**

### 5.4.2 Introducción

Las redes de cómputo de las organizaciones, se vuelven cada vez más complejas y la exigencia de la operación es cada vez más demandante. Las redes, cada vez soportan más aplicaciones y servicios estratégicos de las organizaciones. Por lo cual el análisis y monitoreo de redes se ha convertido en una labor cada vez mas importante y de carácter pro-activo para evitar problemas.

Anteriormente, cuando no existían las herramientas que hoy existen, era necesario contratar a una empresa especializada para esta labor, con un costo muy elevado. Hoy en DIA las herramientas permiten realizar esta importante labor dentro de nuestra misma empresa y contar con un sistema experto como aliado, que ayuda en la interpretación de los resultados obtenidos, que se queda con nosotros todo el tiempo y pasa a ser parte de su activo.

### **5.4.3 Versiones**

#### **5.4.3.1 Observer**

Analizador completo de protocolos, que ayuda a resolver problemas de la red y a estudiar sus tendencias a largo plazo, ya sea que la red sea por cable o inalámbrica. Observer incluye un capturador de paquetes y decodificador de mas de 500 protocolos, estadísticas de tiempo real, estadísticas basadas en una línea de inicio que permiten estudiar las tendencias de tráfico. Es posible adicionar examinadores (probes) para monitorear redes distribuidas por cable o inalámbricas.

#### **5.4.3.2 Expert Observer**

Todas las características de Observer más Análisis Expertos de Tiempo Real. Notificación de Eventos y Modelaje.

#### **5.4.3.3 Observer Suite**

Todas las características de Expert Observer mas una consola de administración SNMP. Consola RMON y Reportes a través del Web.

#### **5.4.3.4 Examinadores (Probes)**

Los examinadores (probes) basados en software permiten un análisis y monitoreo remoto para redes: 10/100 Ethernet, 802.11 a/b/g Wireless, Token Ring y FDDI. Los examinadores (probes) reportan a una consola Observer la información de la actividad de una red sin la necesidad de desplazarse a otras ubicaciones gastando dinero y tiempo.

#### **5.4.4 Introducción Observer**

Observer permite introducirse al nivel de paquetes individuales hasta obtener vistas generales de la actividad de la red. Ofreciendo gran diversidad de niveles de revisión. Descubre e identifica los nodos de la red, monitorea los nodos descubriendo su disponibilidad y rendimiento, decodifica protocolos, produce estadísticas útiles de las actividades que se realizan en la red, ayuda a resolver problemas y reporta el status actual de los dispositivos de la red y sus conexiones

Observer va de lo general a lo particular en varios aspectos de la red, permitiéndole, filtrar el tráfico basado en direcciones de la red, tipos de protocolo y otros criterios de selección.

Observer acelera el diagnóstico de un problema en la red, revelando la naturaleza del

problema, ubicación e impacto. Relacionado la actividad actual con una línea de base de actividad normal previamente capturada, se convierte en parte de la caja de herramientas de planeación informándole de sus tendencias y cambios.

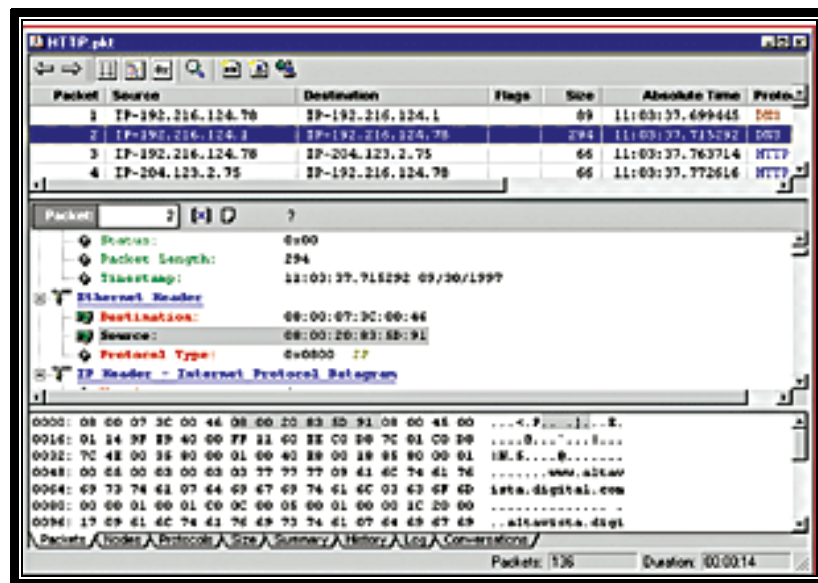


**Gráfico 15. Pantalla Principal Observer**

- Gran capacidad de interpretación y decodificación de protocolos (>500)
- Útiles comentarios del sistema experto
- Gran versatilidad y facilidad de manejo de ventanas para determinar problemas
- La excelente utilidad, facilidad y claridad de sus reportes

#### 5.4.5 Examinadores (Probes) / Advanced Y Rmon

Los examinadores Advanced y RMON recolectan la información de un punto remoto para enviársela a la consola de Observer, con éstas, es posible monitorear LANs, WLANs o WANs desde un punto central.

Los examinadores pueden operar en dos modos: Advanced o RMON, cualquier examinador puede ser configurada para trabajar de un modo o de otro indistintamente. El examinador Advanced es un super conjunto de las examinadores RMON.

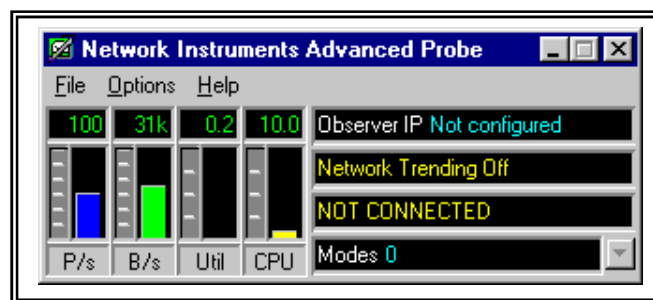


**Gráfico 16. Instrumentos de Red Avanzados**

Redes con switches y compartidas

Los examinadores Advanced ofrecen:

- Mejores costos
- Completa colección de datos Observer para sitios remotos, locales, segmentos remotos o switches Reportes Web con fotografías del status de la red

- Completa protección de la información con contraseñas

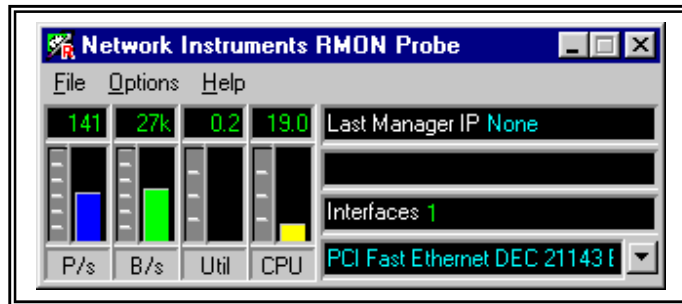


**Gráfico 17. Instrumentos de Red ROMON**

Estándar RMON1 y RMON2

Los examinadores RMON ofrecen:

- Mejores costos
- Completa colección de datos RMON para sitios remotos
- Monitoreo de múltiples interfaces concurrentes
- Múltiples accesos a consolas de administración

#### **5.4.6 Requerimientos**

##### **5.4.6.1 Sistemas operativos**

- Windows® 95/98
- Windows® NT 4.0

#### **5.4.6.2 Protocolo de red**

- SNMP
- TCP/IP

#### **5.4.6.3 Requisitos del hardware**

- PC compatible IBM
- Intel Pentium de 200MHz o superior
- 5 MB de espacio en disco duro 32 / 64 MB de RAM

### **5.5 HP OPENVIEW**

#### **5.5.1 Concepto**

Es una herramienta de administración de gran escala que ofrecen una administración completa de redes, sistemas, aplicaciones y servicios. Ayudan a los administradores de redes a evaluar de forma estratégica el rendimiento general de la red. Aunque es eficiente a la hora de detectar problemas carece de la información detallada necesaria para aislar el origen del problema.

OpenView está organizado en mapas o ventanas con determinados símbolos. Por defecto, la primera vez que arranca, NNM (Network Node Management , Gestión de

Red a Nivel de Nodo) descubre todos los elementos con dirección IP a los que tiene acceso desde la máquina donde gestiona.

Una vez descubiertos, los inserta en el mapa Internet, donde se conectan según la información que obtiene a partir de los nodos de direcciones IP, tablas de routing, etc.

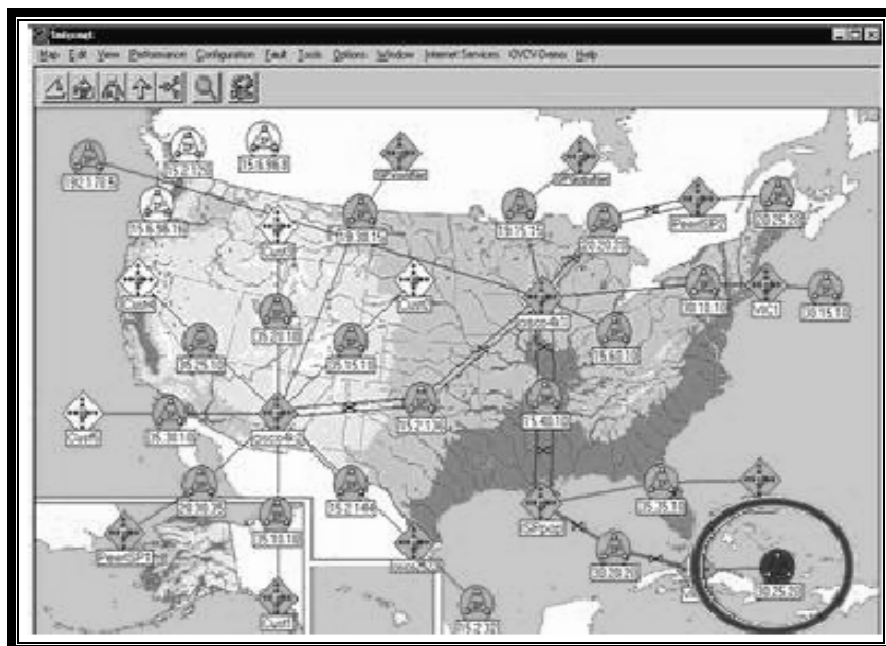


**Gráfico 18. Pantalla Principal de HP Open View**

### 5.5.2 Características

- Cuando se instala HP – Open View lo primero que se hace es, un auto descubrimiento de la red a la cual se esta conectado con tal de detectar los hosts, routers, y otros dispositivos de nivel 3 OSI con los cuales se tiene conectividad directa.

- Pero obviamente es posible añadir todos los nodos que se quiera, aunque no estén conectados directamente al servidor, aunque pertenezca a otra red distinta a la nuestra.
- En HP – Open View además de los mapas y submapas se dispone de los visores de alarmas, en los cuales se puede ir agrupando las alarmas que interesan en distintas categorías, para ello se tiene el menú de Alarm Categories, en el cual aparecen unos botones que al pinchar sobre ellos provocará la acción de abrir el browser de la categoría de alarmas que se quiera.

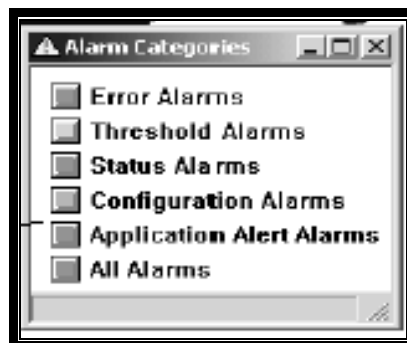


**Gráfico 19. Categorías de Alarmas**

- En el Gráfico 20 se puede ver el All Alarms Browser (Buscador de Todas las Alarmas), esta pantalla mostraría las alarmas correspondientes a la categoría All Alarms (Todas las Alarmas) de la pantalla de Alarm Categories (Categoría de Alarmas).

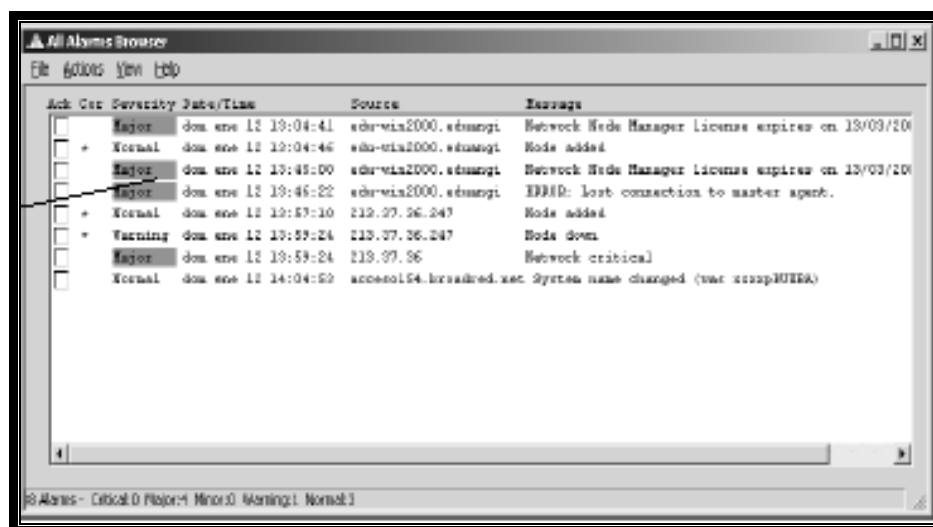


**Gráfico 20. Buscador de Alarmas.**

- Una vez que se hace clic en Internet entonces se puede ver la o las redes conectadas directamente al servidor y se puede ver una a una pinchando en cada una de las subredes.

Haciendo clic sobre cada subred se abrirá otro submapa con la red correspondiente.



**Gráfico 21. Vista de todas las Subredes conectadas al servidor**

- En cada red se tiene las capas de cada uno de los segmentos o dominios de colisión, en el caso de este ejemplo solamente aparece un segmento, pincharemos sobre el para entrar en el siguiente submapa.

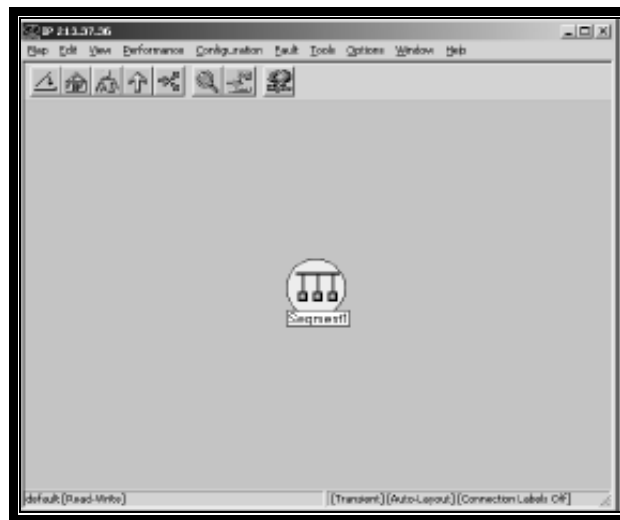


**Gráfico 22. Pantalla del segmento de Red**

- Una vez que se ingresa en el segmento correspondiente se puede ver los equipos del segmento en cuestión, una vez llegados a este submapa ya se puede ver los equipos de la red que se van a monitorear.
- Se debe observar que en un submapa de Open View se tiene equipos de distintas clases e incluso se podría monitorizar servicios y mostrarlos en un mapa especial de servicios, estos servicios podrían ser httpd, ftpd, etc.

- Cuando se ingresa en este submapa se puede empezar a utilizar la potencia de HP – Open View y realizar tareas como:
  - a) Monitorizar cada uno de los interfaces
  - b) Abrir Telnet
  - c) Mostrar alarmas específicas de un nodo
  - d) Ver propiedades de cada interfaz
  - e) Conectarse mediante http, ssh, etc.

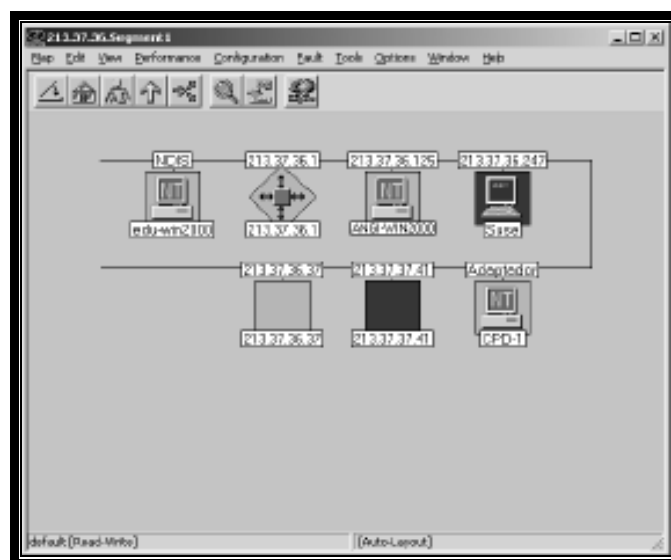


**Gráfico 23. Pantalla de Sub-mapas**

- En cada una de las interfaces de cada una de las máquinas monitorizadas con HP – Open View pueden ser observados directamente, tal y como se puede observar en el Gráfico 24.
- En el Gráfico 24 representa un equipo con tres interfaces Ethernet: eth0, eth1 y eth2.

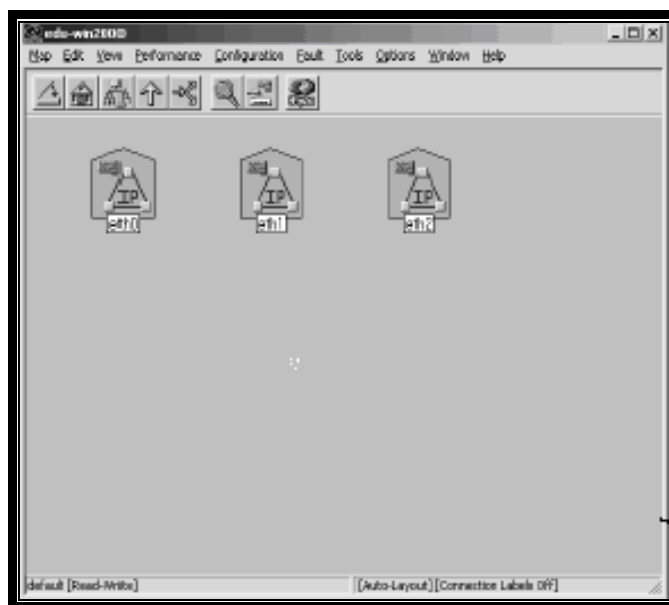


**Gráfico 24 Pantalla de Interfaces**

### **5.5.3 Personalización**

Para que sea mucho más eficiente la red en su administración, se necesita saber a simple vista donde están ubicados los equipos, qué equipos son, para lo cual se debe tener una posición concreta y con un dibujo de fondo que puede ser un mapa en donde se ubicarán las posiciones de cada equipo de la red.

Unas de las cualidades principales de HP – Open View es que es capaz de monitorizar cualquier equipo que responda a peticiones SNMP o incluso de forma muy limitada a equipos que respondan a peticiones ICMP, en este caso sólo se puede saber si el equipo está conectado o no (en muchos casos más que suficiente), pero no es suficiente en determinados casos en los que necesitamos una información más detallada y precisa de un equipo o nodo, como podría ser por ejemplo un router de acceso que es crítico para nuestra compañía, en este caso necesitamos saber casi todo lo que le pueda pasar al router o a un servidor crítico.

HP – Open View como software de gestión que es, recibe una serie de traps que se deben organizar según severidad y categorizar en distintas clases, o incluso se puede querer que una alarma determinada muestre un pop-up o incluso traducir los traps al Español.

En Open View se puede añadir como nodo cualquier cosa, desde un PC Windows hasta un gran router de un gran operador de Internet, pasando por supuesto por servidores UNIX, Mac, etc., routers Cisco, Lucent, etc, las posibilidades del gestor son enormes y el interés principal es explotarlas al máximo debido a su elevado precio y sobre todo posibilidades.

#### **5.5.4 Configuración**

Para añadir un nuevo elemento que esté en una nueva red se tiene que crear la red y posteriormente añadir el elemento, para ello se realiza el siguiente procedimiento:

a) Se añade la red en el submapa deseado, para ello en el menú de Open View:

- Edit (Editar)
- Add Object (Adicional Objeto)
- Seleccionar en Symbol Classes (Clases de Símbolo) el grupo de elementos, en este caso Network
- En la ventana inferior seleccionar el tipo de red a insertar, por ejemplo IP Network.
- Arrastrar la red al mapa correspondiente
- Al arrastrar la red al mapa se abriría la siguiente pantalla en la que indica la dirección de la red con su máscara y en Label se escribe el nombre de la red.

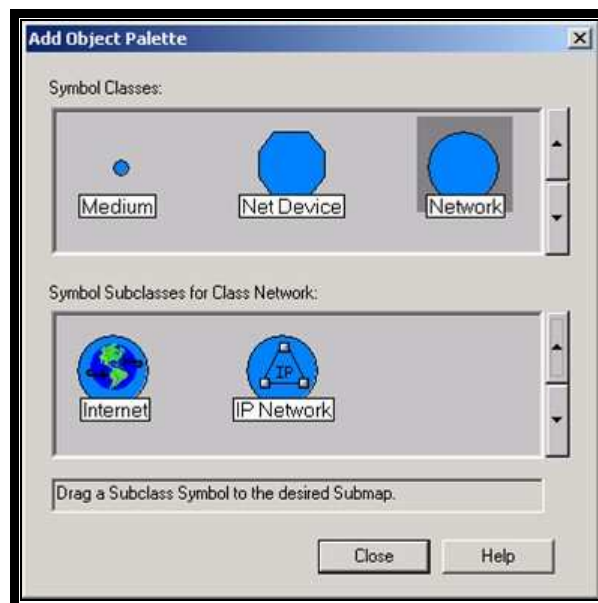


**Gráfico 25 Pantalla para Crear Objetos de la Red**

- b) Dentro de la red creada, se crearía el nuevo nodo en los mismos menús, pero con la diferencia de que en el menú de Add Object (Adiciona Objetos) seleccionaría el elemento en cuestión, que puede ser o no otra red.

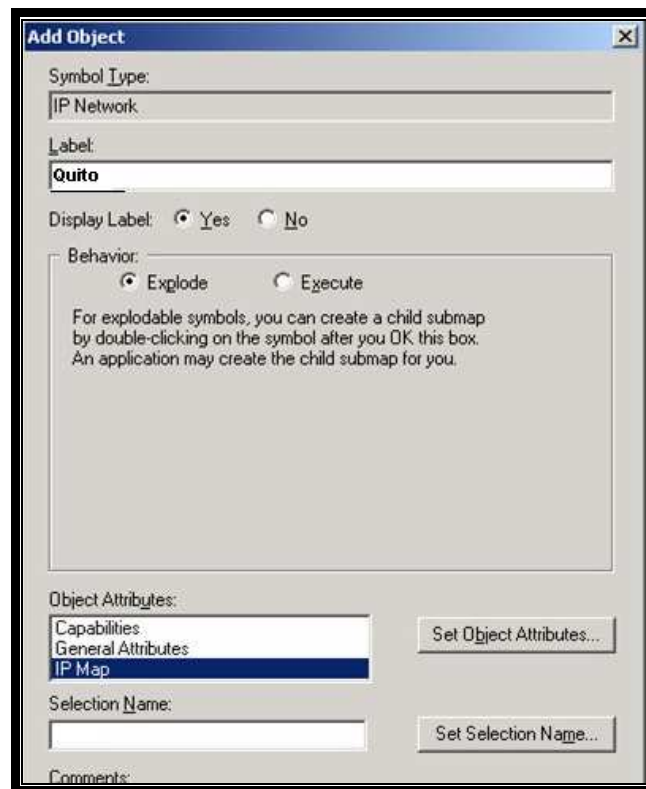


**Gráfico 26 Pantalla para Adicional Objetos**

### 5.5.5 Conclusiones

Esta herramienta de monitoreo es muy importante a la hora de detectar problemas en la red, pero su carencia de aislar el origen del problema que los generó no la hace la

herramienta mas recomendada para el estudio propuesto; sin embargo es muy práctica para estudiar cada nodo registrado independientemente.

## **5.6 SOLARWINDS**

### **5.6.1 Introducción**

Las herramientas de SolarWinds han sido diseñadas por ingenieros de red con un énfasis especial en la facilidad de uso la velocidad de proceso y la precisión de los resultados ofrecidos. Esto puede experimentarse ejecutando el IP Network Browser (buscador de Red IP). Esta herramienta utiliza SNMP para realizar análisis de la red a una velocidad increíble.

Solarwinds es un Software para monitoreo de redes, dispositivos y servidores además verifica la disponibilidad de ancho de banda.

### **5.6.2 Características**

- Verifica la disponibilidad del ancho de banda
- Monitorea el funcionamiento y análisis de la red, descubrimiento y solución de fallas.
- Supervisión remota de funcionamiento del router, switch, servidores desde un tablero del PC.

- Monitorea y ve gráficamente en tiempo real el número de paquetes perdidos, trafico, utilización del ancho de banda y manejo de errores.
- Supervisa cada nodo manejado mediante SNMP
- Provee de gráficos históricos y mapas de la utilización de la red.
- Crea una Base de Datos del inventario detallado de la red.
- Descubre los puerto Ethernet manejados y detalla los dispositivos conectados en la red, por medio de su dirección MAC, IP y Host Name.
- Toda la información de la base de datos puede ser exportada a .pdf.
- Determina que direcciones IP están en uso y cuales no.
- Monitorea la carga del Router, además trasmite un archivo con la configuración del mismo.
- Puede ejecutar un PING desde cualquier Router Cisco a cualquier otro dispositivo SNMP.
- Permite visualizar, actualizar y realizar cambios a cualquier sistema SNMP.

.

## 5.7 PATROL DASHBOARD

Puede ser instalado en ambientes Unix, Linux y Microsoft y utiliza servicios SNMP para la gestión de dispositivos de red.

Dentro de las características de Patrol Dashboard podemos destacar que es capaz de:

- Conocer:
  - Donde están los cuellos de botella en la red (bottlenecks).
  - Que elementos se utilizan más / menos de lo debido.
  - Saber si están cumpliendo sus niveles de servicio (SLA).
- Predecir
  - Posibles Congestionaciones (Planificación de Capacidad)
  - Saturación de enlaces LAN ó WAN.
- Optimizar:
  - La función en general de la red
  - Costos de comunicaciones
- Justificar:
  - La inversión de nuevos elementos de hardware (o upgrades)

- El funcionamiento de la red

Patrol Dashboard puede cumplir esto debido a que aplica inteligencia en la correlación de eventos de red, los que en combinación a las alertas, estadísticas, reportes y tendencias que el mismo software genera y recolecta permiten determinar con exactitud las causas de problemas ó predecirlos.

Patrol Dashboard es una herramienta tan completa que incluso puede ser útil para empresas proveedoras de servicios de comunicaciones e internet, las cuales pueden usar Patrol Dashboard para que los mismos clientes finales puedan medir que servicio están obteniendo de su proveedor, gracias a su amistosa interfaz basada en browser.

Un ejemplo muy interesante es lo que una enorme compañía francesa de comunicaciones hace al entregarle a sus clientes la interfaz web de Dashboard con permisos de usuario que permiten ver los servicios contratados a esta empresa. De esta manera el cliente final puede ver estadísticas de uptime, rendimientos e incluso puede hacer predicciones de capacidad de enlaces o dispositivos. Todo esto acompañado de agradables gráficos.

Patrol Dashboard es una solución integrable y no excluyente de ambientes HP OpenView, Cisco y Computer Associates.

## **6 CAPITULO VI: HERRAMIENTAS DE MONITOREO.**

### **6.1 SOLARWINDS**

#### **6.1.1 Introducción**

Es un Software para monitoreo de redes, dispositivos y servidores además verifica la disponibilidad de ancho de banda.

Las herramientas de Administración de Redes de SolarWinds están distribuidas en nueve categorías, que van desde el ancho de banda y funcionamiento de la red al descubrimiento y solución de fallos.

Son más de 40 herramientas para mantener el control de la red desde un PC, que han sido diseñadas por ingenieros de red con un énfasis especial en la facilidad de uso, la velocidad de proceso y la precisión de los resultados ofrecidos.

Esto puede experimentarse ejecutando el IP Network Browser. Esta herramienta utiliza SNMP para realizar análisis de la red a una velocidad increíble.

La información SNMP e ICMP que facilita incluye: MIB information, Interfaces MAC Address, Port Speed, IP Address, Port Status, Routes, ARP Tables, Accounts, Memory, sysObjectID's y muchas más.

### **6.1.2 Descripción**

Esta edición de SolarWinds Engineer's es una suite de las herramientas del software de la gerencia de una red que contiene entre otras las siguientes herramientas: Network Discovery (Descubrimientos en la Red), Fault Monitoring (Gestión de Fallos), Performance Monitoring and Performance Management Tools (Gestión del Funcionamiento y las Herramientas de Funcionamiento).

Además de todas las herramientas se encontró en el Profesional PLUS Edition, la edición de Engineer's que contiene el New Switch Port mapper (Mapeo de Puerto del Switch Nuevo), el cual realiza automáticamente descubrimiento de la capa 2 y capa 3 en su interruptor.

La edición de Engineer's contiene el browser del MIB de SolarWinds y el Network Performance Monitor (monitor del funcionamiento de la red) así como varias herramientas adicionales de la dirección de la red.

El MIB Browser con su base de datos sobre de 220.000 OID's (Identificadores de Objetos) únicos compilados sobre de mil estándares también se incluye en las herramientas.

Las encuestas, los gráficos, y las alarmas del monitor del funcionamiento de la red en umbrales de ancho de banda, de la avería y del funcionamiento son muy importantes para el mismo.

### 6.1.3 Requerimientos del Sistema

Los requerimientos del SolarWinds se muestran en la Tabla2

| <b>Requerimientos</b><br><b>Versiones</b> | <b>Standard</b>                                                                                                            | <b>Professional</b> | <b>Professional Plus</b> | <b>Engineer's Edition</b> |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|---------------------|--------------------------|---------------------------|
| <b>Sistema Operativo</b>                  | Windows 95 * / 98 / NT / 2000 / yo / XP<br><br>* no muy recomendable; pues algunas herramientas no funcionan correctamente |                     |                          |                           |
| <b>CPU</b>                                | Pentium II 500 MHz o más alto se recomienda                                                                                |                     |                          |                           |
| <b>Memoria</b>                            | 64 MB RAM (128 MB o más alto recomendado)                                                                                  |                     |                          |                           |
| <b>Espacio del Disco</b>                  | Por lo menos 4 MB                                                                                                          | por lo menos 80 MB  | por lo menos 80 MB       | por lo menos 100 MB       |
| <b>Conexión de Red</b>                    | Tarjeta de Red o Modem                                                                                                     |                     |                          |                           |
| <b>Internet Explorer</b>                  | Algunas Herramientas de SolarWinds usan al Explorador de Internet 5.0 objetos.                                             |                     |                          |                           |
| <b>Tarjeta de Sonido</b>                  | Recomendada pero no requerida                                                                                              |                     |                          |                           |

**Tabla 2. Requerimientos del Sistema**

### 6.1.4 Versiones y Costos

Son cinco las versiones del SolarWinds, la que se estudiará es la Versión Enginner's Edition, en la Tabla 3 se muestra una comparación de las versiones vs. sus costos.

| <b>VERSIONES</b>                    | <b>Estándar<br/>Edition</b> | <b>Profesional<br/>Edition</b> | <b>Prof +<br/>Edition</b> | <b>Engineer's<br/>Edition</b> | <b>Broadband<br/>Edition</b> |
|-------------------------------------|-----------------------------|--------------------------------|---------------------------|-------------------------------|------------------------------|
| <b>COSTOS</b>                       | <b>217,50 USD</b>           | <b>667,49 USD</b>              | <b>1.030,75<br/>USD</b>   | <b>1.492,50 USD</b>           | <b>2.580,69<br/>USD</b>      |
| <b>MANTENI<br/>MIENTO<br/>ANUAL</b> |                             | <b>292,50 USD</b>              | <b>442,50 USD</b>         | <b>592,50 USD</b>             |                              |

**Tabla 3. Versiones SolarWinds vs. Costos**

### **6.1.5 Características**

El SolarWinds Engineer's incluye las siguientes herramientas:

#### **6.1.5.1 Network Performance Monitoring Tools (Herramientas para Supervisar el Funcionamiento de la Red)**

Con el SolarWinds Network Performance Monitoring se puede realizar tareas como la supervisión Remota del funcionamiento de Routers, Switch y servidores desde un tablero en el PC. Incluso incluye alertas enviadas como mensaje encriptado a su teléfono celular cuando se acciona un umbral de la interrupción o del funcionamiento.

Con el SNMP Graph (Gráfico SNMP) se puede supervisar cualquier dispositivo manejado por SNMP. Con la utilidad del Network Performance Monitor (Monitor del Funcionamiento de la Red), se puede exhibir una vista gráfica del tráfico en la red. El Advanced CPU Load (Carga del CPU Avanzada) permite supervisar la carga en tiempo real en los routers mientras que el CPU Gauge (Medidas del CPU) exhibe un solo funcionamiento del switch y del servidor o CPU.

En resumen, permite monitorear y ver gráficamente en tiempo real el ancho de banda y la actividad de la red, con la capacidad de generar alertas y enviar mensajes hacia un celular móvil, puede seguir el estado de su red, el número de paquetes perdidos, el tráfico, la utilización de su ancho de banda así como otras estadísticas sobre la red, de igual forma realiza el manejo de errores.

Algunas de las herramientas más populares y características es la Herramienta de supervisión y Funcionamiento de ancho de banda, mientras que muchas aplicaciones requieren de los agentes de hardware o de colectores de datos, el SolarWinds utiliza el protocolo estándar de la red.

#### **6.1.5.1.1 Network Performance Monitor (Monitor del Funcionamiento de la red)**

Esta aplicación es el Monitoreo de la red en tiempo real que puede seguir el estado de la red, la pérdida de paquetes, tráfico, utilización del ancho de banda. Además supervisa cada nodo manejado mediante el SNMP y reporta cuando un nodo reinicia o una interfase esta abajo.

Es ideal para monitorear la utilización del ancho de banda de los routers, switches y servidores, provee de gráficos históricos en línea y mapas históricos de la utilización de la red.

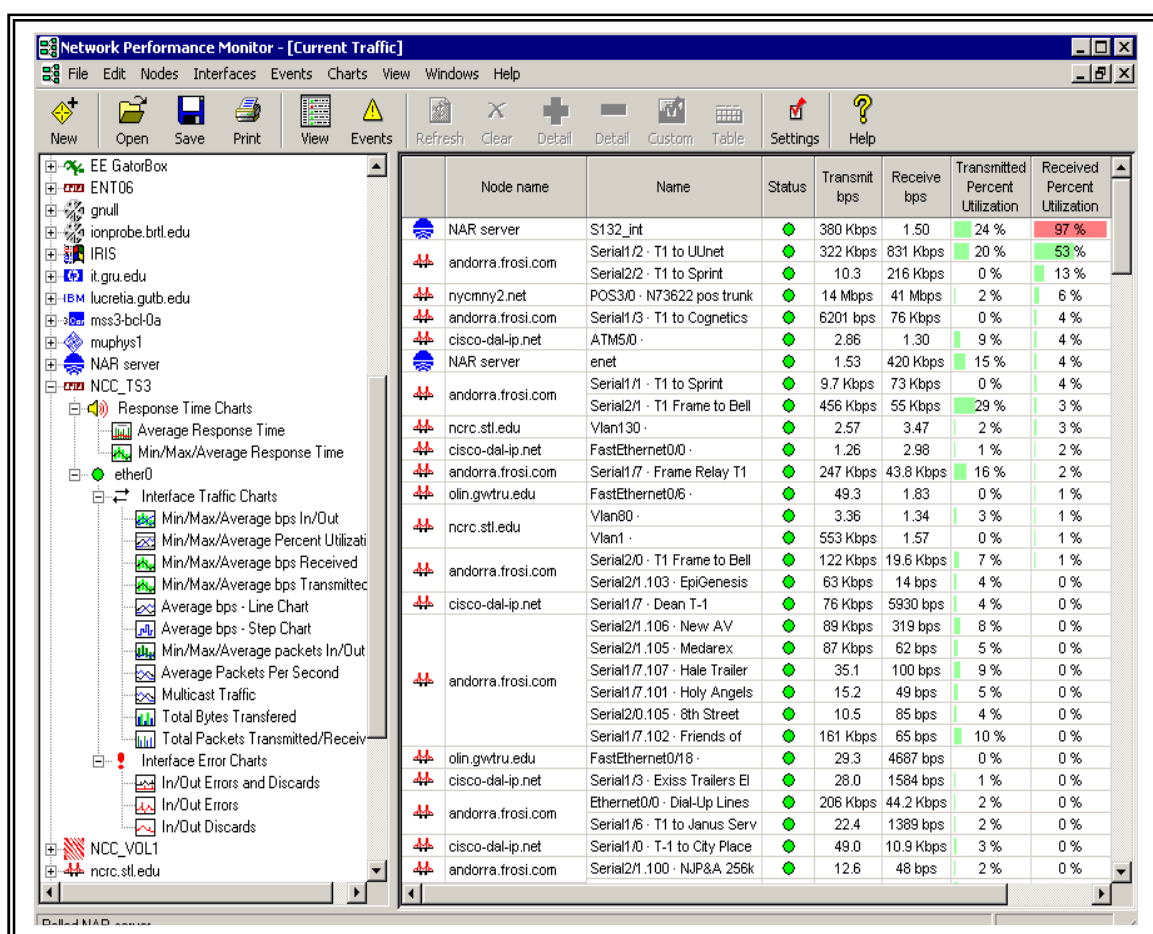


**Gráfico 27. Pantalla del Monitor de Funcionamiento de la Red**

Se puede monitorear el estado de todas las interfaces y recolectar las estadísticas de cada dispositivo.

Si se quiere monitorear el tiempo de respuesta y los paquetes perdidos se necesita tener instalado el SNMP Community String (Cadena Comunidad) y seleccionamos Add Node o Interface Monitor (Adicionar Nodo o Monitor Interfase) del cuadro de dialogo.

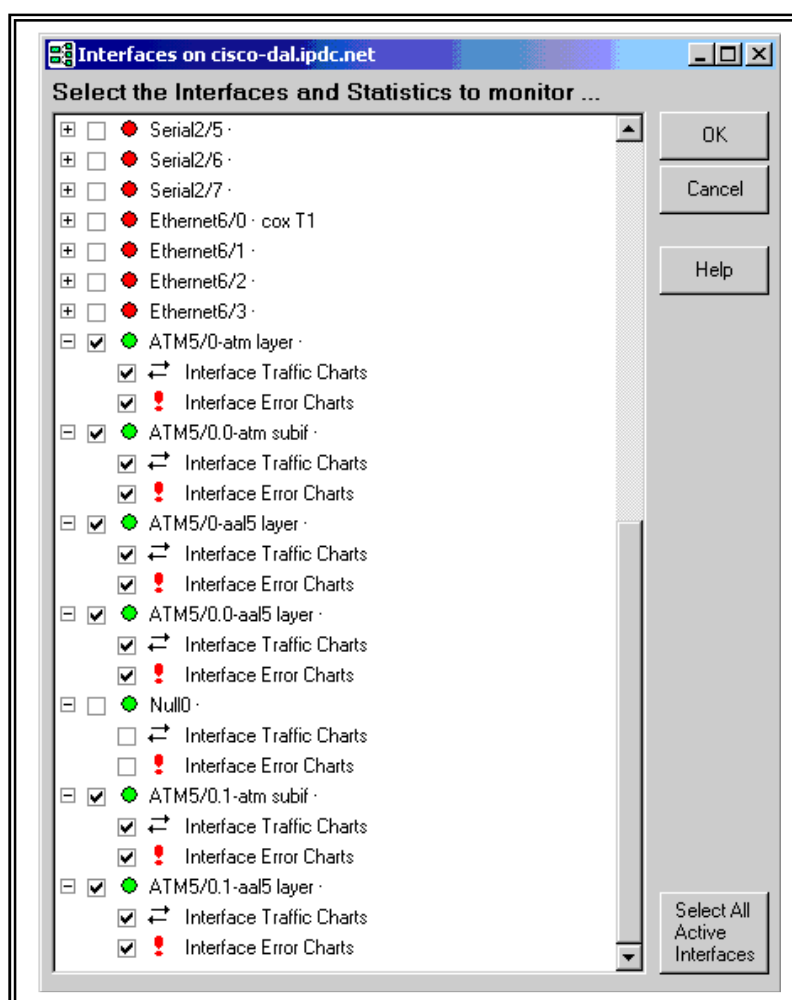


**Gráfico 28. Pantalla para Seleccionar una Interfase y Mostrar la Estadística del Monitoreo**

#### 6.1.5.1.2 SNMP Graph (Gráfico SNMP )

SolarWinds es una colección de datos en tiempo real y una herramienta para graficar los datos desde cualquier MIB (Management Information Base, Base de Información de Gestión) simplemente seleccionando el dispositivo deseado OID.

El SNMP Graph, puede monitorear parámetros como: Trafico, Carga del CPU, Voltaje, usuario Único para el servidor web , temperatura, trafico VoIP (Voz sobre IP), y muchos mas.

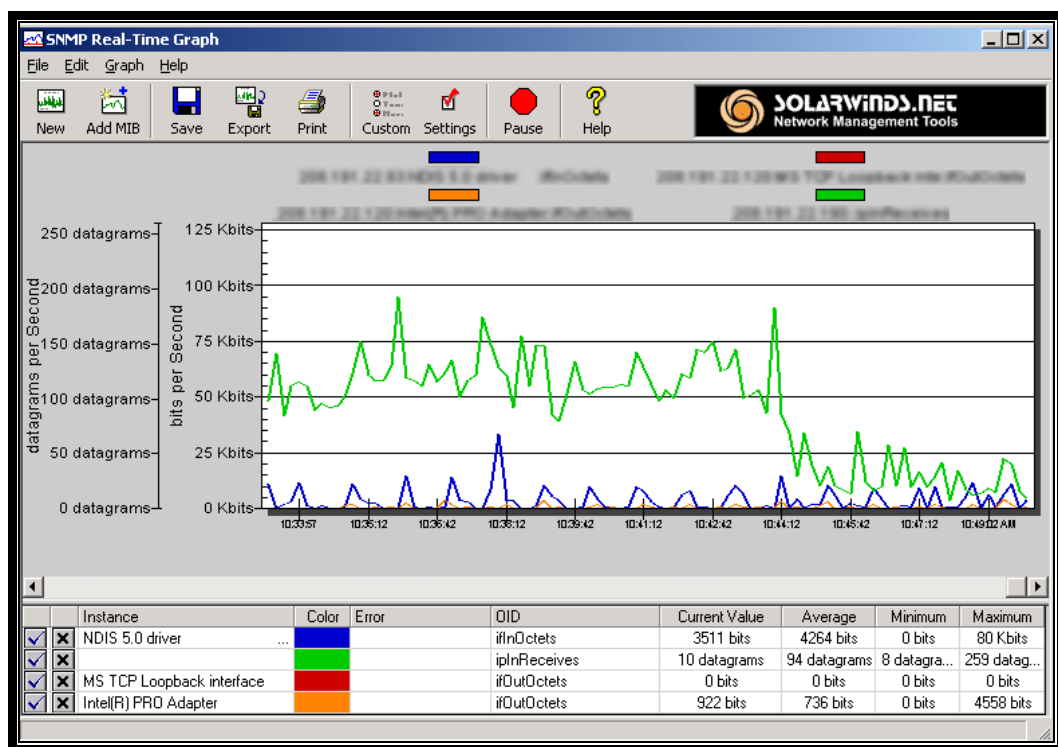
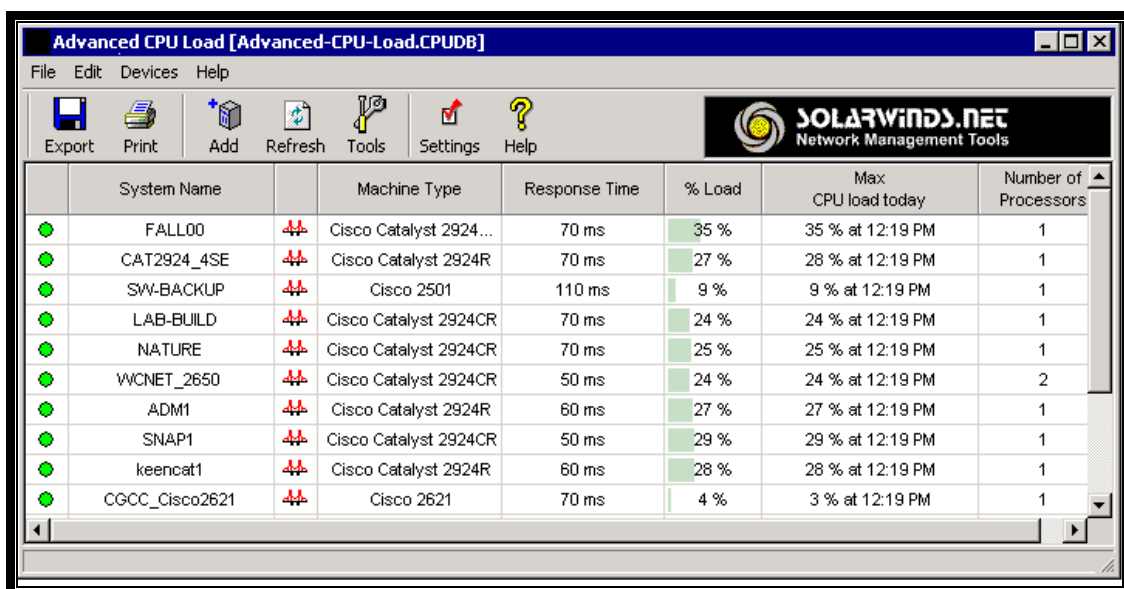


Gráfico 29. Pantalla del Gráfico SNMP (SMNP Graph)

### 6.1.5.1.3 Advanced CPU Load (Carga Avanzada del CPU)

Una utilidad que permite supervisar y graficar la carga de múltiples routers Cisco concurrentemente. Alarmas que pueden ser independientes de cada dispositivo. Si la carga de un router cisco alcanza los parámetros definidos por el usuario para una alarma, la barra de carga se torna en amarillo. Si supera un nivel critico, la barra se torna roja.



The screenshot shows the 'Advanced CPU Load' application window. The title bar reads 'Advanced CPU Load [Advanced-CPU-Load.CPUDB]'. The menu bar includes 'File', 'Edit', 'Devices', and 'Help'. The toolbar contains icons for 'Export', 'Print', 'Add', 'Refresh', 'Tools', 'Settings', and 'Help'. The main area displays a table with the following data:

|   | System Name    |    | Machine Type           | Response Time | % Load | Max CPU load today | Number of Processors |
|---|----------------|----|------------------------|---------------|--------|--------------------|----------------------|
| ● | FALL00         | 🔴🔴 | Cisco Catalyst 2924... | 70 ms         | 35 %   | 35 % at 12:19 PM   | 1                    |
| ● | CAT2924_4SE    | 🔴🔴 | Cisco Catalyst 2924R   | 70 ms         | 27 %   | 28 % at 12:19 PM   | 1                    |
| ● | SW-BACKUP      | 🔴🔴 | Cisco 2501             | 110 ms        | 9 %    | 9 % at 12:19 PM    | 1                    |
| ● | LAB-BUILD      | 🔴🔴 | Cisco Catalyst 2924CR  | 70 ms         | 24 %   | 24 % at 12:19 PM   | 1                    |
| ● | NATURE         | 🔴🔴 | Cisco Catalyst 2924CR  | 70 ms         | 25 %   | 25 % at 12:19 PM   | 1                    |
| ● | WCNET_2650     | 🔴🔴 | Cisco Catalyst 2924CR  | 50 ms         | 24 %   | 24 % at 12:19 PM   | 2                    |
| ● | ADM1           | 🔴🔴 | Cisco Catalyst 2924R   | 60 ms         | 27 %   | 27 % at 12:19 PM   | 1                    |
| ● | SNAP1          | 🔴🔴 | Cisco Catalyst 2924CR  | 50 ms         | 29 %   | 29 % at 12:19 PM   | 1                    |
| ● | keencat1       | 🔴🔴 | Cisco Catalyst 2924R   | 60 ms         | 28 %   | 28 % at 12:19 PM   | 1                    |
| ● | CGCC_Cisco2621 | 🔴🔴 | Cisco 2621             | 70 ms         | 4 %    | 3 % at 12:19 PM    | 1                    |

Gráfico 30. Pantalla de la Carga Avanzada del CPU

### 6.1.5.1.4 CPU Gauges (Medidor del CPU)

El CPU SolarWinds cargará el windows 2000 en las maquinas en forma eficiente, también a los routers Cisco y switch. El CPU Gauges utiliza SNMP para comunicar

con el dispositivo remoto y desplegar los resultados. Esta aplicación usa varias formas que pueden cambiarse para acomodar la preferencia de los usuarios.



**Gráfico 31. Pantalla Mediciones CPU (CPU Gauges)**

#### **6.1.5.2 Network Discovery Tools (Descubrimiento de la Red)**

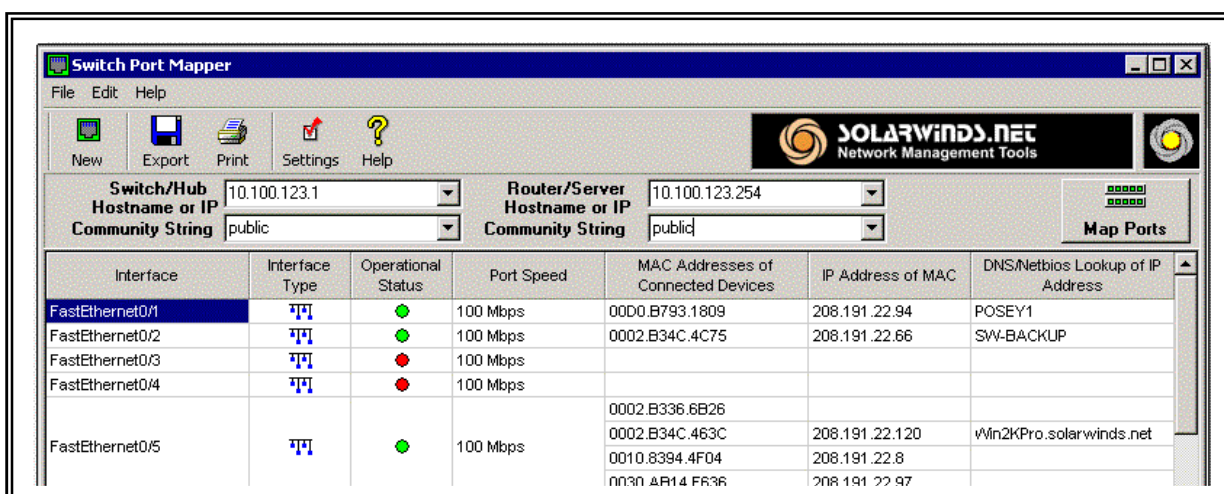
Hay varias aplicaciones del descubrimiento y herramientas incluidas en esta versión de SolarWinds. Algunos hacen la dirección IP mucho más fácil; mientras otros identifican errores de DNS en su red de datos de velocidad alta. Los dos más populares son el Sonar de la red, capaz de crear una base de datos del inventario de clase múltiple y el Buscador de red del IP, es en gran medida el más rápido y el motor más robusto del descubrimiento en la industria.

Es una de las razones por las que SolarWinds fue reconocido en el Network Computing Magazine's como la mejor herramienta de la gestión de redes en el 2002.

Las herramientas incluidas en esta categoría son:

#### 6.1.5.2.1 Switch Port Mapper (Mapeo del Puerto del Interruptor)

Cansados de perseguir los cables y de pasar horas intentando identificar qué está conectado al Switch, ahora se puede descubrir los puertos en cualquier Ethernet manejable y detallar los dispositivos conectados con esos puertos por MAC address, IP address, y el hostname. Puesto que esto es un descubrimiento en tiempo real se puede ver el estado operacional y la velocidad del puerto de cada puerto. El **Switch Port Mapper** hace la documentación de la red fácil. Se puede exportar para sobresalir, pdf, CSV, y HTML.



| Interface       | Interface Type | Operational Status | Port Speed | MAC Addresses of Connected Devices | IP Address of MAC | DNS/Netbios Lookup of IP Address |
|-----------------|----------------|--------------------|------------|------------------------------------|-------------------|----------------------------------|
| FastEthernet0/1 | FastEthernet   | Operational        | 100 Mbps   | 00D0.B793.1809                     | 208.191.22.94     | POSEY1                           |
| FastEthernet0/2 | FastEthernet   | Operational        | 100 Mbps   | 0002.B34C.4C75                     | 208.191.22.66     | SW-BACKUP                        |
| FastEthernet0/3 | FastEthernet   | Not Operational    | 100 Mbps   |                                    |                   |                                  |
| FastEthernet0/4 | FastEthernet   | Not Operational    | 100 Mbps   |                                    |                   |                                  |
| FastEthernet0/5 | FastEthernet   | Operational        | 100 Mbps   | 0002.B336.6B26                     |                   |                                  |
|                 |                |                    |            | 0002.B34C.463C                     | 208.191.22.120    | vWin2KPro.solarwinds.net         |
|                 |                |                    |            | 0010.8394.4F04                     | 208.191.22.8      |                                  |
|                 |                |                    |            | 0030.8B14.F636                     | 208.191.22.97     |                                  |

Gráfico 32. Pantalla del Mapeo del Puerto Switch

#### 6.1.5.2.2 IP Network Browser ( Buscador de Red IP)

Es el buscador de red interactivo de TCP/IP para Windows. Explora una sub red del IP y demuestra qué dispositivos están respondiendo en esa subred. Descubre los detalles sobre cada interfaz, Frame Relay DLCIs,, niveles del IOS, flash memory, puertos del hub (si tiene un hub integrado), tarjetas instaladas, routers, tablas del ARP, y muchos

otros detalles. Incluso puede dar una visión del software instalado y del software ejecutándose en sus servidores.

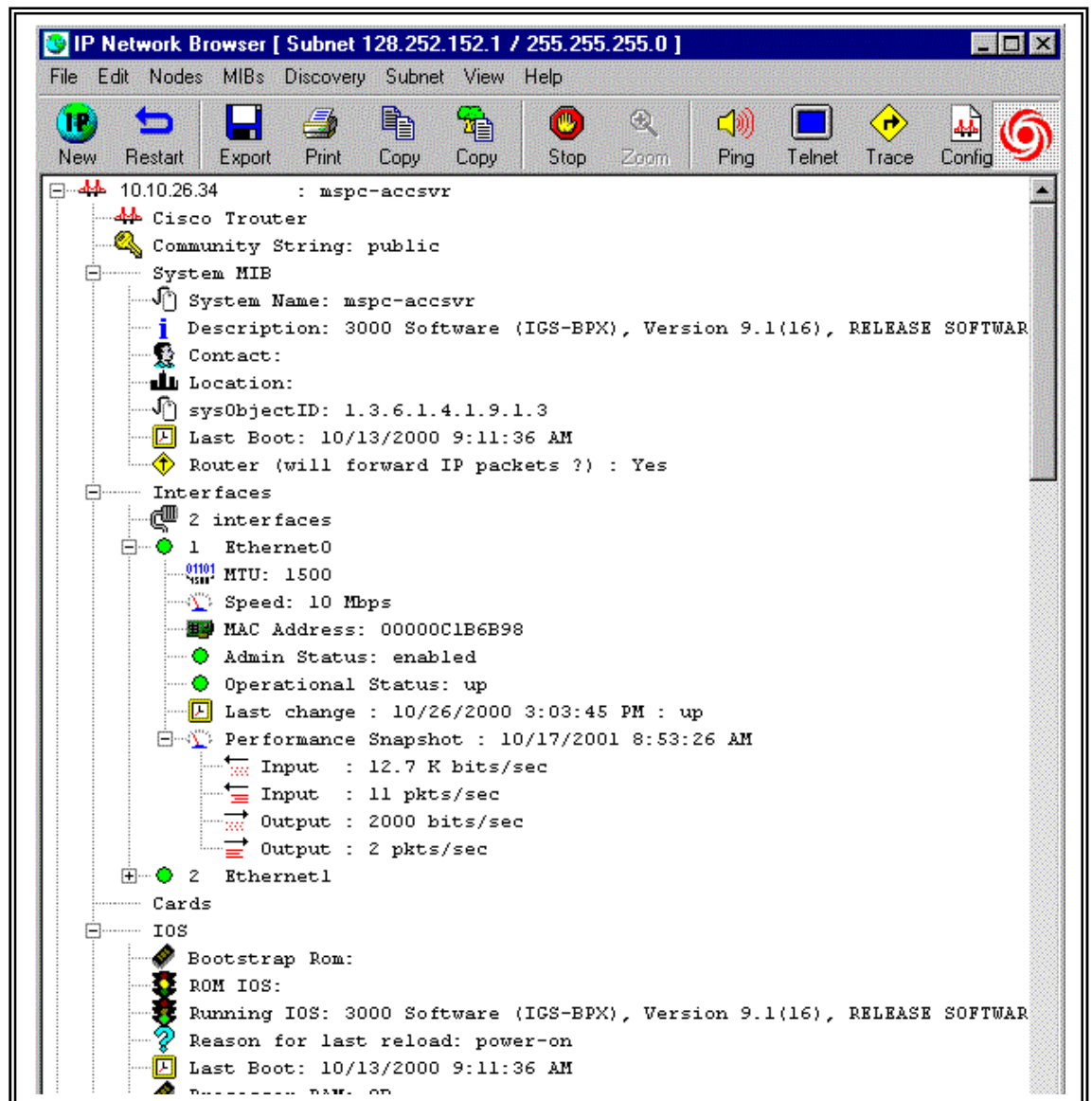
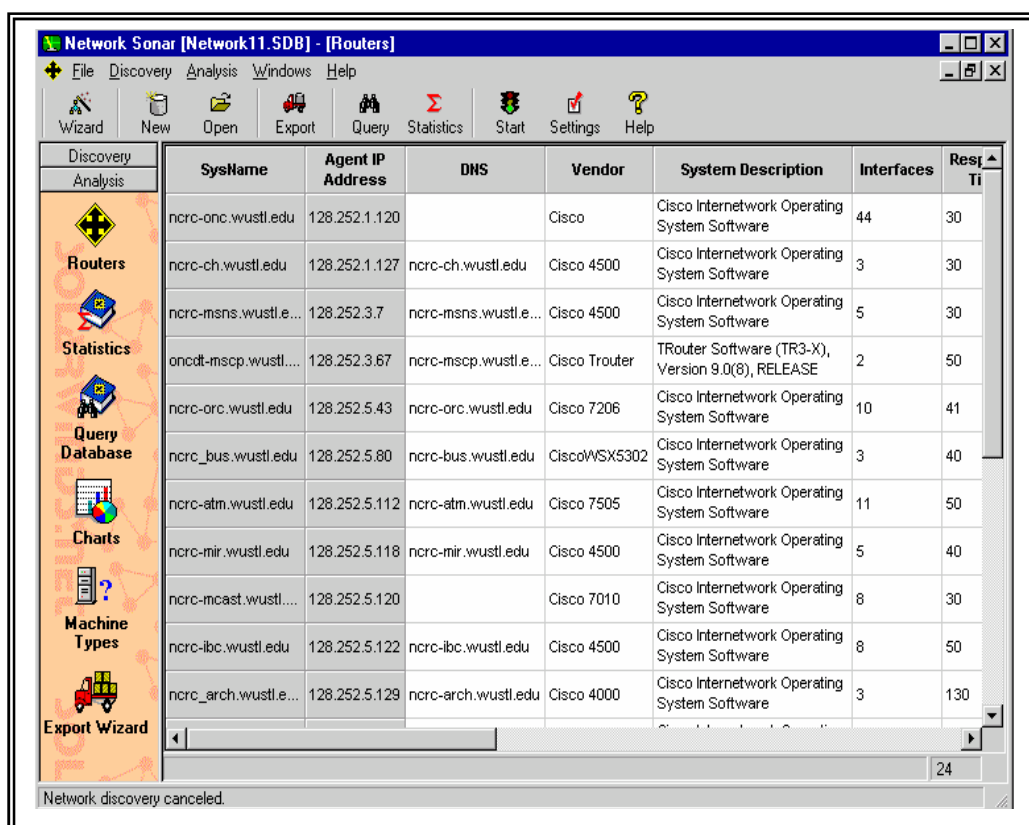


Gráfico 33. Pantalla del Buscador de Red IP

### 6.1.5.2.3 Network Sonar (Sonar de la Red)

El SNMP crea una base de datos detallada del descubrimiento de su red de datos de alta velocidad. Las exportaciones resultan en el MS acceso para el análisis fácil. Tan poderoso alcance, el sonar incluso descubre los dispositivos que no apoyan el SNMP. Éste es el motor más rápido del descubrimiento de la industria para las redes complejas, multi-vendedor. La clase múltiple se puede explorar en cuestión de minutos. El sonar viene con varios informes por defecto y gráficos que se pueden exhibir en el inventario.

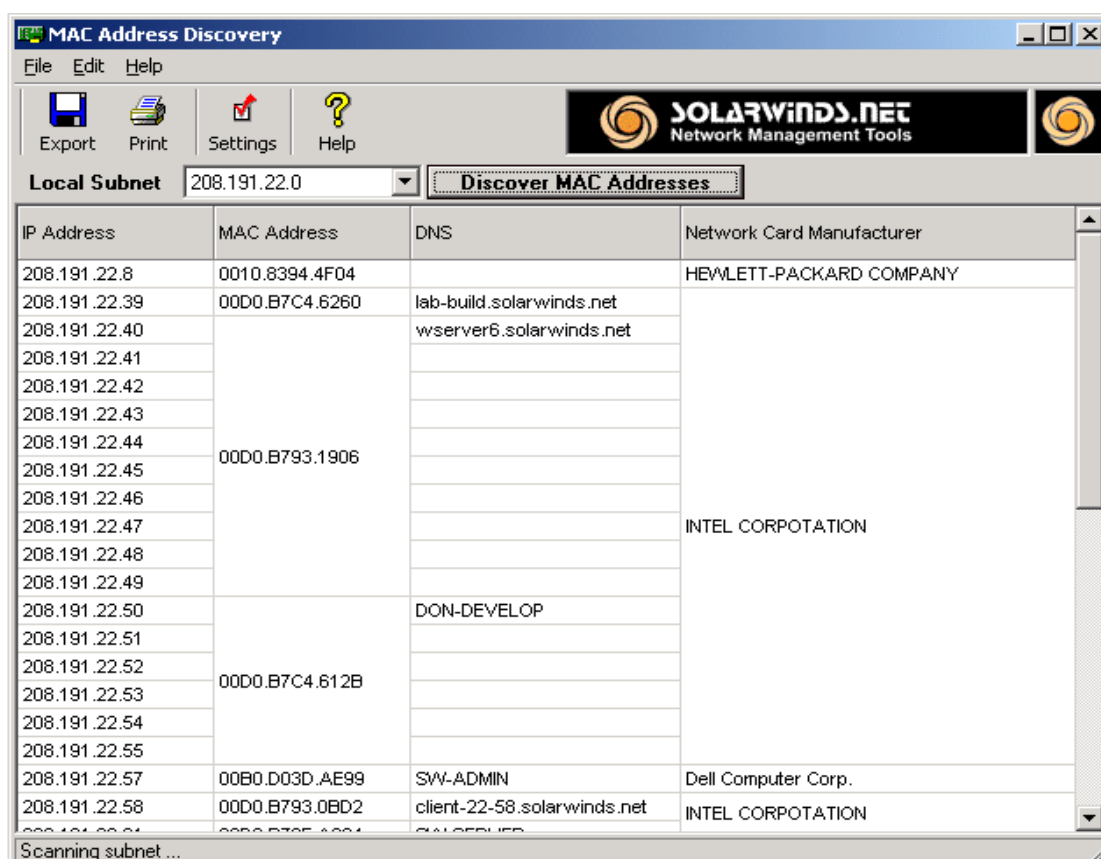


| SysName              | Agent IP Address | DNS                  | Vendor        | System Description                                | Interfaces | Res |
|----------------------|------------------|----------------------|---------------|---------------------------------------------------|------------|-----|
| ncrc-orc.wustl.edu   | 128.252.1.120    |                      | Cisco         | Cisco Internetwork Operating System Software      | 44         | 30  |
| ncrc-ch.wustl.edu    | 128.252.1.127    | ncrc-ch.wustl.edu    | Cisco 4500    | Cisco Internetwork Operating System Software      | 3          | 30  |
| ncrc-msns.wustl.e... | 128.252.3.7      | ncrc-msns.wustl.e... | Cisco 4500    | Cisco Internetwork Operating System Software      | 5          | 30  |
| oncdt-mscp.wustl.... | 128.252.3.67     | ncrc-mscp.wustl.e... | Cisco Trouter | TRouter Software (TR3-X), Version 9.0(8), RELEASE | 2          | 50  |
| ncrc-orc.wustl.edu   | 128.252.5.43     | ncrc-orc.wustl.edu   | Cisco 7206    | Cisco Internetwork Operating System Software      | 10         | 41  |
| ncrc_bus.wustl.edu   | 128.252.5.80     | ncrc-bus.wustl.edu   | CiscoWSX5302  | Cisco Internetwork Operating System Software      | 3          | 40  |
| ncrc-atm.wustl.edu   | 128.252.5.112    | ncrc-atm.wustl.edu   | Cisco 7505    | Cisco Internetwork Operating System Software      | 11         | 50  |
| ncrc-mir.wustl.edu   | 128.252.5.118    | ncrc-mir.wustl.edu   | Cisco 4500    | Cisco Internetwork Operating System Software      | 5          | 40  |
| ncrc-mcast.wustl.... | 128.252.5.120    |                      | Cisco 7010    | Cisco Internetwork Operating System Software      | 8          | 30  |
| ncrc-ibc.wustl.edu   | 128.252.5.122    | ncrc-ibc.wustl.edu   | Cisco 4500    | Cisco Internetwork Operating System Software      | 8          | 50  |
| ncrc_arch.wustl.e... | 128.252.5.129    | ncrc-arch.wustl.edu  | Cisco 4000    | Cisco Internetwork Operating System Software      | 3          | 130 |

Gráfico 34. Monitoreo de una Sub Red con el Sonar

#### 6.1.5.2.4 MAC Address Discovery (Descubrimiento de Direcciones MAC)

El descubrimiento del MAC Address de SolarWinds explorará la subred en la cual se unirá y construirá una tabla relacional de IP address con el MAC address, el DNS, el fabricante de la tarjeta de la red y la dirección del fabricante. El mejor método de descubrir las direcciones del MAC de otras subredes es colocar las herramientas SolarWinds en una computadora portátil y llevar la computadora para escanear en forma remota la subred. Para explorar múltiples subredes, se recomienda utilizar el Network Sonar



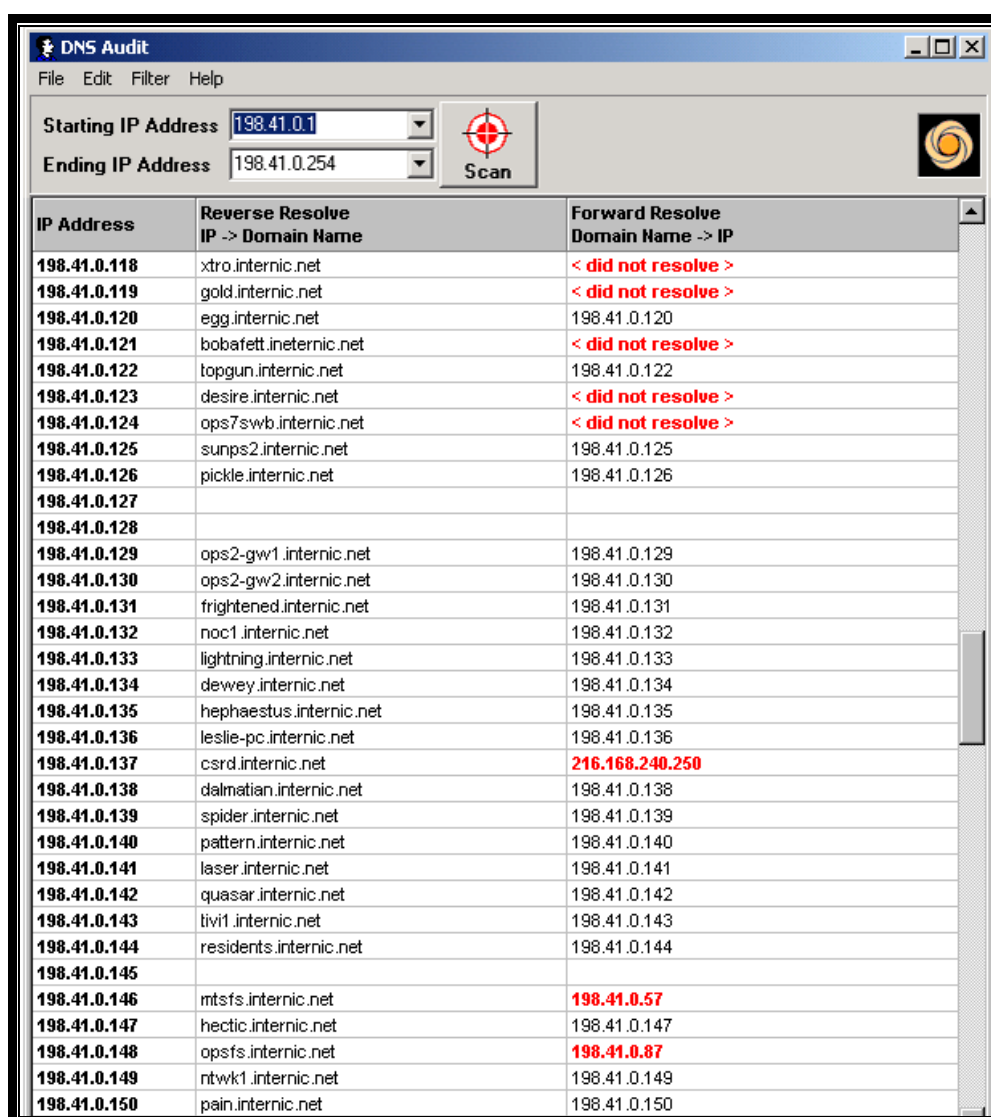
The screenshot shows the 'MAC Address Discovery' application window. It has a menu bar (File, Edit, Help) and a toolbar with icons for Export, Print, Settings, and Help. The 'Local Subnet' is set to '208.191.22.0'. A 'Discover MAC Addresses' button is visible. Below the toolbar is a table with four columns: IP Address, MAC Address, DNS, and Network Card Manufacturer. The table contains several rows of data, including IP addresses from 208.191.22.8 to 208.191.22.58, various MAC addresses, DNS names like 'lab-build.solarwinds.net' and 'client-22-58.solarwinds.net', and manufacturer names like 'HEWLETT-PACKARD COMPANY', 'INTEL CORPOTATION', and 'Dell Computer Corp.'. A status bar at the bottom indicates 'Scanning subnet ...'.

| IP Address    | MAC Address    | DNS                         | Network Card Manufacturer |
|---------------|----------------|-----------------------------|---------------------------|
| 208.191.22.8  | 0010.8394.4F04 |                             | HEWLETT-PACKARD COMPANY   |
| 208.191.22.39 | 00D0.B7C4.6260 | lab-build.solarwinds.net    |                           |
| 208.191.22.40 |                | wserver6.solarwinds.net     |                           |
| 208.191.22.41 |                |                             |                           |
| 208.191.22.42 |                |                             |                           |
| 208.191.22.43 |                |                             |                           |
| 208.191.22.44 | 00D0.B793.1906 |                             |                           |
| 208.191.22.45 |                |                             |                           |
| 208.191.22.46 |                |                             |                           |
| 208.191.22.47 |                |                             | INTEL CORPOTATION         |
| 208.191.22.48 |                |                             |                           |
| 208.191.22.49 |                |                             |                           |
| 208.191.22.50 |                | DON-DEVELOP                 |                           |
| 208.191.22.51 |                |                             |                           |
| 208.191.22.52 | 00D0.B7C4.612B |                             |                           |
| 208.191.22.53 |                |                             |                           |
| 208.191.22.54 |                |                             |                           |
| 208.191.22.55 |                |                             |                           |
| 208.191.22.57 | 00B0.D03D.AE99 | SVV-ADMIN                   | Dell Computer Corp.       |
| 208.191.22.58 | 00D0.B793.0BD2 | client-22-58.solarwinds.net | INTEL CORPOTATION         |

Gráfico 35. Pantalla para Obtener la Dirección MAC

### 6.1.5.2.5 DNS audit (Auditoria DNS)

Con el crecimiento de la red, no se puede perder de vista cada IP address y dominio asignados. El inventario del DNS no solamente es importante para la IP address sino también para validar los nombres correctos del dominio.



The screenshot shows the 'DNS Audit' application window. It has a menu bar with 'File', 'Edit', 'Filter', and 'Help'. Below the menu bar, there are two input fields: 'Starting IP Address' with the value '198.41.0.1' and 'Ending IP Address' with the value '198.41.0.254'. To the right of these fields is a 'Scan' button with a target icon. Further right is a small circular logo. Below the input fields is a table with three columns: 'IP Address', 'Reverse Resolve IP -> Domain Name', and 'Forward Resolve Domain Name -> IP'. The table contains 32 rows of data, showing a range of IP addresses from 198.41.0.118 to 198.41.0.150 and their corresponding domain names. Some entries in the 'Forward Resolve' column are marked as 'did not resolve' or show an external IP address.

| IP Address   | Reverse Resolve<br>IP -> Domain Name | Forward Resolve<br>Domain Name -> IP |
|--------------|--------------------------------------|--------------------------------------|
| 198.41.0.118 | xtro.internic.net                    | < did not resolve >                  |
| 198.41.0.119 | gold.internic.net                    | < did not resolve >                  |
| 198.41.0.120 | egg.internic.net                     | 198.41.0.120                         |
| 198.41.0.121 | bobafett.internic.net                | < did not resolve >                  |
| 198.41.0.122 | topgun.internic.net                  | 198.41.0.122                         |
| 198.41.0.123 | desire.internic.net                  | < did not resolve >                  |
| 198.41.0.124 | ops7swb.internic.net                 | < did not resolve >                  |
| 198.41.0.125 | sunps2.internic.net                  | 198.41.0.125                         |
| 198.41.0.126 | pickle.internic.net                  | 198.41.0.126                         |
| 198.41.0.127 |                                      |                                      |
| 198.41.0.128 |                                      |                                      |
| 198.41.0.129 | ops2-gw1.internic.net                | 198.41.0.129                         |
| 198.41.0.130 | ops2-gw2.internic.net                | 198.41.0.130                         |
| 198.41.0.131 | frightened.internic.net              | 198.41.0.131                         |
| 198.41.0.132 | noc1.internic.net                    | 198.41.0.132                         |
| 198.41.0.133 | lightning.internic.net               | 198.41.0.133                         |
| 198.41.0.134 | dewey.internic.net                   | 198.41.0.134                         |
| 198.41.0.135 | hephaestus.internic.net              | 198.41.0.135                         |
| 198.41.0.136 | leslie-pc.internic.net               | 198.41.0.136                         |
| 198.41.0.137 | csrd.internic.net                    | 216.168.240.250                      |
| 198.41.0.138 | dalmatian.internic.net               | 198.41.0.138                         |
| 198.41.0.139 | spider.internic.net                  | 198.41.0.139                         |
| 198.41.0.140 | pattern.internic.net                 | 198.41.0.140                         |
| 198.41.0.141 | laser.internic.net                   | 198.41.0.141                         |
| 198.41.0.142 | quasar.internic.net                  | 198.41.0.142                         |
| 198.41.0.143 | tivi1.internic.net                   | 198.41.0.143                         |
| 198.41.0.144 | residents.internic.net               | 198.41.0.144                         |
| 198.41.0.145 |                                      |                                      |
| 198.41.0.146 | mtsfs.internic.net                   | 198.41.0.57                          |
| 198.41.0.147 | hectic.internic.net                  | 198.41.0.147                         |
| 198.41.0.148 | opsfs.internic.net                   | 198.41.0.87                          |
| 198.41.0.149 | ntwk1.internic.net                   | 198.41.0.149                         |
| 198.41.0.150 | pain.internic.net                    | 198.41.0.150                         |

Gráfico 36. Auditoria DNS

#### 6.1.5.2.6 SNMP Sweep (Barrido SNMP)

Es una combinación de Ping Sweep (Barrido Ping) y SNMP Discovery tool (herramienta de descubrimiento SNMP).

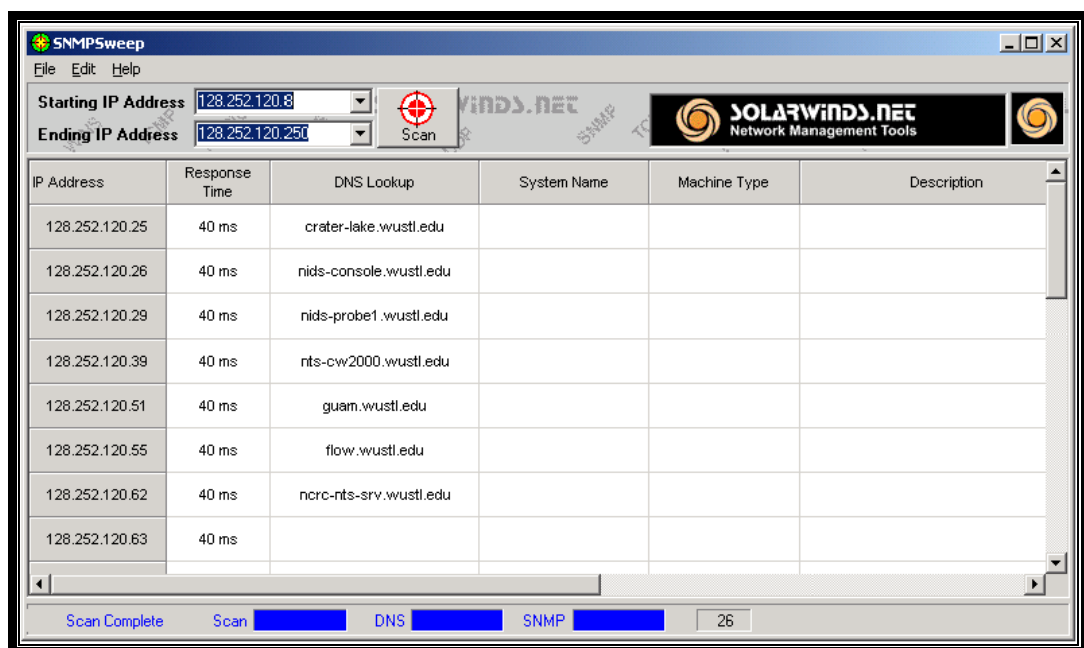


**Gráfico 37. Barrido SNMP**

El **SNMP Sweep** define el rango de las IP address y después localiza las direcciones usadas y no usadas. Es una manera rápida y simple de explorar una subred y un descubrimiento de su contenido.

#### 6.1.5.2.7 Subnet List (Lista SubRed)

Con la lista de la subred (subset list) se puede descubrir rápidamente todas las subredes y máscaras en una red.

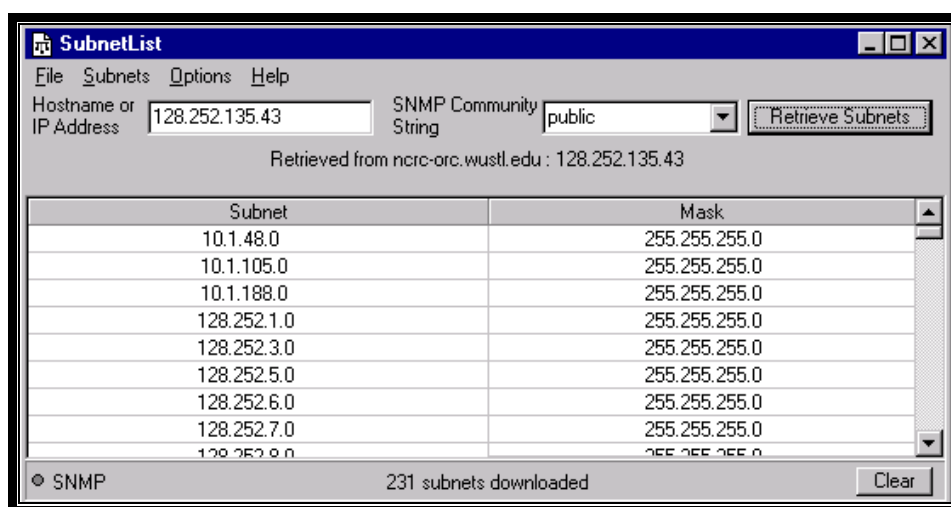


Gráfico 38. Lista de Subred

#### 6.1.5.3 Tools For Cisco Routers (Herramientas para Redes Cisco)

Esta edición contiene específicamente varias herramientas diseñadas para mantener una interfase gráfica simple la dirección de sus Routers de Cisco. Del **Config Downloader** al **Config Uploader** al **Config Editor/Viewer** estas herramientas hacen mucho mas fácil la configuración del Router. Con el **Compare Running vs. Startup Configs** se puede Comparar incluso la configuración Ejecutándose vs. Iniciándose en sus Routers de Cisco remotos. Con el **Advanced Router CPU Load** se puede ver la carga del

tiempo real en los routers. Otras herramientas incluidas son: Proxy Ping, Router Password Decryption, Router Security Check and CPU Gauge.

#### 6.1.5.3.1 Advanced Router CPU Load (Carga Avanzada del CPU Router)

Permite monitorear en tiempo real la carga de los routers Cisco. Cada Router es nvisto como una barra horizontal

Puede ser configurado para enviar alertas de mensajes; sin embargo la carga de los Routers va sobre el punto de un usuario definido.

Advirtiendoy por medio de Alarmas que pueden ponerse umbrales independientemente para cada dispositivo. Si la carga en un Router de Cisco alcanza la definida por el usuario, el umbral del indicador se pone Amarillo o Rojo.

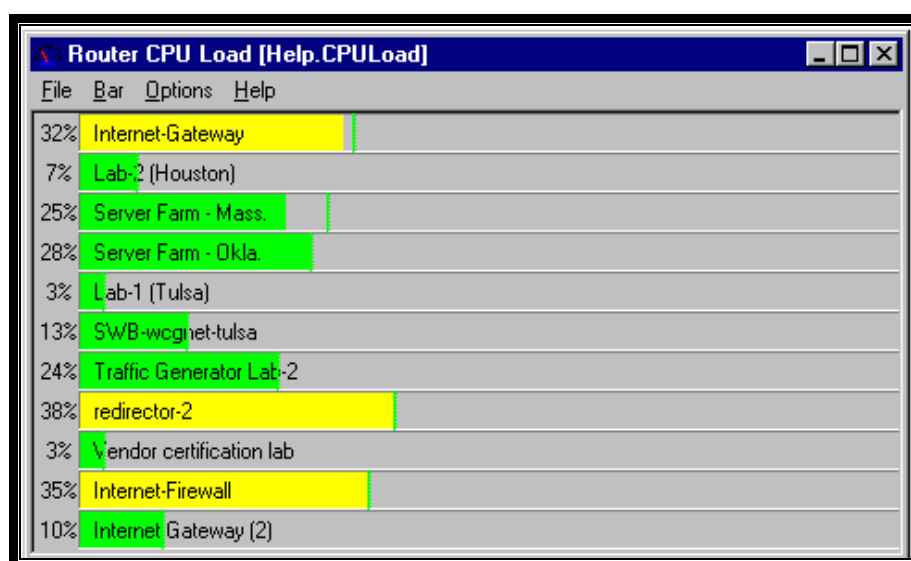


Gráfico 39. Carga Avanzada del CPU Router1

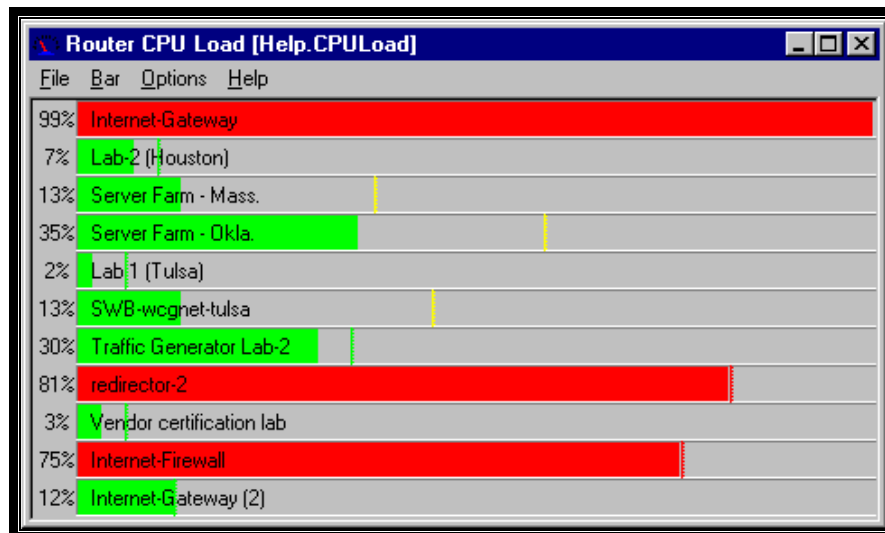


**Gráfico 40. Carga Avanzada del CPU Router2**

Se puede imprimir la carga de todos los Routers. Se muestra como la impresora saca desde la vista de esta herramienta.

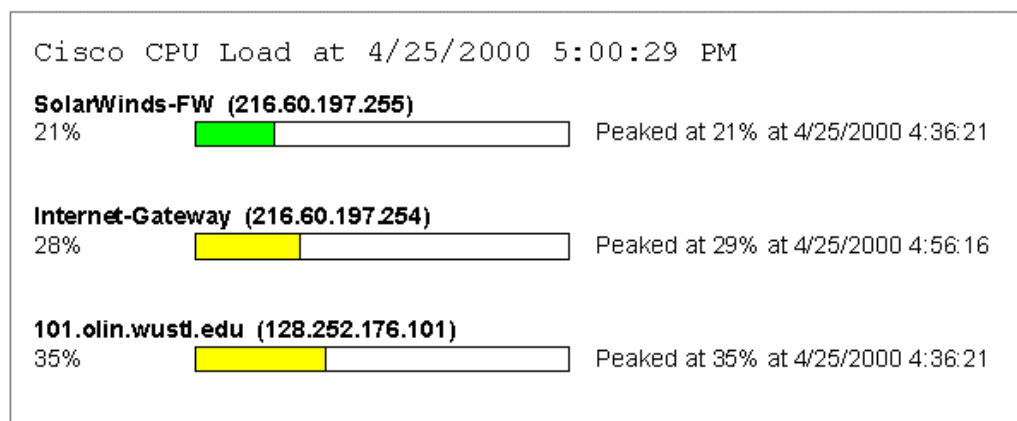


**Gráfico 41. Muestra de Impresión por Pantalla de la Carga del CPU Avanzada**

#### 6.1.5.3.2 Config Downloaded (Descarga de Configuración)

Transmite un archivo de la configuración de un Cisco CMTS o Router de la red a su PC. El Config Download es la herramienta que puede transmitir configuraciones rápidamente y puede archivarlas para el uso más tarde. No necesita ver la Configuración transmitida cada tiempo. La mayor utilidad del Config Download es que puede especificar el directorio designado y que configuración se guarda.

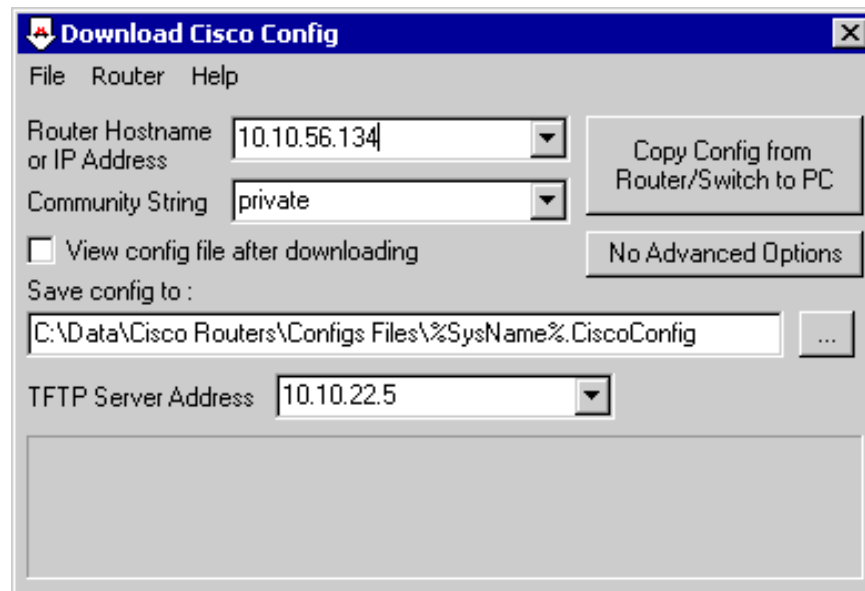


**Gráfico 42. Descarga de la Configuración.**

#### 6.1.5.3.3 Config Uploader (Carga de Configuración)

Puede ser usada no sólo upload de nuevo a una nueva configuración a un Router de Cisco pero también puede cambiarse cualquier configuración Cisco o parámetro vía SNMP. Esto incluye cambiando a un desconocido habilitado o contraseña de Login.

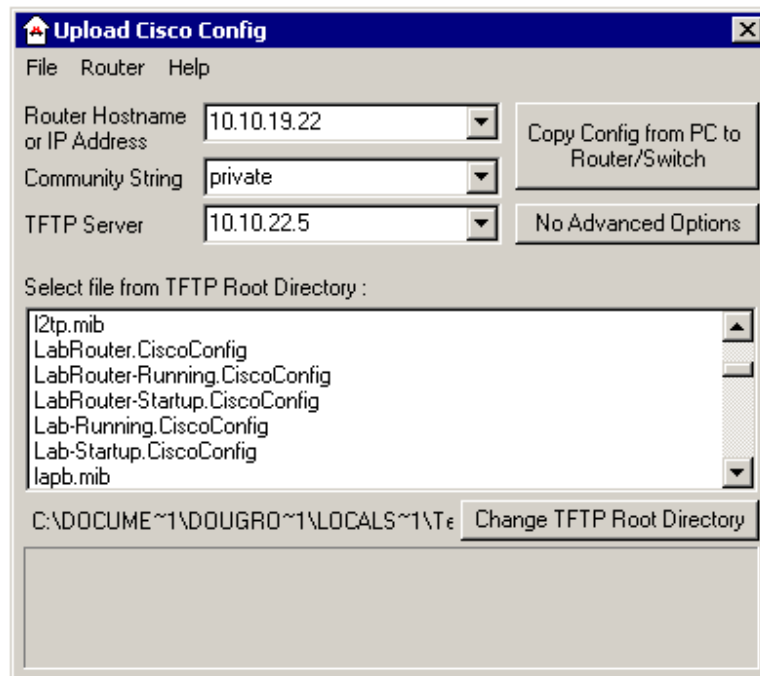


**Gráfico 43. Carga de la Configuración.**

#### **6.1.5.3.4 Config Editor/Viewer (Vista/Edición Configuración)**

Con el Config Viewer se puede rapidamente extraer la Configuración del router Cisco y archivarla para referencia futura. También es capaz de desencriptar contraseñas . Si se usa al Config Viewer se puede descargar la configuración del Router Cisco desde el Cisco PIX o Servidores de Acceso (ex: AS5200) se puede desencriptar todas las Contraseñas del usuario en segundos.

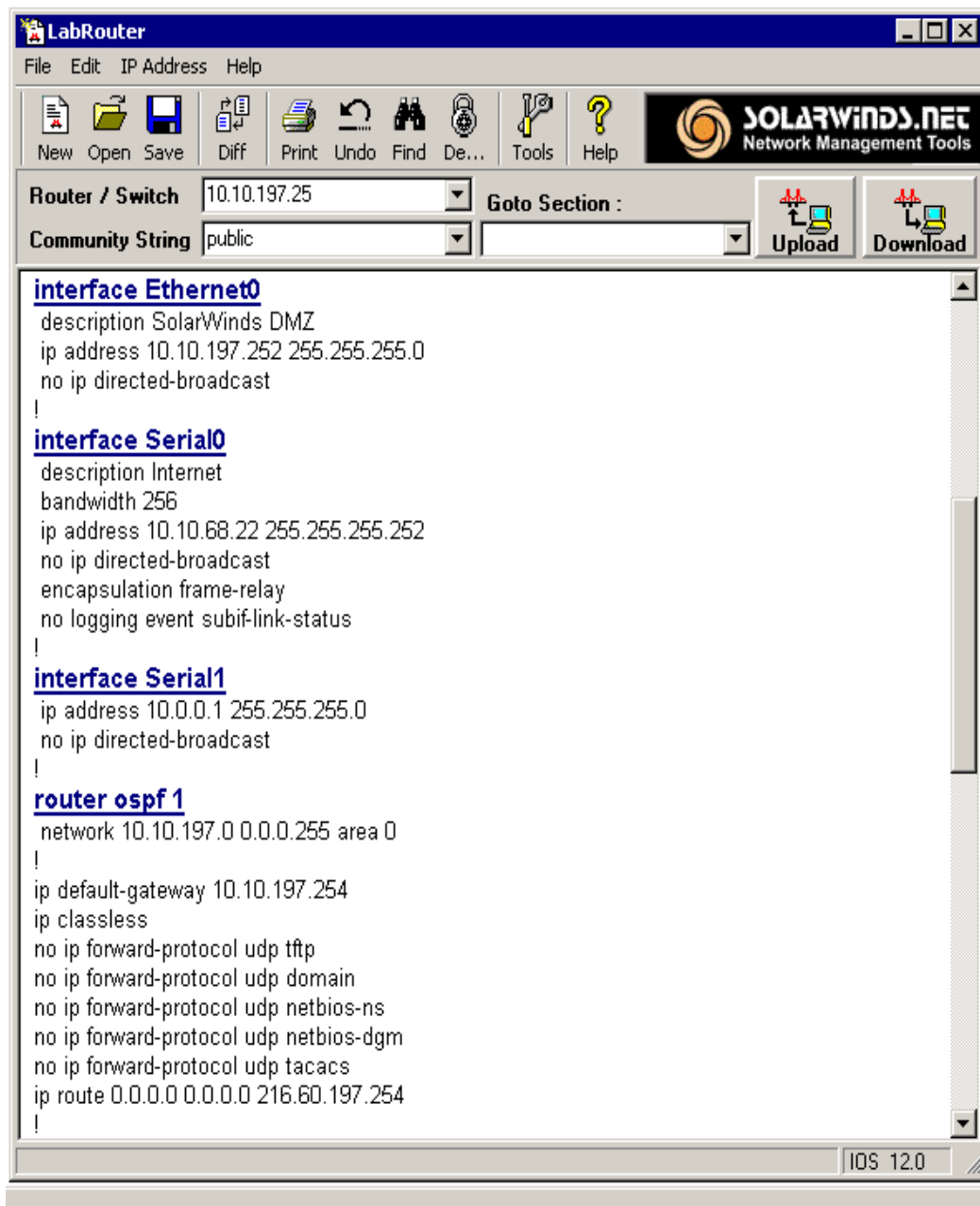


**Gráfico 44. Pantalla Vista Edición y Configuración.**

#### 6.1.5.3.5 Compare Running vs Startup Configs (Comparación de Configuración Inicial vs Ejecución)

Puede ser usado para comparar el Config Running de un Router Cisco con el Startup Config y almacenarla esta comparación en la NVRAM no-volátil. Si alguien ha cambiado la configuración de un Router Cisco, pero no ha comprometido los cambios en la memoria no-volátil, habrá diferencias entonces en las dos configuraciones.

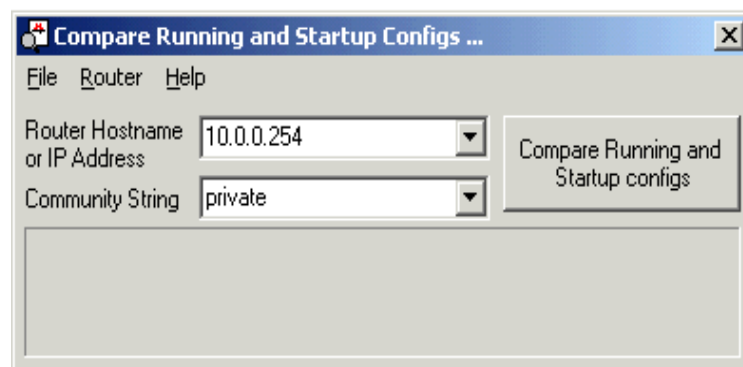


**Gráfico 45. Pantalla de Comparación de Configuración Inicial vs Ejecución**

#### 6.1.5.3.6 Proxy Ping (Apoderado Ping )

Con Proxy Ping es posible comenzar una prueba de PING remotamente desde cualquier Router Cisco a cualquier otro dispositivo SNMP habilitado. El resultado del ICMP se calculan basándose en los paquetes enviados directamente desde el Router Cisco a otro dispositivo remoto. Estas herramientas son excelentes para probar links entre dos sitios remotos.

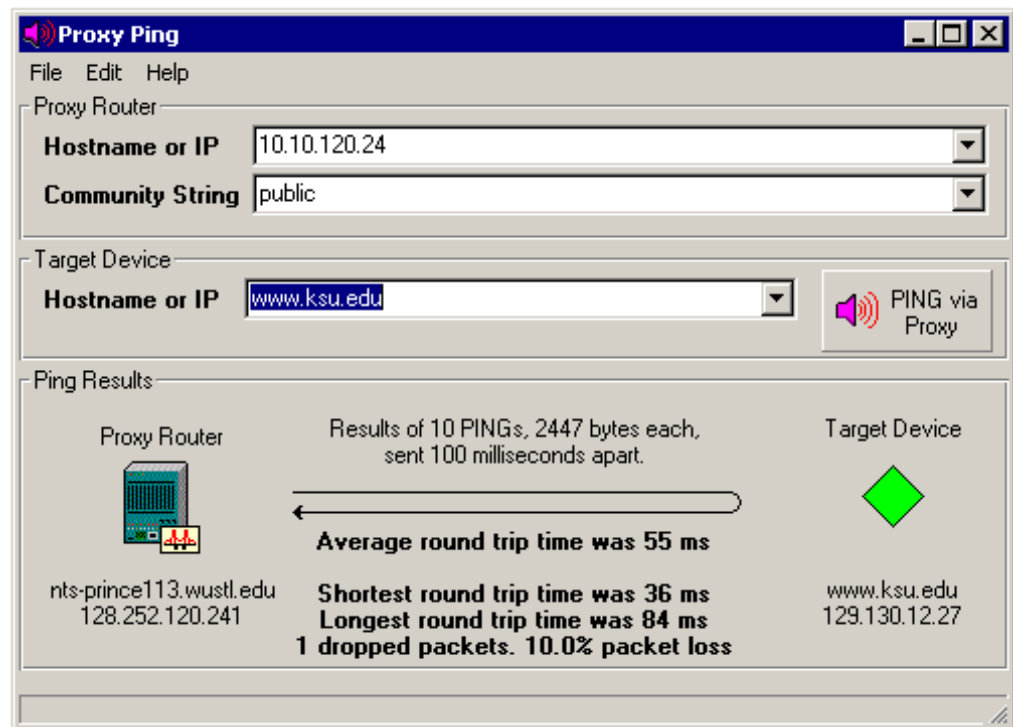


**Gráfico 46. Ping Apoderado**

Para iniciar el Proxy Ping se necesita ingresar el host name o la dirección IP del router Cisco que se quiera usar como proxy.



**Gráfico 47. Icono Proxy Ping.**

#### 6.1.5.3.7 Router Password Decryption (Desencriptar Clave del router)

Puede desencriptar cualquier tipo de Contraseñas de Cisco para los Routers Cisco. Simplemente descargar la configuración del router Cisco y obtener el login en un archivo encriptado y habilitar las contraseñas. Copiar y Pegar esta encriptación en el Router Password Decryption y tenemos la contraseña.

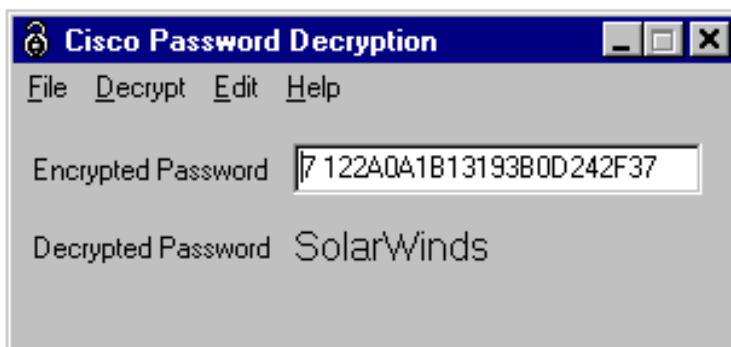


**Gráfico 48. Desencriptar Clave Router.**

#### 6.1.5.3.8 CPU Gauge (Medidas CPU)

Supervisar la carga de las máquinas en Windows 2000 así como los Routers de Cisco y switches. El CPU Gauges utiliza SNMP para comunicarse con el dispositivo remoto y desplegar los resultados.

Esta utilidad tiene tres áreas del usuario: Setup (configuración), Load Saved Profile y Change Tool Skin. Esta aplicación envía varios formas que pueden cambiarse para acomodar la preferencia de los usuarios.

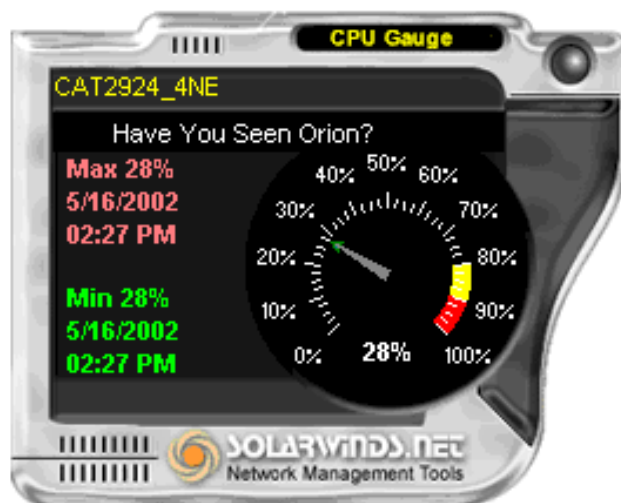


**Gráfico 49. Medidas CPU**

#### **6.1.5.3.9 Router Security Check (Chequeo Seguridad Router)**

Debido a la naturaleza de seguridad de esta herramienta la Versión de Evaluación de SolarWinds no contiene una versión del funcionamiento de la herramienta Router Security Check.

Router Security Check analiza el Router de Cisco y determina si el SNMP Community String es vulnerable e intentará determinar solo lectura o lectura – escritura para SNMP Community String., además es importante asegurarse que sus SNMP Community String sea seguro y confiable.

Los resultados desplegados son:

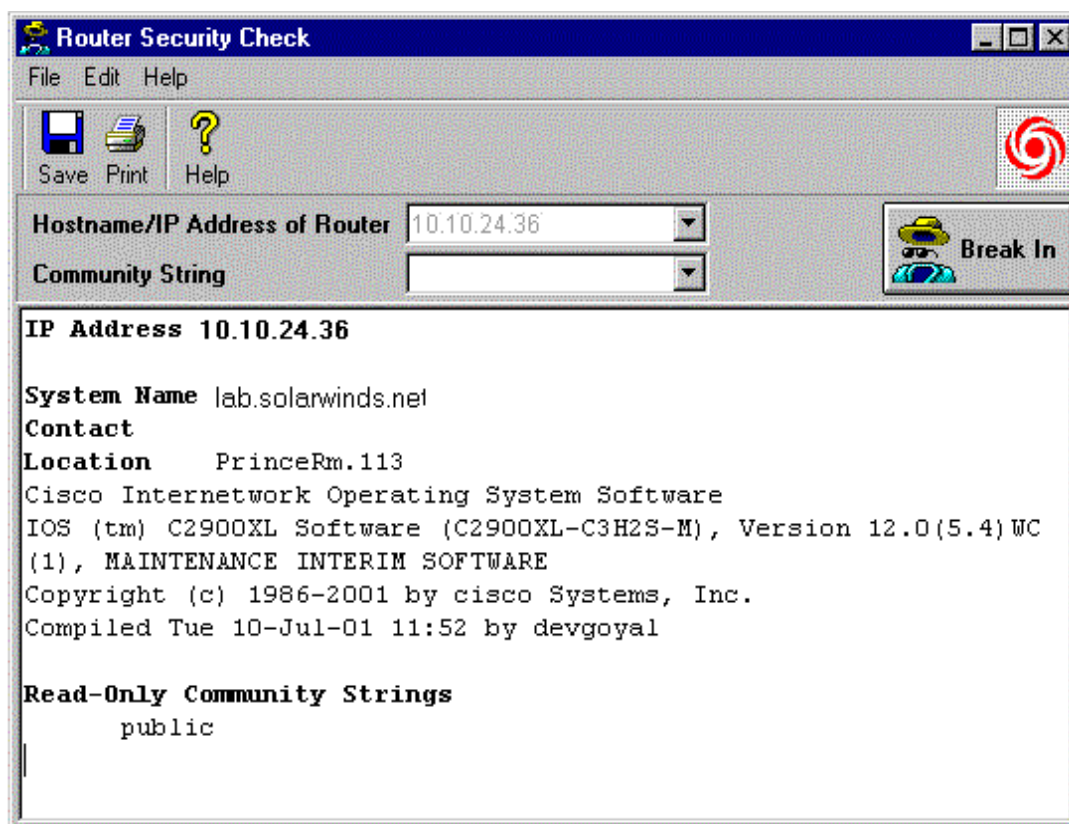


**Gráfico 50. Chequeo Seguridad Router**

#### **6.1.5.4 Fault Monitoring Tools (Herramienta que Supervisa Fallas)**

El Network Monitorings totalmente una aplicación de dirección interactiva que permite supervisar dispositivos seleccionados y enviar alarmas en condiciones del paro.

Otra herramienta útil es el **Watch It!** utilidad que permite guardar en el pulso de la red.

Con la **Bandwidth Monitor** se puede desplegar una vista gráfica del tráfico en la red.

Las herramientas que incluye esta categoría son:

#### **6.1.5.4.1 Network Monitor (Monitor de Red)**

Se Guarda en el pulso de la red 24 horas, un día con el Network Monitor supervisará cientos de nodos concurrentemente y proporcionará indicadores alertas visuales y Alarmas audibles, así como también envían mensajes de e-mail y páginas cuando los dispositivos no responden.

Network Monitor archiva sobre los 3 años de historia Gráfica de la velocidad alta monitoreada en los nodos y le permiten mostrar los resultados.

Se puede ver mapas totalmente interactivos de tiempo de respuesta y pérdida de paquetes. Usar el Mouse para resaltar un área del mapa y mostrar mas detalles.

Esta aplicación es una actuación en tiempo real , la cual puede rastrear latencia de la red, pérdida de paquetes, tráfico, uso del ancho de banda, y muchas otras estadísticas de la red, además puede manejar cada nodo e interfase vía SNMP y reportar cuando un reboots o una interfase esta abajo.

Es ideal para supervisar la utilización del bandwidth de los routers, switches y servidores que están en línea y los mapas históricos de la red.

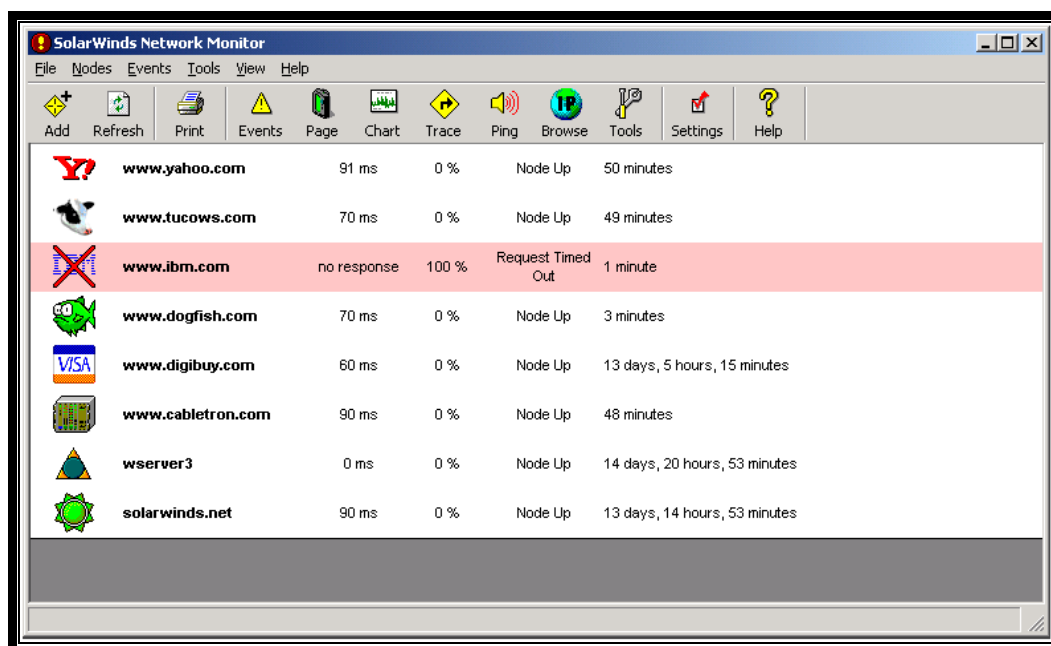


**Gráfico 51. Monitor de Red**

#### 6.1.5.4.2 SysLog Server (Servidor SysLog)

Esta herramienta escucha los mensajes entrantes de Syslog sobre el puerto 514 UDP y los descifra a los mensajes con el propósito de anotarlos.

Con el SolarWinds Syslog server se puede enviar también mensajes de Syslog a otro servidor del syslog.

Esta característica normalmente se usa para agregar mensajes manualmente a la base de datos del syslog remoto durante la actualización del sistema o mientras es arreglando algún problema de la red.

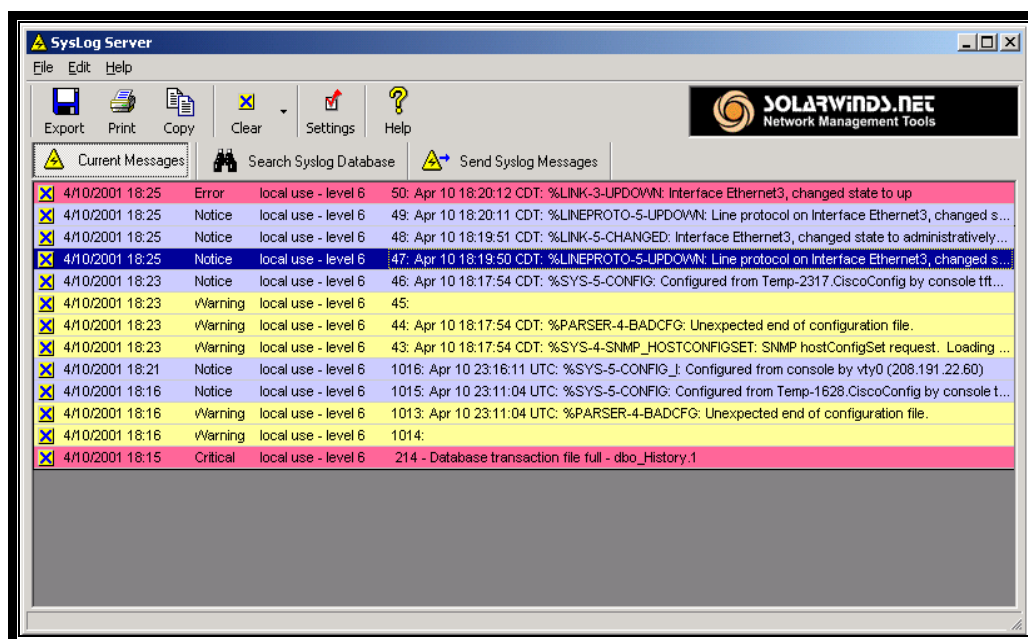


Gráfico 52. Pantalla Servidor SysLog

#### 6.1.5.4.3 Watch it; (Miraloj)

Nunca otra vez conteste el teléfono para decir que el servidor está abajo. Con el Watch It ; se puede supervisar la disponibilidad de varios dispositivos anunciando los estados o indicadores de alertas con los colores verde, amarillo y rojo.



Gráfico 53. Pantalla Miraloj

#### **6.1.5.5 MIB Browser Tools (Herramientas MIB)**

Uno de los métodos primarios para supervisar remotamente y manejar los dispositivos de la red es el uso de MIB. La información disponible en los dispositivos de la red vía SNMP se define por un juego de objetos manejados llamados como el SNMP Dirección Información Base (MIB). Las herramientas de red del SolarWinds utilizan normas para coleccionar la información de varios dispositivos de la red. SolarWinds ha compilado una biblioteca de MIB extensa por encima de 200,000 OID (el Objeto ID).

Las herramientas de esta suite son las siguientes:

##### **6.1.5.5.1 MIB Browser (Buscador MIB)**

SolarWinds utiliza esta aplicación como una base de datos extensa que contiene mas de 200,000 únicos OID y ha compilado por encima de mil MIBs normales. El Navegador de MIB puede mostrar el árbol MIB, tablas de vista MIB, Bowser MIBs, modificar remotamente valores SNMP y muchas otras funciones de SNMP. Además permite a un ingeniero hacer los cambios al dispositivo remoto. El dispositivo remoto podría ser un Router, Switch Hub, Servidor, Firewall, o cualquier otro dispositivo que soporta SNMP.

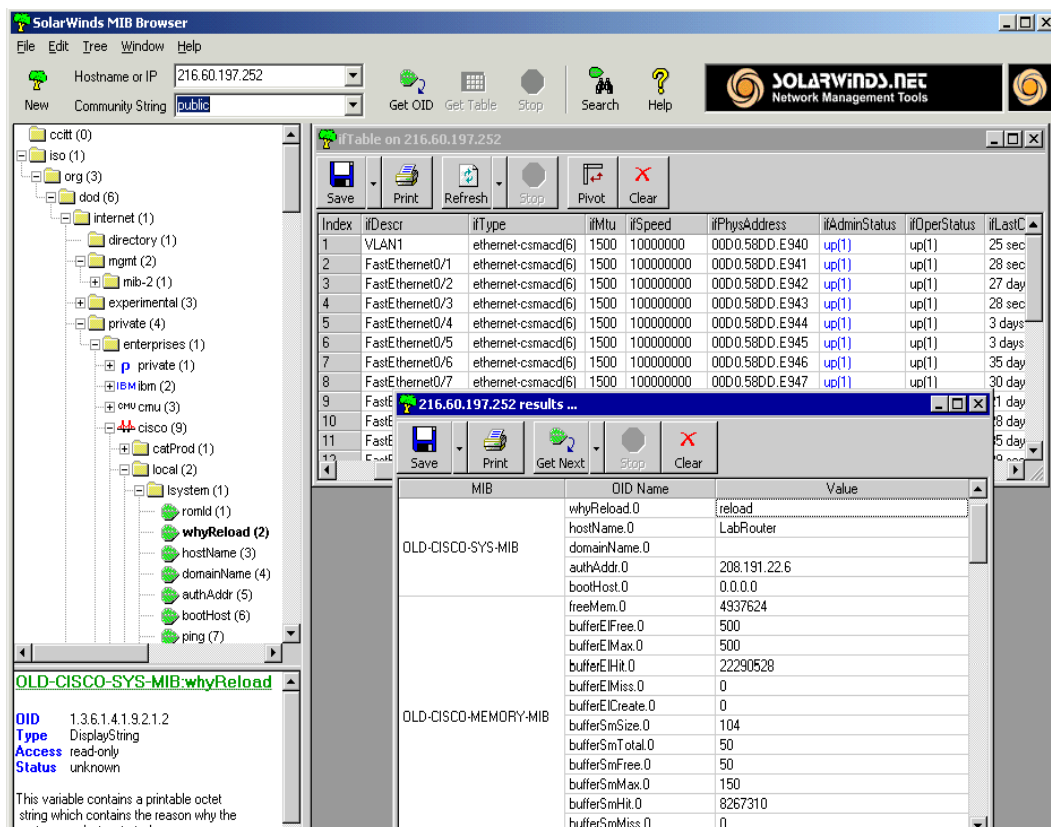


Gráfico 54. Buscador MIB

#### 6.1.5.5.2 MIB Viewer (Vista MIB)

Usa SolarWinds la base de datos de MIB extensa para desplegar cualquier OID o Tablas. Tiene el mismo rendimiento como el Navegador de MIB, pero es un método más rápido de recuperar los MIBs usados mas frecuentemente. Su uso es muy fácil tiene el API de Programador poderoso. El MIB Viewer normalmente es llamado programática mente por otras herramientas de SolarWinds.

| Index | ifIndex | ifDescr   | ifType                     | ifMtu | ifSpeed  | ifPhysAddress  | ifAdminStatus | ifOperStatus | ifLastChange        |
|-------|---------|-----------|----------------------------|-------|----------|----------------|---------------|--------------|---------------------|
| 1     | 1       | Ethernet0 | ethernet-csmacd(6)         | 1500  | 10000000 | 00E0.F71A.1CA1 | up(1)         | up(1)        | 6 seconds           |
| 2     | 2       | Ethernet1 | ethernet-csmacd(6)         | 1500  | 10000000 | 00E0.F71A.1CA4 | up(1)         | up(1)        | 7 seconds           |
| 3     | 3       | Ethernet2 | ethernet-csmacd(6)         | 1500  | 10000000 | 00E0.F71A.1CA7 | up(1)         | up(1)        | 7 seconds           |
| 4     | 4       | Ethernet3 | ethernet-csmacd(6)         | 1500  | 10000000 | 00E0.F71A.1CAA | up(1)         | up(1)        | 3 days, 21 hours, 2 |
| 5     | 5       | Ethernet4 | ethernet-csmacd(6)         | 1500  | 10000000 | 00E0.F71A.1CAD | up(1)         | down(2)      | 6 seconds           |
| 6     | 6       | Ethernet5 | ethernet-csmacd(6)         | 1500  | 10000000 | 00E0.F71A.1CB0 | up(1)         | up(1)        | 7 seconds           |
| 7     | 7       | Serial0   | propPointToPointSerial(22) | 1500  | 1544000  |                | down(2)       | down(2)      | 6 seconds           |
| 8     | 8       | Serial1   | propPointToPointSerial(22) | 1500  | 1544000  |                | down(2)       | down(2)      | 6 seconds           |
| 9     | 9       | Serial2   | propPointToPointSerial(22) | 1500  | 1544000  |                | down(2)       | down(2)      | 6 seconds           |
| 10    | 10      | Serial3   | propPointToPointSerial(22) | 1500  | 1544000  |                | down(2)       | down(2)      | 6 seconds           |

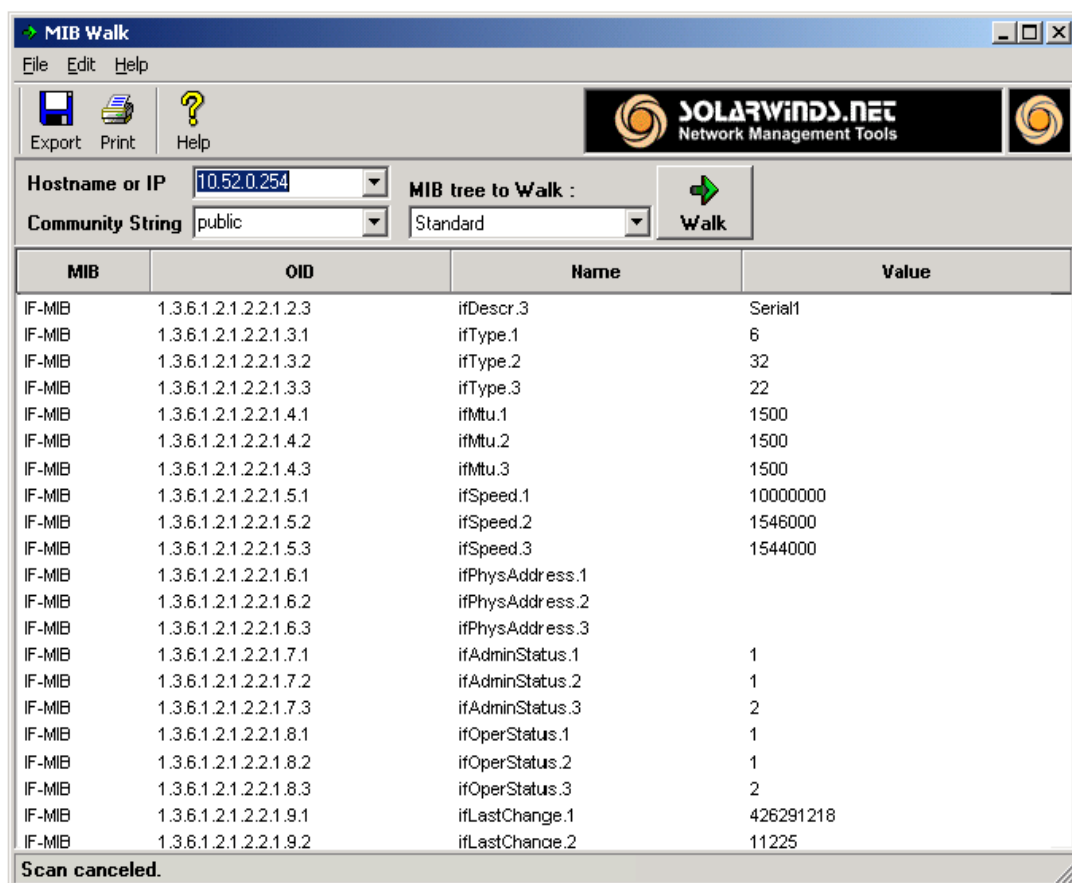
**MIB** RFC1213-MIB  
**Name** ifIndex.1  
 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifIndex.1  
**OID** 1.3.6.1.2.1.2.2.1.1  
**Type** INTEGER  
**Access** read-only  
**Status** unknown  
**Value** Please Wait ...

A unique value for each interface. Its value ranges between 1 and the value of ifNumber. The

**Gráfico 55. Vista MIB**

#### 6.1.5.5.3 MIB Walk (Camino MIB)

Esta utilidad obligara a los dispositivos SNMP a refugiarse en un árbol y descargar el valor de cada OID. Esta herramienta normalmente usa y encuentra que MIBs y OID son apoyadas en un dispositivo particular. MIB Walk proporcionara una lista completa de todos MIBs y OID e informa el estado actual para cada OID. Además usa la base de datos extensa de información de MIB para determinar el nombre inglés para cada OID y el MIB al que pertenece. No sólo reconoce MIBs de Cisco, HP, SUN y BAY SINO TAMBIEN MIBs privados.



| MIB    | OID                   | Name            | Value     |
|--------|-----------------------|-----------------|-----------|
| IF-MIB | 1.3.6.1.2.1.2.2.1.2.3 | ifDescr.3       | Serial1   |
| IF-MIB | 1.3.6.1.2.1.2.2.1.3.1 | ifType.1        | 6         |
| IF-MIB | 1.3.6.1.2.1.2.2.1.3.2 | ifType.2        | 32        |
| IF-MIB | 1.3.6.1.2.1.2.2.1.3.3 | ifType.3        | 22        |
| IF-MIB | 1.3.6.1.2.1.2.2.1.4.1 | ifMtu.1         | 1500      |
| IF-MIB | 1.3.6.1.2.1.2.2.1.4.2 | ifMtu.2         | 1500      |
| IF-MIB | 1.3.6.1.2.1.2.2.1.4.3 | ifMtu.3         | 1500      |
| IF-MIB | 1.3.6.1.2.1.2.2.1.5.1 | ifSpeed.1       | 10000000  |
| IF-MIB | 1.3.6.1.2.1.2.2.1.5.2 | ifSpeed.2       | 1546000   |
| IF-MIB | 1.3.6.1.2.1.2.2.1.5.3 | ifSpeed.3       | 1544000   |
| IF-MIB | 1.3.6.1.2.1.2.2.1.6.1 | ifPhysAddress.1 |           |
| IF-MIB | 1.3.6.1.2.1.2.2.1.6.2 | ifPhysAddress.2 |           |
| IF-MIB | 1.3.6.1.2.1.2.2.1.6.3 | ifPhysAddress.3 |           |
| IF-MIB | 1.3.6.1.2.1.2.2.1.7.1 | ifAdminStatus.1 | 1         |
| IF-MIB | 1.3.6.1.2.1.2.2.1.7.2 | ifAdminStatus.2 | 1         |
| IF-MIB | 1.3.6.1.2.1.2.2.1.7.3 | ifAdminStatus.3 | 2         |
| IF-MIB | 1.3.6.1.2.1.2.2.1.8.1 | ifOperStatus.1  | 1         |
| IF-MIB | 1.3.6.1.2.1.2.2.1.8.2 | ifOperStatus.2  | 1         |
| IF-MIB | 1.3.6.1.2.1.2.2.1.8.3 | ifOperStatus.3  | 2         |
| IF-MIB | 1.3.6.1.2.1.2.2.1.9.1 | ifLastChange.1  | 426291218 |
| IF-MIB | 1.3.6.1.2.1.2.2.1.9.2 | ifLastChange.2  | 11225     |

Scan canceled.

**Gráfico 56. Camino MIB**

#### 6.1.5.5.4 Update System MIB's (Actualización de Sistemas MIB)

La utilidad de MIB es una herramienta rápida y simple que permite ver, actualizar y publicar los cambios a la descripción del usuario para cualquier dispositivo del SNMP. Los cambios son: El Nombre del sistema, Localización, Contacto, etc. Simplemente ingresar la dirección IP y la cadena correspondiente y hacer clic en Retrieve Details.

Esta utilidad es usada normalmente para poner la información del sistema sobre las impresoras de la red (incluyendo las tarjetas), hubs, terminales, y servidores.

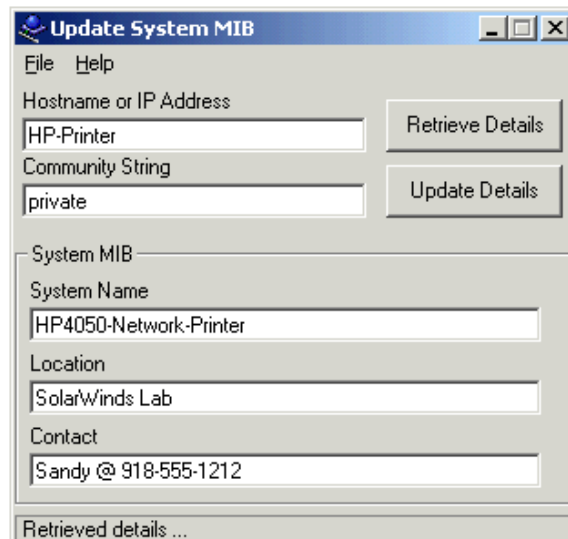


**Gráfico 57. Actualización MIB**

#### **6.1.5.6 Security And Attack Tools (Herramientas de Seguridad y Ataque)**

Solarwinds ofrece una colección de herramientas de seguridad y aplicaciones que permiten probar y validar la seguridad de la red. Se pueden usar estas herramientas combinadas con la Red de IP Browser para realizar su propia auditoria de seguridad. El Router Security Check es ideal para evaluar la seguridad de los IO actuales del router.

##### **6.1.5.6.1 SNMP Brute Force Attack (Ataque SNMP)**

Atacara una dirección IP con SNMP consultas y determinara si la comunidad SNMP es de solo lectura o lectura escritura, hace esto probando cada posible comunidad.

Se puede especificar caracteres para construir palabras con una longitud máxima de la cadena de la comunidad.

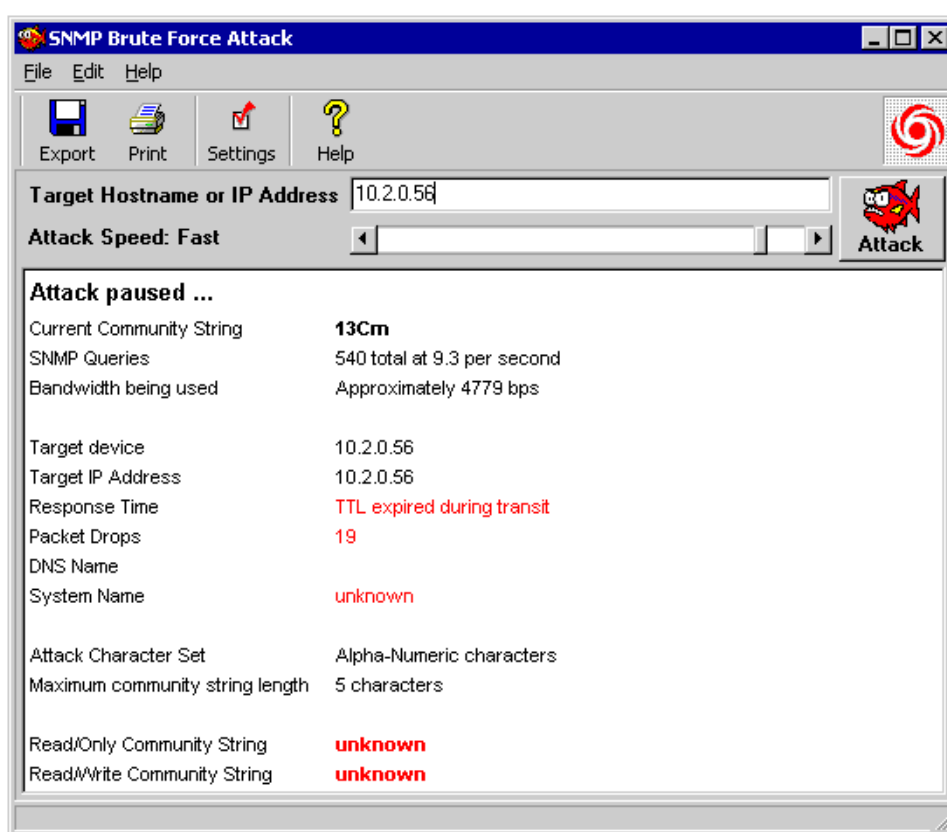


Gráfico 58. Ataque SNMP

#### 6.1.5.6.2 SNMP Dictionary Attack (Ataque Diccionario SNMP)

Usa el diccionario de las computadoras para atacar dispositivos de la red en un esfuerzo por irrumpir en ellos o descubrir sus cadenas de comunidad. **SNMP Brute**

**Force Attack** fue escrito para permitir crear en un ambiente controlado, un ataque en la seguridad de la red.

Esta aplicación no sólo atacará agresivamente los dispositivos de la red pero permitirán importar y permutar sus propios diccionarios en el módulo del ataque.

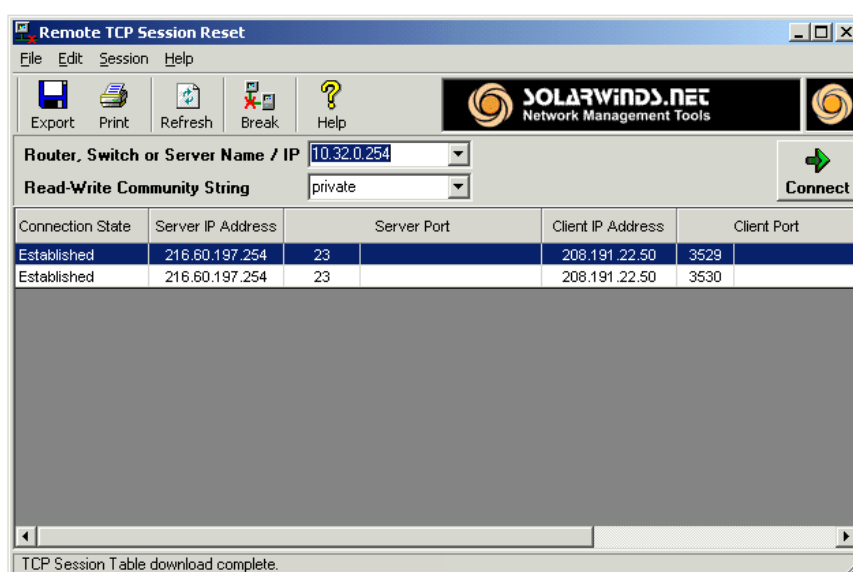


**Gráfico 59. Ataque Diccionario SNMP**

#### **6.1.5.6.3 Remote TCP Reset (Reseteo TCP Remoto)**

Esta herramienta de seguridad puede desplegar todas las sesiones activas remotamente en un servidor terminal, Router, dial-en servidor, servidor de acceso, etc. También puede restablecer fácilmente y remotamente cualquier sesión de TCP, este puede ser un Router, Servidor, Nodo de acceso, dial-a el servidor, el etc. Cualquier dispositivo que apoya SNMP.



| IP Address    | Complete                            | Word Count / Results | DNS                            | Sysname                   | Community | Response Time     |
|---------------|-------------------------------------|----------------------|--------------------------------|---------------------------|-----------|-------------------|
| 10.252.1.120  | <input type="checkbox"/>            | 2300 words           |                                |                           |           | 109 milliseconds  |
| 10.252.1.127  | <input checked="" type="checkbox"/> | Complete             | ch.llab.org                    | Chinese base NT           | @#SDH     | 246 milliseconds  |
| 10.252.1.130  | <input checked="" type="checkbox"/> | No response          | frog.llab.org                  |                           |           | Request Timed Out |
| 10.252.3.7    | <input checked="" type="checkbox"/> | Complete             | msns.llab.org                  | MSNS                      | public    | 50 milliseconds   |
| 10.252.3.67   | <input type="checkbox"/>            | 4523 words           | mscp.llab.org                  | MSCP                      |           | 63 milliseconds   |
| 10.252.3.134  | <input checked="" type="checkbox"/> | Complete             | cid.llab.org                   | CID                       | public    | 57 milliseconds   |
| 10.252.3.249  | <input type="checkbox"/>            | 4562 words           | msw.llab.org                   | MSSW                      |           | 36 milliseconds   |
| 10.252.5.43   | <input checked="" type="checkbox"/> | Complete             | orc.llab.org                   | ORC                       | public    | 35 milliseconds   |
| 10.252.5.112  | <input checked="" type="checkbox"/> | Complete             | german-2000.llab.org           | German 2000 Test          | warped    | 50 milliseconds   |
| 10.252.5.118  | <input checked="" type="checkbox"/> | Complete             | nir.llab.org                   | MIR                       | public    | 40 milliseconds   |
| 10.252.5.121  | <input checked="" type="checkbox"/> | Complete             | german.llab.org                | German base NT            | warped    | 38 milliseconds   |
| 10.252.5.122  | <input checked="" type="checkbox"/> | Complete             | tinnet-qwes.llab.org           | TRINET Customer           | tinnet2   | 81 milliseconds   |
| 10.252.5.129  | <input checked="" type="checkbox"/> | Complete             | arch.llab.org                  | ARCH 2000                 | public    | 97 milliseconds   |
| 10.252.5.132  | <input checked="" type="checkbox"/> | Complete             | socwork.llab.org               | SDCWORK                   | private   | 53 milliseconds   |
| 10.252.5.142  | <input type="checkbox"/>            | 4562 words           | cf.llab.org                    | CF NT                     |           | 39 milliseconds   |
| 10.252.5.144  | <input checked="" type="checkbox"/> | Complete             | french-95.llab.org             | French 95 Test            | warped    | 40 milliseconds   |
| 10.252.5.171  | <input checked="" type="checkbox"/> | Complete             | english-2000.llab.org          | German 2000 Test          | warped    | 52 milliseconds   |
| 10.252.5.173  | <input checked="" type="checkbox"/> | Complete             | russian.llab.org               | Russian base NT           | warped    | 42 milliseconds   |
| 10.252.5.204  | <input type="checkbox"/>            |                      | orient.llab.org                |                           |           |                   |
| 10.60.197.2   | <input checked="" type="checkbox"/> | 4566 words           |                                |                           |           | 5 milliseconds    |
| 10.60.197.3   | <input checked="" type="checkbox"/> | Complete             | Traffic-4 Com                  | Traffic Generator         | public    | 1 milliseconds    |
| 10.60.197.200 | <input type="checkbox"/>            | 4560 words           | Gateway TestLab.SolarWinds...  | TestLab Cisco 7500        | swtlab    | 1 milliseconds    |
| 10.60.197.204 | <input checked="" type="checkbox"/> | Complete             | Remote TestLab.SolarWinds...   | TestLab Remote Cisco 3... | hidden    | 350 milliseconds  |
| 10.60.197.217 | <input checked="" type="checkbox"/> | Complete             | Server1 TestLab.SolarWinds...  | NT Server 1               | swtlab    | 362 milliseconds  |
| 10.60.197.218 | <input checked="" type="checkbox"/> | Complete             | Server2 TestLab.SolarWinds...  | NT Server 2               | swtlab    | 361 milliseconds  |
| 10.60.197.220 | <input type="checkbox"/>            | 1350 words           | Development TestLab.SolarWi... | NT Development            |           | 1 milliseconds    |
| 10.60.197.245 | <input checked="" type="checkbox"/> | No response          | DAVE'S                         |                           |           | Request Timed Out |
| 10.60.197.250 | <input checked="" type="checkbox"/> | No response          |                                |                           |           | Request Timed Out |
| 10.60.197.251 | <input checked="" type="checkbox"/> | 1350 words           | SNMP/Warp TestLab.SolarWi...   | SNMP Warp                 | bogus     | 1 milliseconds    |
| 10.60.197.252 | <input checked="" type="checkbox"/> | Complete             | nt3.llab.org                   | NT 3                      | swtlab    | Request Timed Out |
| 10.60.197.253 | <input checked="" type="checkbox"/> | Complete             | nt4.llab.org                   | NT 4                      | swtlab    | 1 milliseconds    |
| 10.60.197.254 | <input checked="" type="checkbox"/> | Complete             | french-2000.llab.org           | French 2000 Test          | warped    | 3 milliseconds    |

**Gráfico 60. Reseteo TCP Remoto**

#### 6.1.5.7 Ping And Diagnostic Tools (Herramientas para Diagnostico y Ping )

Manejar cualquier dato complejo conectado a una red de computadoras y teniendo una colección de Ping y herramientas de diagnóstico es un requisito.

Las herramientas son:

##### 6.1.5.7.1 Trace Route (Router Ruta)

La Ruta del Rastro de SolarWinds es la ruta del rastro más rápida en el internet. Esta utilidad puede rastrear una ruta rápidamente de su computadora a cualquier otro dispositivo. La Ruta del rastro no sólo despliega el tiempo de la contestación por cada nodo pero resoluciones el DNS en tiempo real. Reporta la información de ICMP normal pero también la información de SNMP como: el Tipo de la Máquina, ISO Level, boot time, etc. en tiempo real.

| Hop | IP              | DNS                        | Current Response Time | Average Response Time | Packet Loss | Machine Type | IOS Image    | IOS Version | Last Boot |
|-----|-----------------|----------------------------|-----------------------|-----------------------|-------------|--------------|--------------|-------------|-----------|
| 1   | 208.191.22.62   |                            | 0 ms                  | 0 ms                  | 0 %         | Cisco 4500   | C4500-DS40-M | 11.2(2)     | 2/3/2001  |
| 2   | 216.60.197.254  |                            | 0 ms                  | 0 ms                  | 0 %         | Cisco 2501   | C2500-IO-L   | 11.2(18)P   | 3/5/2001  |
| 3   | 151.164.68.21   |                            | 20 ms                 | 9 ms                  | 0 %         | Cisco 7513   | RSP-K4PV-M   | 12.0(11)S3  | 12/4/2000 |
| 4   | 151.164.67.241  | edge1-fa6-1-0.tulsok.sw... | 0 ms                  | 22 ms                 | 0 %         | Cisco 7507   | RSP-PV-M     | 12.0(6)S    | 8/10/2000 |
| 5   | 151.142.220.221 | tulsok1wct1.sbc-tulsa.5... | 20 ms                 | 43 ms                 | 0 %         | Cisco 7513   | RSP-PV-M     | 11.1(25)CC  | 2/23/2001 |
| 6   | 151.142.221.81  |                            | 10 ms                 | 11 ms                 | 0 %         | Cisco 12008  | GSR-P-M      | 12.0(5)S    | 12/6/1999 |
| 7   | 64.200.240.254  | chcgil1wvx2-oc12.ipcc....  | 20 ms                 | 26 ms                 | 0 %         |              |              |             |           |
| 8   | 64.200.233.62   | chcgil1wvx3-oc48.ipcc....  | 20 ms                 | 28 ms                 | 0 %         |              |              |             |           |
| 9   | 157.130.117.109 | 34.ATM3-0.GW1.CH12.A...    | 30 ms                 | 35 ms                 | 0 %         |              |              |             |           |
| 10  | 152.63.64.130   | 161.at-5-0-0.XR1.CH12.A... | 80 ms                 | 77 ms                 | 0 %         |              |              |             |           |
| 11  | 152.63.67.130   | 0.so-7-0-0.XR1.CH12.AL...  | 70 ms                 | 78 ms                 | 0 %         |              |              |             |           |
| 12  | 152.63.15.86    | 0.so-3-0-0.TR1.CH12.AL...  | 60 ms                 | 76 ms                 | 0 %         |              |              |             |           |
| 13  | 152.63.1.90     | 126.at-5-1-0.TR1.NYC8...   | 90 ms                 | 100 ms                | 10 %        |              |              |             |           |
| 14  | 152.63.21.25    | 185.ATM6-0.XR1.NYC1....    | 100 ms                | 108 ms                | 0 %         |              |              |             |           |
| 15  | 152.63.20.5     | 195.ATM5-0.GW8.NYC1....    | 91 ms                 | 99 ms                 | 0 %         |              |              |             |           |
| 16  | 157.130.60.250  | dante-nyc1-gw.custome...   | 90 ms                 | 95 ms                 | 0 %         |              |              |             |           |
| 17  | 212.1.200.26    | ny-mi.garr.net             | 150 ms                | 157 ms                | 0 %         |              |              |             |           |
| 18  | 193.206.134.2   | bo-mi-1.garr.net           | 160 ms                | 163 ms                | 0 %         | Cisco 7507   | RSP-PV-M     | 12.0(10)S1  | 1/29/2001 |
| 19  | 193.206.134.94  | fi-bo-2.garr.net           | 160 ms                | 167 ms                | 0 %         | Cisco 7507   | RSP-PV-M     | 12.0(10)S1  | 8/2/2000  |
| 20  | 193.206.136.66  | cnrf1-rc.fi.garr.net       | 160 ms                | 164 ms                | 0 %         |              |              |             |           |
| 21  | 149.139.229.2   |                            | 170 ms                | 180 ms                | 0 %         | Cisco 4000   | C4000-D-M    | 12.0(10)    | 8/31/2000 |
| 22  | 149.139.13.77   | castor.iue.it              | 170 ms                | 173 ms                | 0 %         | HP 9000/700  |              |             | 7/28/2000 |

**Gráfico 61. Pantalla Ruta del Router**

#### 6.1.5.7.2 TFTP Server (Trivial File Transfer Protocol , Servidor Versión FTP)

El Servidor de TFTP mientras haya muchos Servidores de TFTP disponibles, podemos trabajar en un proyecto de auditoria de red grande y necesitamos un Multi – Threaded Servidor de TFTP que podría ocuparse de la transferencia de muchos archivos simultáneamente. Además no podríamos encontrar uno que sea fiable.

El SolarWinds TFTP Servidor tiene la habilidad para enviar y recibir los archivos múltiples concurrentemente. Este Servidor de TFTP normalmente se usa para upload/download las imágenes ejecutables y configuraciones de los routers, Switches, hubs, Terminales, etc.

#### 6.1.5.7.3 Wake – On-LAN (Encender en LAN)

Esta utilidad tiene la habilidad de encender remotamente un PC. Cuando el adaptador de la red remoto oye que un Paquete creado para él es único, la MAC se dirige al adaptador de la red y alerta a la computadora del encendido. Si **Wake – On-LAN** fue habilitado en la configuración del BIOS de la computadora, el sistema enciende como si el botón de encendido hubiera sido presionado.



Gráfico 62. Encendido LAN

#### 6.1.5.7.4 PING

La versión de SolarWinds es el PING Simple esta herramienta guarda la respuesta y permite exportar a HTML, RTF y archivos de Texto. Este PING gráfico muestra lo siguiente continuamente:

- El tiempo de la contestación actual
- El tiempo medio de la contestación corriente en milisegundos (ms)

- La Pérdida del Paquete actual debido a los paquetes dejados caer

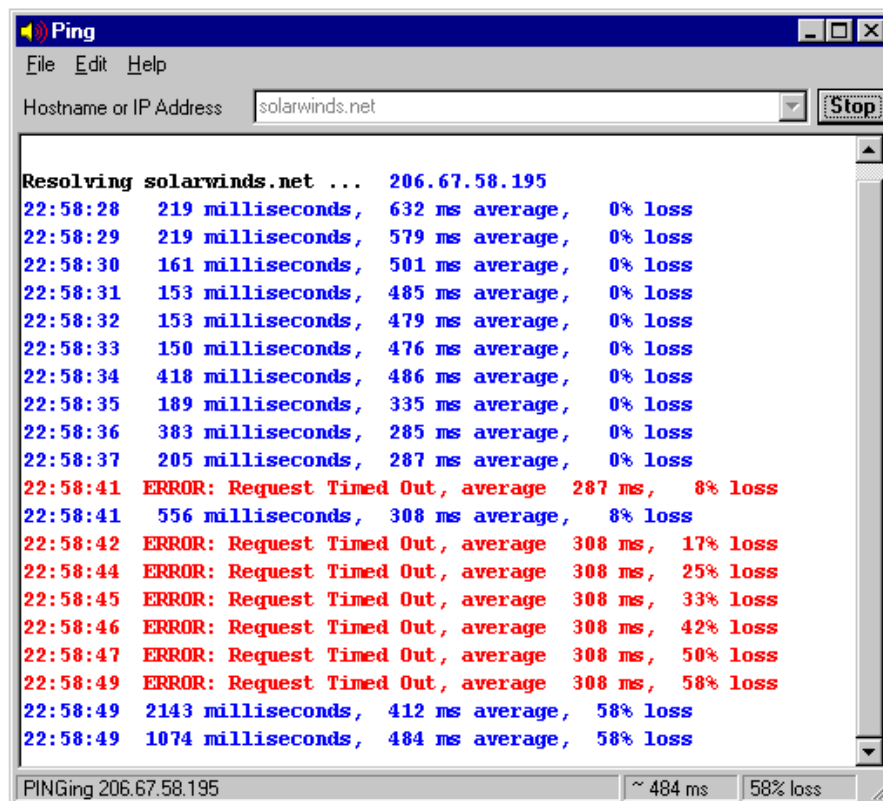


Gráfico 63. Ping

#### 6.1.5.7.5 WAN Killer (Asesino LAN)

Esta utilidad no es un Asesino, es más de un Área Ancha generadora de tráfico de red. Se debe poner el bandwidth del circuito y el porcentaje de carga necesarios y el WAN Killer generará el tráfico aleatorio. Con el WAN Killer se puede especificar la cantidad de carga que se desee, 25% 50% 100% o incluso 150%. Además probará la conexión interactivamente y ajustará el tráfico generado para lograr la carga deseada basada en sus requisitos.

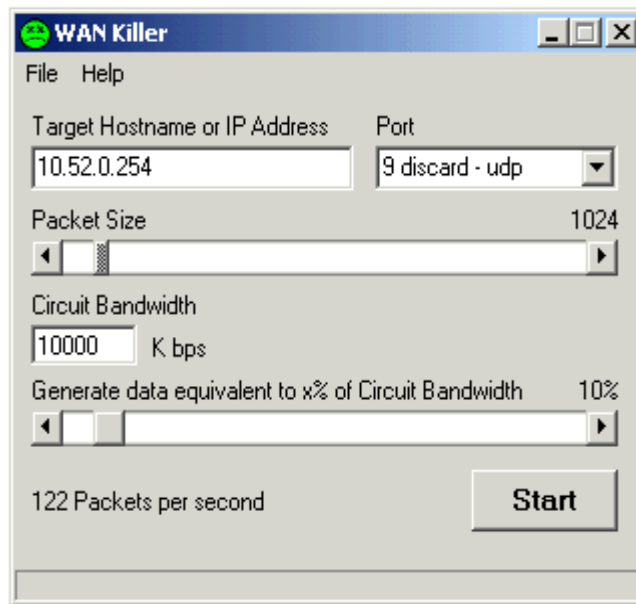


**Gráfico 64. Asesino LAN**

#### **6.1.5.8 IP Address Management Tools (Herramientas de Gestión de Direcciones)**

Esta herramienta fue diseñada para ayudar a manejar el espacio de direcciones IP en un día. Puede emitir finalmente hojas de cálculo y listas en papel para saber qué usuarios están en la subred.

##### **6.1.5.8.1 IP Address Management (Gestión de Dirección IP)**

Es muy fácil de usar ya que automáticamente determina qué direcciones de IP no están en uso y cuánto tiempo ha sido desde que ellas se han usado. Esta herramienta también apoya SNMP durante su descubrimiento de la red.

SolarWinds ayuda a organizar los datos del ancho de banda y conectar una red de computadoras con sus respectivas direcciones IP.

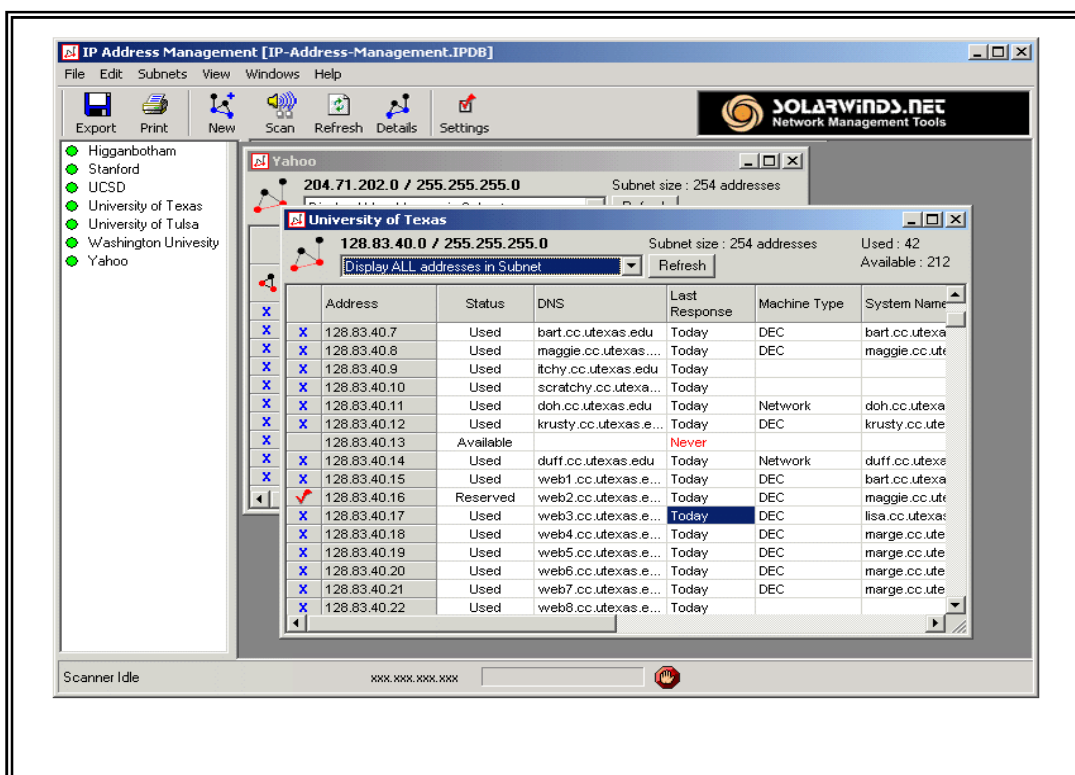


Gráfico 65. Gestión de Direcciones IP

#### 6.1.5.8.2 DHCP Scope Monitor (Monitor DHCP)

El DHCP (Protocolo Anfitrión de la Configuración Dinámico) El Scope Monitor monitoreará y supervisará los Alcances de DHCP y mostrará que alcances son bajos en las direcciones. Despliega el número asignado dinámicamente de Dirección IP para cada alcance.

| DHCP Scope           | Scope Name            | Size | Leased | Available | Server    |                               |
|----------------------|-----------------------|------|--------|-----------|-----------|-------------------------------|
| 10.131.22.64         | Austin WAN Lab        | 35   | 4      | 31        | SW-SERVER | Last poll at 11/10/2000 12:57 |
| <b>10.123.22.128</b> | <b>Office Network</b> | 31   | 30     | <b>1</b>  | SW-SERVER | Last poll at 11/10/2000 12:57 |
| 10.65.197.0          | Dallas Lab            | 31   | 1      | 30        | SW-SERVER | Last poll at 11/10/2000 12:57 |
| 10.71.122.0          | Austin NOC            | 44   | 17     | 27        | SW-SERVER | Last poll at 11/10/2000 12:57 |
| 10.37.72.128         | Austin Development    | 35   | 4      | 31        | SW-SERVER | Last poll at 11/10/2000 12:57 |
| <b>10.83.2.128</b>   | <b>Boston Support</b> | 23   | 19     | <b>4</b>  | SW-SERVER | Last poll at 11/10/2000 12:57 |
| 10.58.83.64          | London Sales Office   | 31   | 4      | 27        | SW-SERVER | Last poll at 11/10/2000 12:57 |
| 10.16.33.0           | Singapore Sales       | 29   | 6      | 23        | SW-SERVER | Last poll at 11/10/2000 12:57 |
| <b>10.113.25.128</b> | <b>Boston Sales</b>   | 25   | 22     | <b>3</b>  | SW-SERVER | Last poll at 11/10/2000 12:57 |
| 10.25.82.0           | Tulsa Development     | 30   | 7      | 23        | SW-SERVER | Last poll at 11/10/2000 12:57 |
| 10.25.55.0           | Tulsa Sales Office    | 27   | 6      | 21        | SW-SERVER | Last poll at 11/10/2000 12:57 |

Copied selection to Windows clipboard.

**Gráfico 66. Monitor DHCP**

#### 6.1.5.8.3 Advanced Subnet Calculador (Calculador de Sub Red Avanzado)

Este Subnet Calculador emite y resuelve la dirección inversa del DNS. Calcula subredes basadas en Mascaras de red, Máscaras de Bits, Host Bits, Número de Subredes y Host por cada Subred.

**Advanced Subnet Calculator**

File Edit Skins Help

Export Print ? Help

SOLARWINDS.NET  
Network Management Tools

Address Details Classful Subnet Calculator CIDR Calculator Subnet Addresses

IP Address: 66.218.71.89 ✓ Lookup Hostname

Hostname: www.yahoo.com ✓ Lookup IP Address

Response Time: 60 milliseconds

Hex: 66.218.71.89 = 42.DA.47.59

Binary: 66.218.71.89 = 01000010.11011010.01000111.01011001

Address Class Info: **Class A address (1.0.0.0 - 126.255.255.255)**

Address: Yahoo! (NETBLK-A-YAHOO-U23)

Owner / Info: 701 First Avenue  
Sunnyvale, California 94089  
US  
Netname: A-YAHOO-U23  
Netblock: 66.218.64.0 - 66.218.79.255  
Maintainer: YAOO  
Coordinator: Admin, Netblock (NA258-ARIN) netblockadmin@yahoo-inc.com

**Gráfico 67. Calculador Sub Red Avanzado**

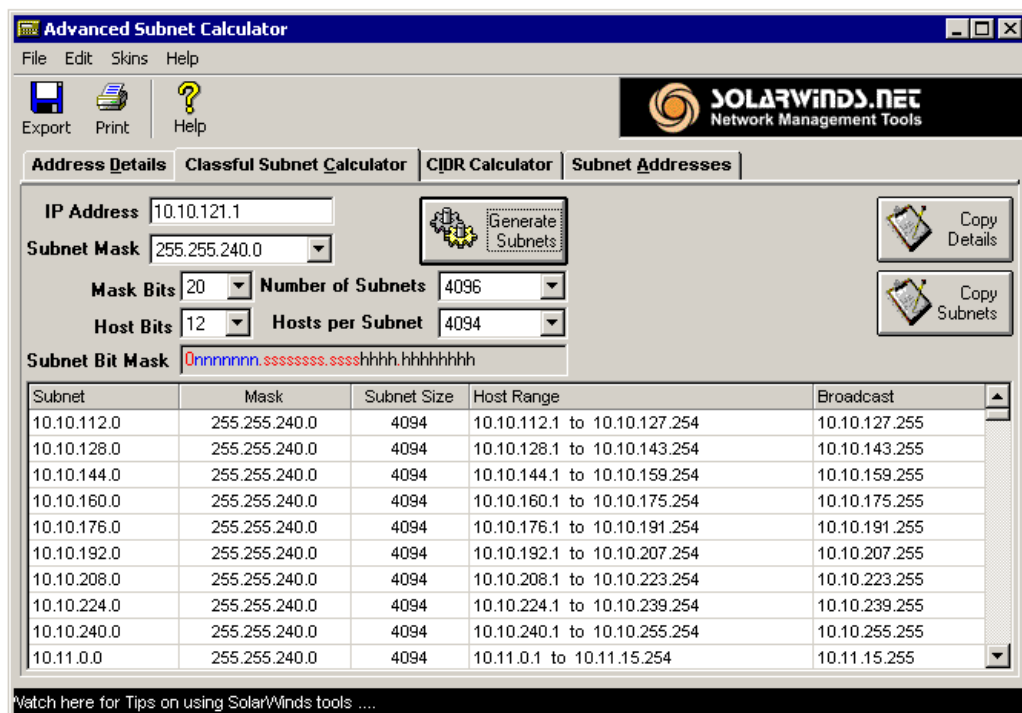


**Gráfico 68. Calculador Sub red Avanzado y Clasificado**

#### **6.1.5.8.4 DNS Audit. (Auditoria DNS)**

Como las redes crecen, guardar cada dirección IP asignada y el nombre del Dominio es una tarea desalentadora. DNS Audit no sólo inventaría sus direcciones IP sino también valida la resolución correcta de los Nombres del Dominio.

#### **6.1.5.8.5 DNS/ Who Is Resolver (Cómo Resolver DNS)**

DNS Resolver busca y crea un informe detallado en el Nombre del Dominio, URL, IP Address, Dirección de la Red o Dirección del correo electrónico. Incluso puede definir su propio quién es el servidor.

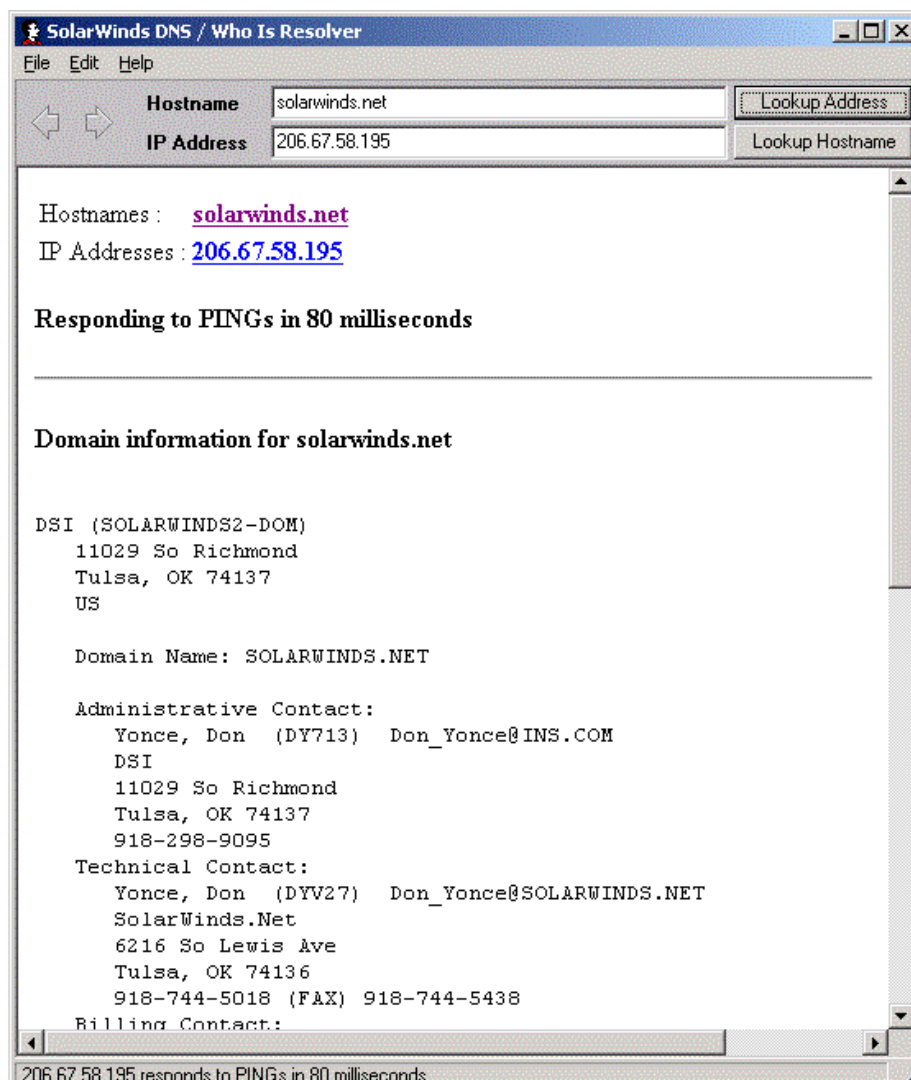


**Gráfico 69. Cómo resolver DNS**

#### **6.1.5.9 Miscellaneous Tools (Herramientas Misceláneas)**

Son un par de herramientas que no han sido incluidas en el Solarwinds Engineer; pues, no entran en una categoría específica y se han etiquetado como misceláneas.

Estas son:

#### 6.1.5.9.1 TFTP Server (Servidor TFTP)

El Servidor de TFTP tiene la habilidad para enviar y recibir archivos múltiples concurrentemente. También tiene un filtro de seguridad muy hábil y pantalla de mando para limitar acceso a este Servidor de TFTP.

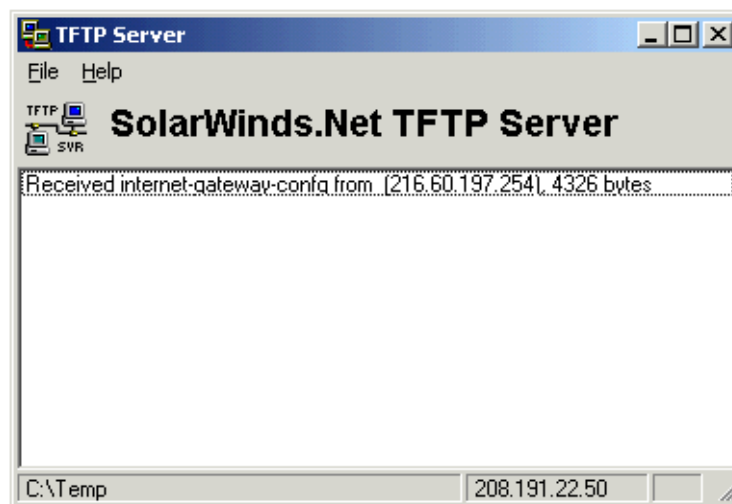


**Gráfico 70. Servidor TFTP**

#### 6.1.5.9.2 Update System MIB's (Actualización de Sistemas MIB)

La utilidad de MIB es una herramienta rápida y simple que lo permite ver, poner al día y publicar cambios en los campos de Descripción del Usuario para cualquier dispositivo de SNMP.

Estos cambios son: Nombre del sistema, Localización, Contacto, etc. Simplemente se debe ingresar la dirección IP y la cadena de comunidad correspondiente y pulsar el botón Recupere Detalles.

## **6.2 PATROL DASHBOARD**

### **6.2.1 Introducción**

Los encargados de las redes están buscando las herramientas que les ayuden a entender cómo la red efectúa su funcionamiento, el tiempo de reacción del usuario final del correlativo a los embotellamientos de la red, evaluar inversiones de la red del ancho-área (WAN) y asistir con planeamientos de capacidad y de red.

Patrol Dashboard maneja los dispositivos en una red, y realiza varias funciones, incluyendo recoger estadísticas del SNMP, almacenar la información en su base de datos, y generar informes sobre los dispositivos de los cuales es responsable.

Patrol Dashboard se ha diseñado con un Web-based, una arquitectura del servidor de cliente y aplicaciones en su propia base de datos del objeto, diseñada especialmente para asegurar disponibilidad óptima y compatibilidad. En redes grandes, varios módulos Patrol Dashboard se combinan bajo control de un módulo corporativo del tablero.

### **6.2.2 Arquitectura**

El servidor del Patrol dashboard fue desarrollado en Java y se puede utilizar con diversas plataformas, tales como:

- NT de Microsoft Windows,
- Windows 95/98,

- Windows 2000,
- Linux,
- Solaris,
- AIX y HP-UX.

El cliente de Patrol Dashboard es un browser del Web y puede ser utilizado con la versión 5 de Microsoft Internet Explorer o una versión más adelante.

Así, los usuarios de Patrol Dashboard pueden tener acceso a todas las funciones del producto a través de un browser de cualquier computadora.

Además, Patrol Dashboard puede exportar los datos recogidos en un depósito del CIM (modelo común de la información), que es una base de datos del óracle (véase el gráfico 71).

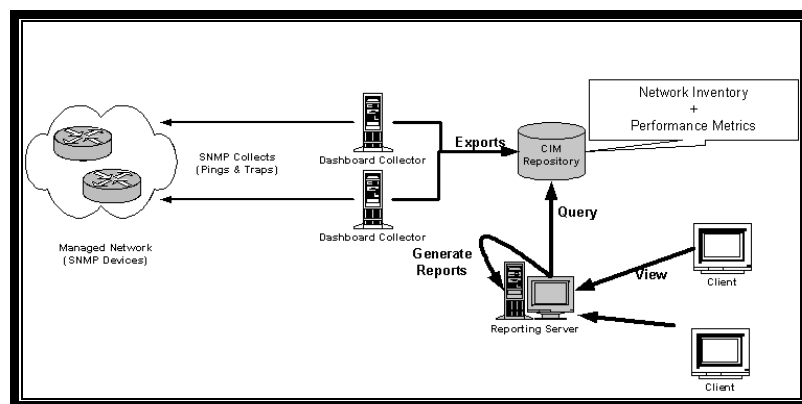


**Gráfico 71. SNMP Data Collect and Export to a CIM Repository**

### **6.2.3 Características Dominantes**

- PATROL DashBoard es un Web y un sistema de gerencia Java basado en el funcionamiento de la red que se instala en aproximadamente quince minutos. Permite proactivamente manejar la red y mejorar su calidad de servicio (QoS).
- PATROL DashBoard automáticamente descubrirá su red, fijará automáticamente umbrales y comenzará a recoger datos relevantes para permitir que usted localice problemas de la red.
- Este producto puede también anticipar pérdidas o caídas de funcionamiento y optimizar la eficacia total de la red.
- Proporciona una vuelta rápida en la inversión, proporcionando la operación inmediata usando el automático descubrimiento de la red y el ajuste automático de umbrales.
- Permite el acceso dinámico a todos los datos que usa un browser del Web.
- Distribuye la información útil recogiendo, almacenando y analizando los indicadores significativos.
- Integra seamlessly con las plataformas de la dirección de la red tales como HP OpenView y el CA Unicenter TNG(r) que usa una arquitectura de Web-browser
- Reduce esfuerzos al localizar averías usando la información útil de los e-mail en formato de informe HTML

- Permite que usted resuelva las necesidades de QoS de redes muy grandes usando una correlación automática y un diagnóstico.
- Permite que el acceso sea manejado en el perfil del individuo o del grupo.

#### 6.2.4 Conexión para un cliente Patrol Dashboard

1. De cualquier sistema operativo, lance un browser del Internet.
2. Incorpore el URL siguiente:
  - a) **http://HostName:HttpPort/patrol/dashboard**
  - b) **HostName** corresponde al nombre o IP address del servidor de PATROL DashBoard.
  - c) **HttpPort** corresponde al numero de puerto usado por el servidor PATROL DashBoard. El numero por defecto es 8000.
3. Para una conexión, incorpore su nombre del usuario, contraseña y clic en login in.

##### 6.2.4.1 Conexión para un servidor Patrol Dashboard

Usted necesitará parar el servidor de PATROL DashBoard bajo circunstancias siguientes:

- Si usted necesita cerrar la computadora en la cual el servidor de PATROL DashBoard reside.

- Si necesita la reserva la base de datos.
- Si necesita restaurar datos de una reserva.

### 6.2.5 Descripción de la Herramienta

Después de logearse en PATROL DashBoard, la siguiente pantalla que despliega es la que se muestra en el gráfico 72.

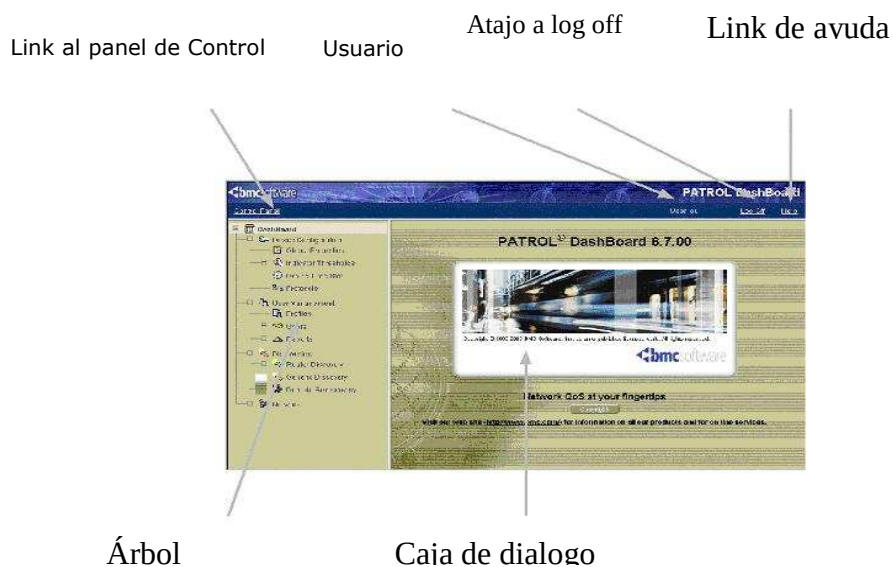


**Gráfico 72. Pantalla Principal PATROL Dashboard**

### 6.2.6 Estructura del Árbol

Este árbol se exhibe en la izquierda de la pantalla según lo demostrado abajo. Para la información sobre menús que tienen acceso en el árbol, vea las acciones.

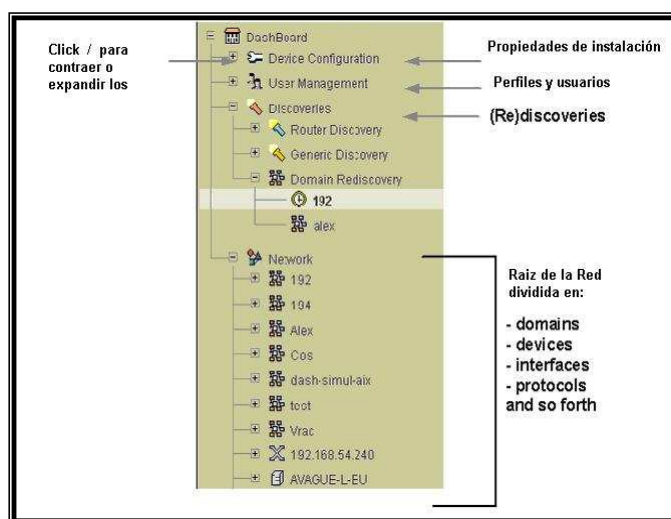


**Gráfico 73. Estructura del árbol**

La vista del dispositivo configuración y las partes de Discovery del árbol son del superusuario (SU). La vista depende del tipo de usuario y perfil.

|                                                         |                                                                                                                                                                                                             |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Configuration<br>(Configuración del Dispositivo) | Permite acceder a las características de configuración de Patrol Dashboard y a los parámetros globales del dispositivo                                                                                      |
| User Management<br>(Gestor de Usuario)                  | Maneja los perfiles de usuario, crea, modifica y suprime a usuarios (el de defecto es un solo usuario su con un perfil de superusuario) para asignar dominios e informes de la red a los usuarios           |
| Discoveries<br>(Descubrimientos)                        | Descubre y redescubre automáticamente los objetos de la red                                                                                                                                                 |
| Network<br>(Red)                                        | Accede a la configuración de red que usted desea manejar. Esta raíz se divide en los dominios, dispositivos, interfaces, sub-interfaces, tales como DLCIs, VPs, VCs, pares, protocolos y así sucesivamente. |

**Tabla 4. Descripción de componentes principales.**

### 6.2.7 PROPIEDADES GLOBALES

Esta ventana se utiliza para especificar las características globales del dispositivo. Puede seleccionar el tipo de dispositivo que desea configurar, estos están definidos en tablero de instrumentos de la PATROL, como se especifica abajo y se describen algunas de las más utilizadas.

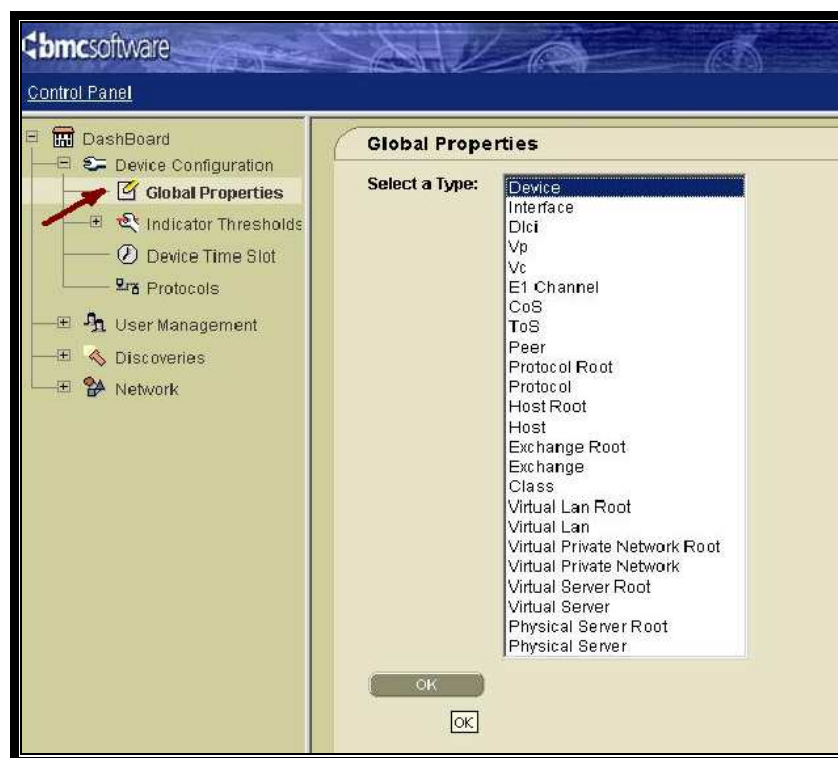


**Gráfico 74. Propiedades Globales (Global Properties)**

#### **6.2.7.1 Device (Dispositivo)**

Los device pueden ser de los siguientes tipos:

- hubs
- switches
- routers
- Servidores y clientes workstations que corren o distribuyen aplicaciones

Por razones de la seguridad, una contraseña, llamada Community Name, se requiere para tener acceso a un MIB y manejar el dispositivo.

De vez en cuando, un nombre de la comunidad se define para el acceso read-Only al dispositivo y otro nombre de la comunidad se define para las operaciones de read/write.

#### **6.2.7.2 Interface (Interface)**

Los dispositivos de la red se unen a los acoplamientos de la transmisión a través de las interfaces de diversos tipos.

Por ejemplo:

- Interfaces de la red de área local (conexiones de Ethernet)
- Interfaces de la red de área amplia
- Modo de transferencia Asynchronous y así sucesivamente.

#### **6.2.7.3 DLCI**

DLCI es un corto identificador de la conexión de transmisión de datos.

#### **6.2.7.4 VP (Path Virtual)**

VP es un pequeño path virtual. En una red ATM liga dos nodos vecinos.

#### **6.2.7.5 VC (Canal Virtual)**

VC es un corto canal virtual, que en una red ATM, es la conexión de intercambio par-a-par a las células. Entre dos nodos, un VP esta dividido en VCs. En una conexión par-a-par cruces VC en serie de VPs.

#### **6.2.7.6 E1 Channel (Canal)**

Un canal de transmisión digital europeo (línea arrendada) que lleva datos en un índice de 2.048 millones de bits por segundo y puede llevar 32 canales de 64 Kbps cada uno.

#### **6.2.7.7 CoS (Clase de Servicio)**

Clase del servicio. CoS es una manera de manejar tráfico en una red agrupando tipos de tráfico similares (por ejemplo, E-mail, vídeo que fluye, voz, transferencia de archivo grande de documento) juntos y tratando cada tipo como clase con su propio nivel de la prioridad del servicio.

#### **6.2.7.8 ToS (Tipo de Servicio)**

La ToS es un pequeño tipo de servicio. La característica ToS-Basada en NetFlow de la agregación de un router proporciona la capacidad de permitir la ToS de los datos de la exportación de NetFlow, que los resultados en los datos resumidos de la exportación de NetFlow que se exportarán a un dispositivo de la colección. Las routers Bintec soportan este tipo de características. La ToS es uno de los campos de un IP packet. Especifica la prioridad de este paquete según las políticas de QoS.

#### **6.2.7.9 Peer (Par)**

Un Peer es un par de dispositivos, de la fuente y de la destinación, que se utiliza para medir los tiempos de reacción entre estos dos dispositivos.

#### **6.2.7.10 Protocol Root (Raíz de protocolo)**

Un título con los artículos del protocolo abajo. Este concepto es exclusivo ya que miran Netflow solamente. Los protocolos debajo de tal raíz se unen a los interfaces físicas de prueba RMON2.

### **6.2.8 Propiedades del Dispositivo**

Esta ventana especifica las características globales de todos los dispositivos del tipo seleccionado, para la gráfica de un dispositivo.

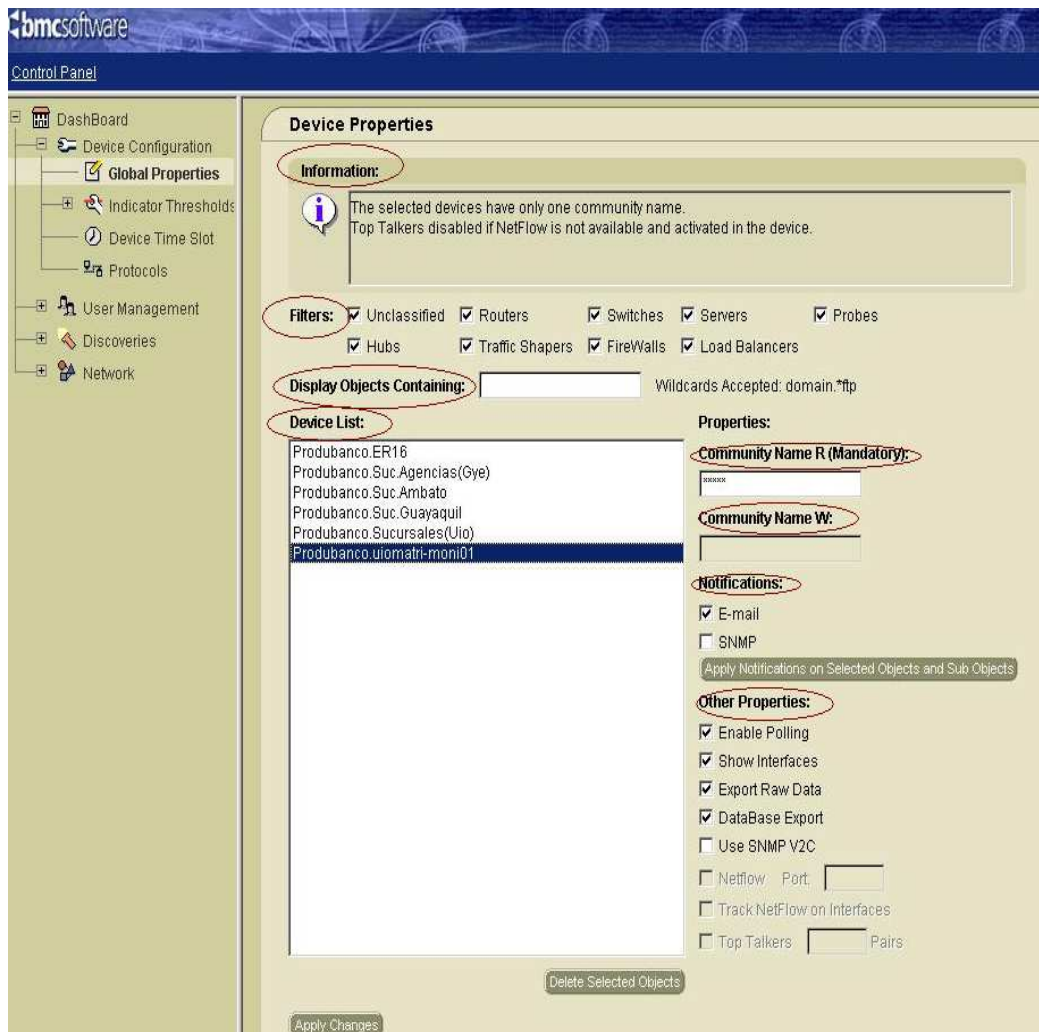


**Gráfico75. Propiedades globales de un dispositivo.**

|                             |                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device List                 | Lista de los dispositivos que encajan la selección.                                                                                                                                                                                                                                                                                       |
| Filters                     | Selecciona el tipo de dispositivo.                                                                                                                                                                                                                                                                                                        |
| Display Objects containing: | Escriba una cadena para seleccionar el o los tipos de objetos que desee.                                                                                                                                                                                                                                                                  |
| Community Name (R)          | Ingrese la contraseña que requieren para leer los datos SNMP de los dispositivos. Por omisión(defecto), esta contraseña es puesta para igualar el Nombre de Comunidad que es usado en discovery del dispositivo. Si este parámetro es modificado, una conexión al dispositivo es realizada para comprobar que el nuevo valor es correcto. |
| Community Name (W)          | Ingrese la contraseña que requieren si usted quiere modificar los datos SNMP de los dispositivos. Puede ser diferente del nombre de comunidad para lectura; para hacer una diferencia entre los derechos de tener acceso al dispositivo en solo modo de lectura y el modo escritura..                                                     |
| E-mail notifications        | Escoja esta opción para enviar una notificación cuando cruce el umbral.(e-mail)                                                                                                                                                                                                                                                           |
| SNMP notifications          | Escoja esta opción para enviar una notificación cuando cruce el umbral.(SNMP traps).                                                                                                                                                                                                                                                      |
| Information                 | Este campo muestra el resultado del sistema de propiedades o un mensaje de error en caso de problemas después de que usted pulsa Apply Changes.                                                                                                                                                                                           |

**Tabla 5. Descripción de las propiedades de un dispositivo.**

|                             |                                                                                                                                                                                                                                                                           |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Polling              | Escoja esta opción para que periódicamente recoja información de los dispositivo, generar un indicador del dispositivo y muestre el dispositivo en el Tablero de Patrol. De ser puesto a falso, el dispositivo y sus sub-objetos no son mostrados en el informe generado. |
| Show Interfaces             | Escoja esta opción para ampliar la red y mostrar las interfaces bajo cada artículo de dispositivo. Si los interfaces son gris, el poleo esta deshabilitado en su nivel.                                                                                                   |
| Export Raw Data             | Escoja esta opción para exportar datos en el archivo de informe de ASCII.                                                                                                                                                                                                 |
| DataBase Export             | Escoja esta opción para exportar datos en bases de datos en modelo Patrol Dashboard CIM.                                                                                                                                                                                  |
| Use SNMP V2C                | Escoja esta opción para usar los datos SNMP que son compatibles con SNMP v2 estándar. Use esta opción a no ser que la compatibilidad SNMP v1 sea obligatoria.                                                                                                             |
| Netflow and Port            | Escoja esta opción para activar la función de Netflow de dispositivos Cisco. Especifique el número de puerto que es asociado a Netflow.                                                                                                                                   |
| Track Netflow on Interfaces | Escoja esta opción para detallar la información Netflow en el nivel de interfaces de dispositivo.                                                                                                                                                                         |
| Top Talkers and Pairs       | Defina cuantos pares de TopN talkers deben ser tenidos en cuenta en la estadística y gráficos TopN.                                                                                                                                                                       |

**Tabla 6. Descripción de otras propiedades de un dispositivo.**

### 6.2.9 Tipos de Indicadores d Límites (Thresholds)

Para cada uno de los dispositivos, se pueden establecer que tipos de reportes se desea; así como también los límites para cada uno de ellos. Solo es necesario escoger el tipo de indicador como Work load (carga de trabajo) y establecer los parámetros deseados.

Los indicadores se detallan como se muestra en el Gráfico 76.

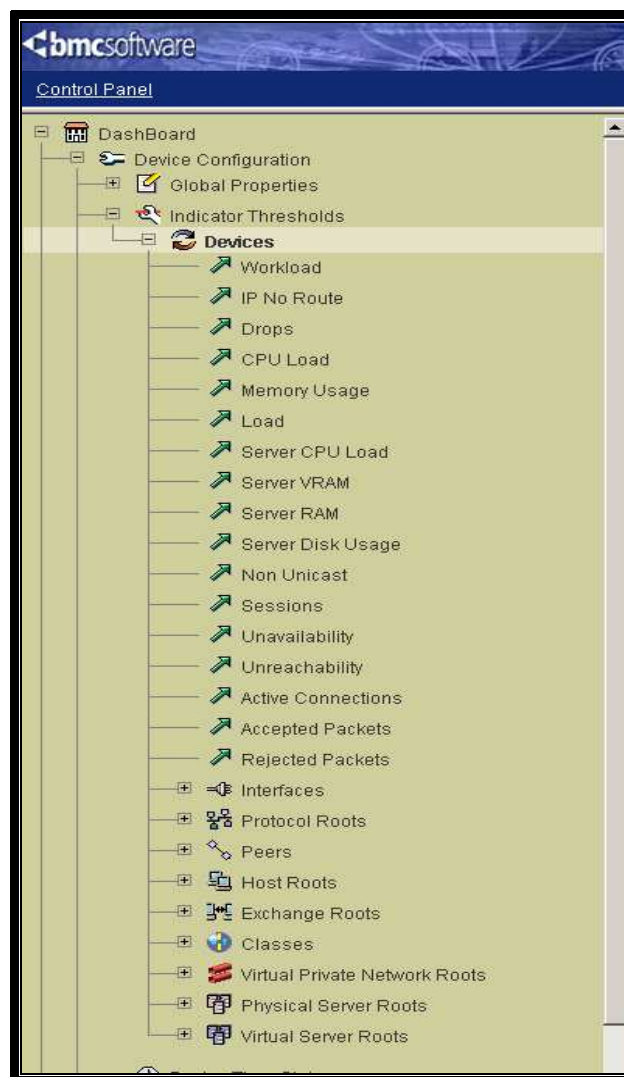


**Gráfico 76. Tipos de Indicadores**

### 6.2.10 Estableciendo Limites

Los dispositivos tienen un límite o thresholds por defecto que lo extraen de la información que obtienen del propio dispositivo, pero también se los puede configurar de acuerdo a las necesidades de información.

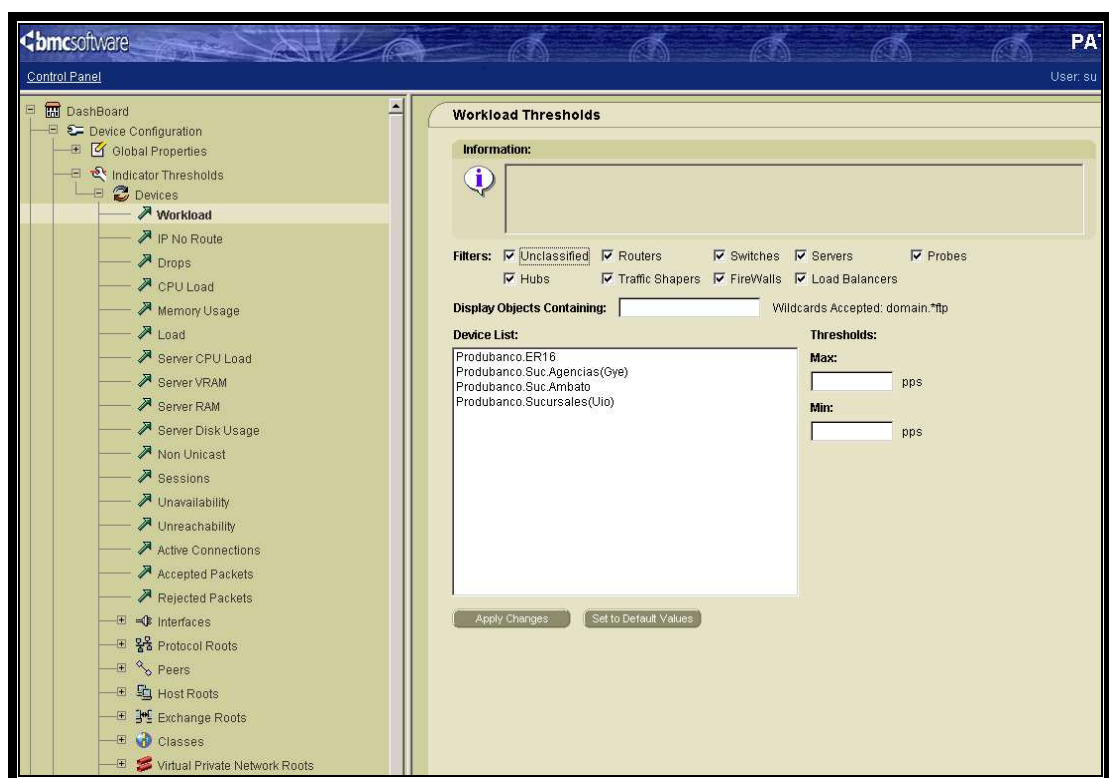


**Gráfico 77. Indicadores de limites para Workload.**

En la tabla 7 se describen cada uno de los parámetros que Patrol proporciona para configurar los thresholds o límites, en esta caso como ejemplo para Workload.

|                             |                                                                                                                                                 |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Filters                     | Use estas cajas de comprobación para seleccionar los tipos de dispositivo a lo que se aplicará la regla. Aplíquese a algún objeto.              |
| Display Objects containing: | Escriba una cadena para seleccionar el o los tipos de objetos que desee.                                                                        |
| Max                         | Ingresa un valor para el umbral superior                                                                                                        |
| Min                         | Ingresa un valor para el umbral inferior                                                                                                        |
| Information                 | Este campo muestra el resultado del sistema de propiedades o un mensaje de error en caso de problemas después de que usted pulsa Apply Changes. |
| <b>Buttons</b>              |                                                                                                                                                 |
| Set to Default Values       | Retorna a los valores por defecto                                                                                                               |
| Apply Changes               | Confirma el Umbral                                                                                                                              |

**Tabla 7. Descripción de Indicadores de límites para Workload.**

### 6.2.11 Intervalos de Tiempo del Dispositivo

Aquí se configura y define un período de tiempo para ser considerado cuando se calcula los promedios diarios o semanales para los indicadores de dispositivos seleccionados.

En la grafica 78 muestra la hora del día en que envíe el mail de reporte(DAILY). Así como también que día(s) de la semana requiera el informe.

Por defecto configura un reporte diario a las 24h00

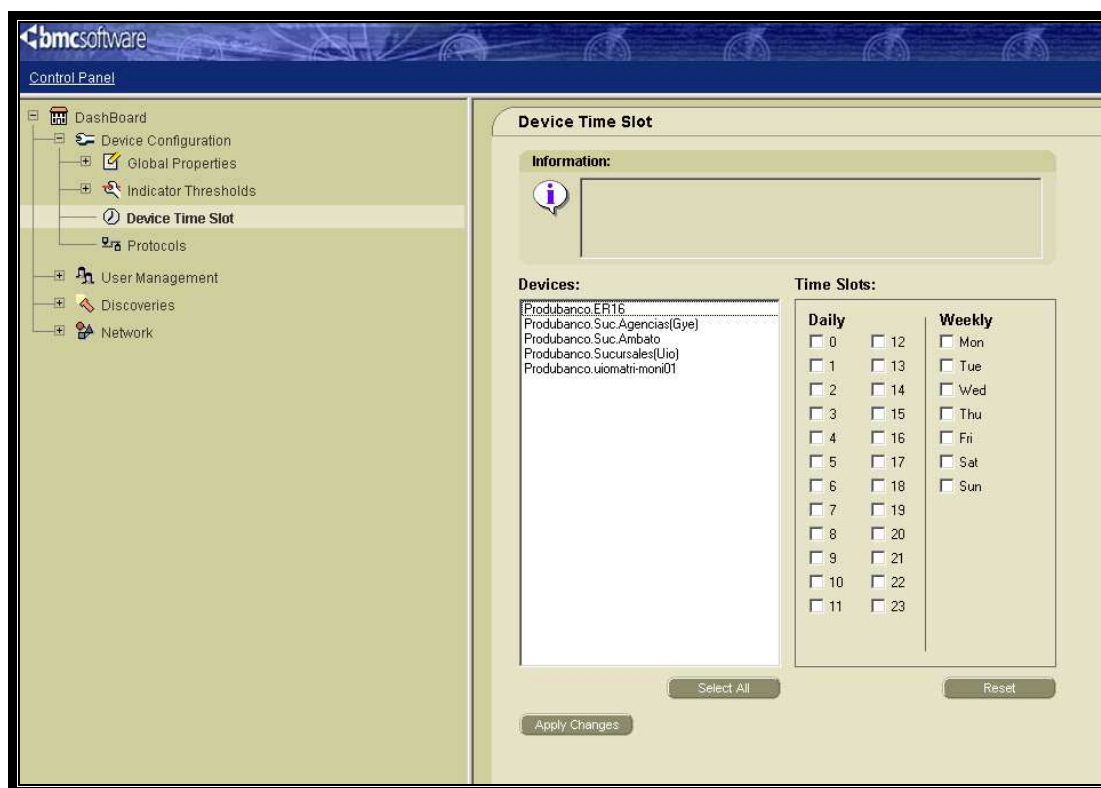


**Gráfico 78. Intervalos de tiempo de dispositivos**

### 6.2.12 Protocolos

Estos conceptos se consideran solo para Netflow y RMON2. Los protocolos debajo de tal raíz son conectados a las interfaces físicas de sondas de RMON2.

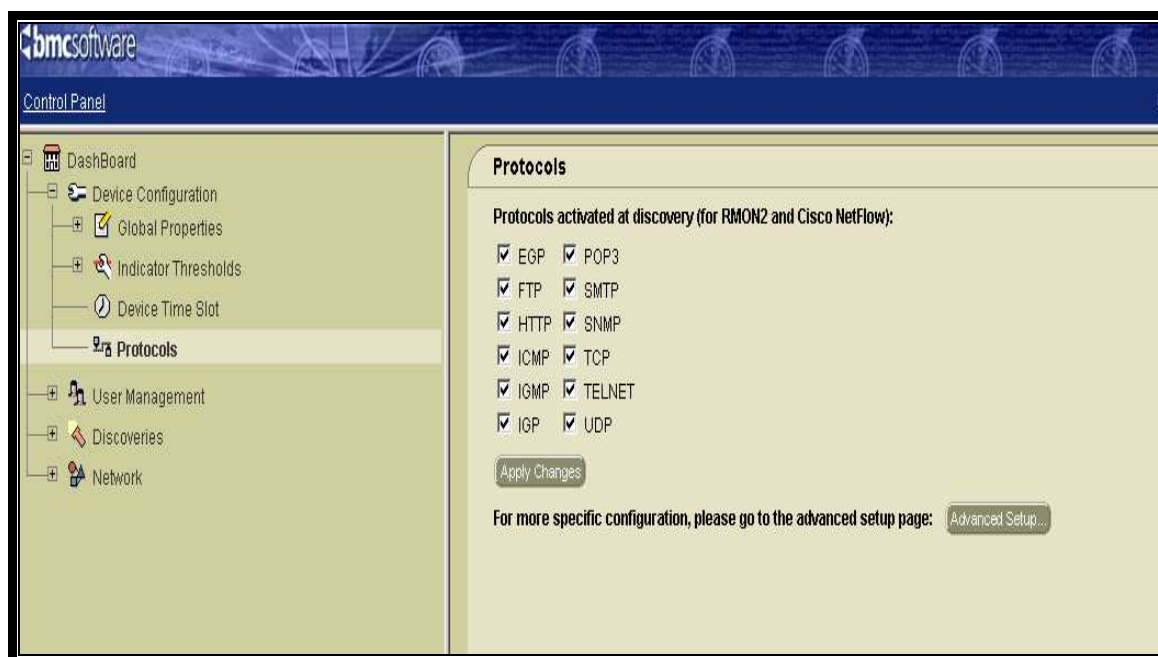


**Gráfico 79. Protocolos que utiliza Patrol**

### **6.2.13 Perfiles**

Un perfil está compuesto de un nivel de permisos así como los datos de detalle a los cuales un usuario con este perfil tiene el acceso. Los perfiles existentes es el Cliente y perfiles Estándar. Pero se pueden crear los necesarios en el caso de requerirlos.

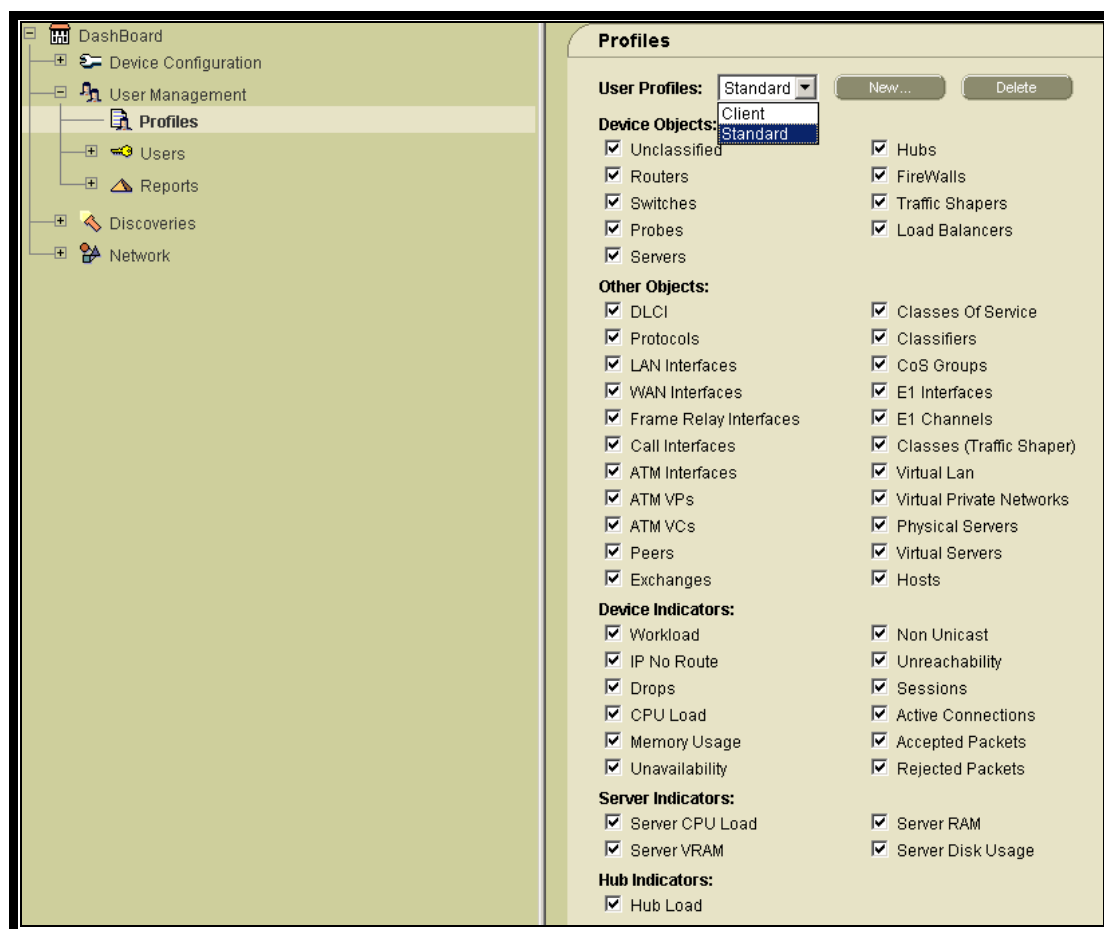


**Gráfico 80. Perfiles de usuario**

#### **6.2.14 Usuarios**

Par acceder a este ítem debe asegurarse de estar conectado con privilegios de Súper Usuario (SU) o un perfil que le permita crear usuarios.

Como datos principales debe ingresar el nombre del usuario, la clave, su confirmación y el e-mail a donde enviará los reportes. Adicionalmente le permite especificar a que tipo de reporte accesoria el usuario, como también cada cuanto recibe los reportes.

The screenshot shows the 'Control Panel' window of the Patrol DashBoard. On the left is a tree view with categories: DashBoard, Device Configuration, User Management (containing Profiles and Users), Reports, Discoveries, and Network. Under 'Users', the user 'acunaee' is selected. The main area is titled 'User Properties' and contains the following fields and options:

- User Name:** acunaee
- Password:** [masked with asterisks]
- Password Confirmation:** [masked with asterisks]
- Email:** acunaee@produbanco.com
- Profile:** Standard (dropdown menu)
- Threshold Notification:** ☒ (checked)
- Notification Period:** ☒ 5 min, ☐ Hourly
- Notification on Threshold Crossing:** ☒ Downward, ☒ Upward
- Automatic Scale:** ☒ (checked)
- Buttons:** Advanced Mail Configuration... (disabled), Apply Changes (disabled)

Below the email field, there is a note: 'In case of address solving problem (DNS troubles, NAT...) with hyperlinks in mails, please set up the way to read PATROL DashBoard server by clicking on the Advanced Mail Configuration button:'.

**Gráfico 81. Usuarios de Patrol DashBoard**

### 6.2.15 Reportes

Este ítem permite establecer formatos preestablecidos de informe, así como también el periodo en que se emitirán que se pueden asociar a los usuarios creados, según el tipo de información que requiera cada uno.

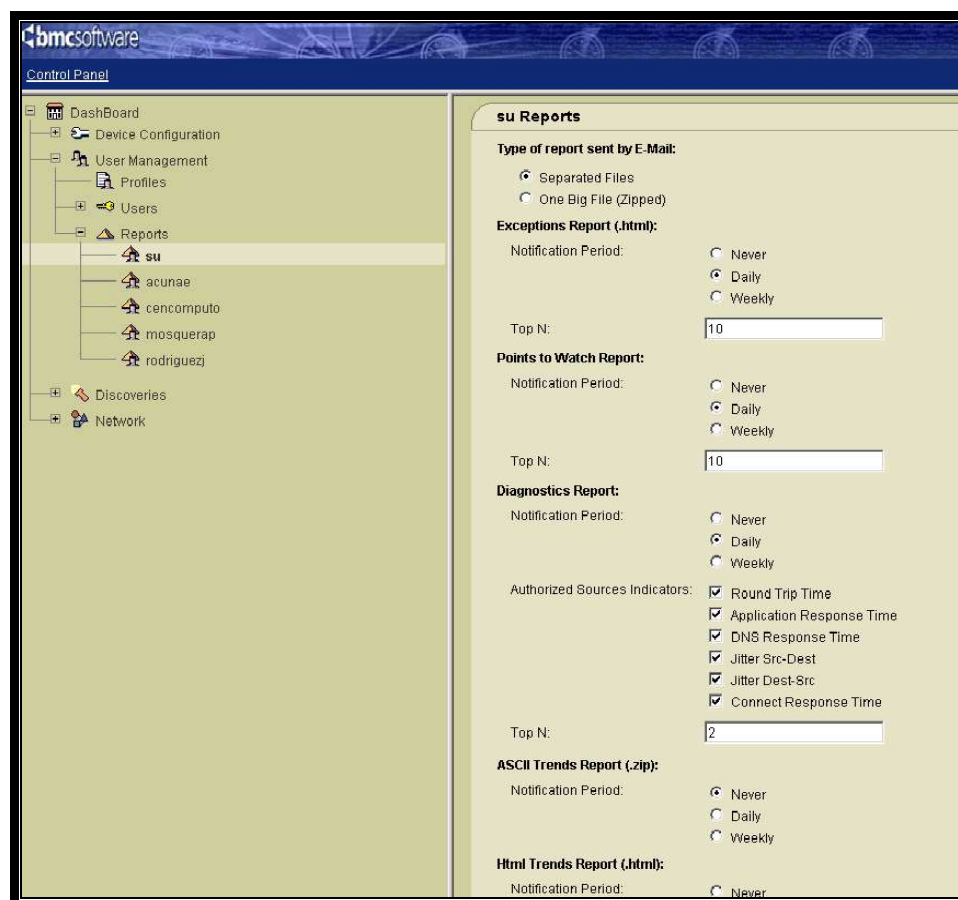


**Gráfico 82. Reportes de Alarmas**

### 6.2.16 Network (Red)

Aquí se establecen o se configuran la red a monitorear, estas pueden estar divididas internamente según los tipos de dispositivos que contengan dicha red.

El numero de Network que permite ingresar esta definido por la compra del paquete.

Este informe muestra los acontecimientos de cruces de umbral dentro de un día seleccionado para un dispositivo, internaz o la subinterfaz) bajo la raíz de la Red.

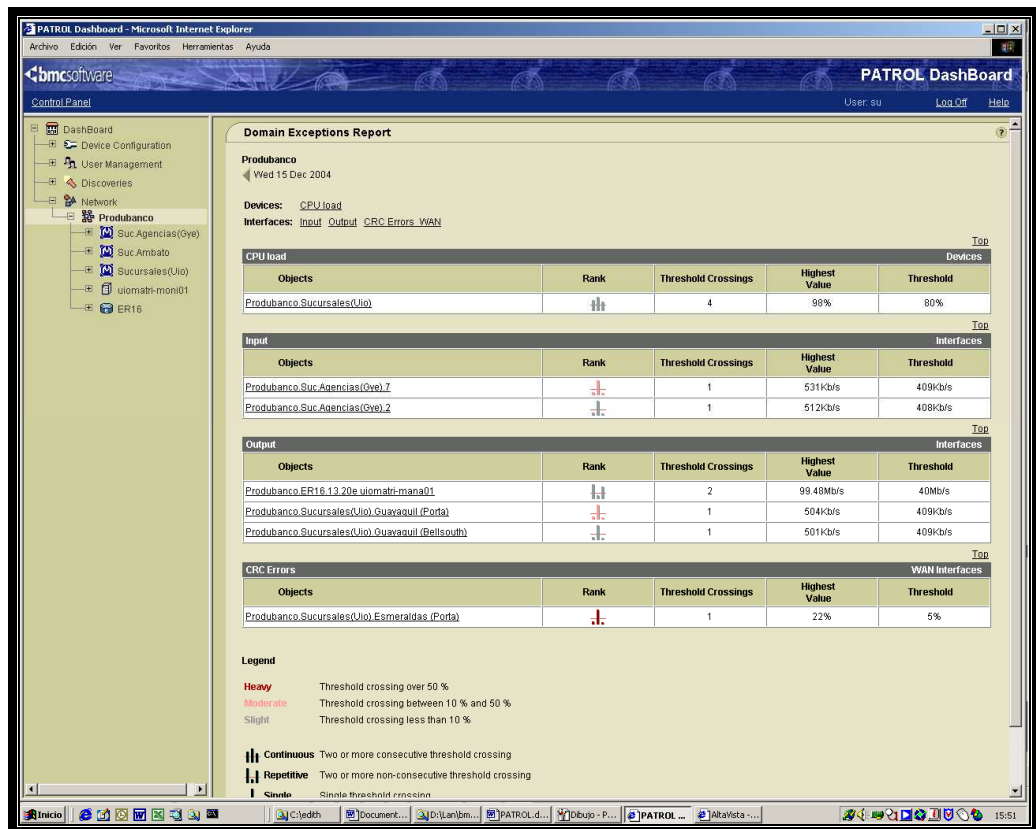


**Gráfico 83. Red de Monitoreo**

### 6.2.17 Alertas y Notificaciones

Al detectar una situación anormal en algún dispositivo, servicio, protocolo o aplicación, PATROL DashBoard puede llevar a cabo diferentes acciones, incluyendo notificaciones predefinidas vía e-mail.

Estos mensajes de alerta pueden ser personalizados por el usuario en cuanto a tiempo y tipo de información.

Los eventos típicos que pueden ser notificados son, entre otros:

- Limite (threshold) sobrepasado de SNMP
- Performance de Windows sobrepasado
- Limite (threshold) sobrepasado de Novell NetWare
- Disponibilidad de servicio de red sobrepasado
- Host disponible /no disponible
- Servicio de red disponible /no disponible
- Recepción de trap de SNMP
- Servicio de Windows interrumpido, corriendo, pausado
- Descubrimiento de host, borrado, disponible, no disponible

Cada uno de estos eventos depende del dispositivo y marca, así como la configuración establecida en ellos para permitir el acceso a la información.

Como primera parte el dispositivo debe estar configurado como mínimo en **Read** para **SNMP** y **RMON**. Su configuración se lo hace en el menú del dispositivo según la marca. Para el caso de cisco y motorola solo es necesario habilitar (ENABLED) SNMP y RMON Read o Read /Write con el nombre de la comunidad.

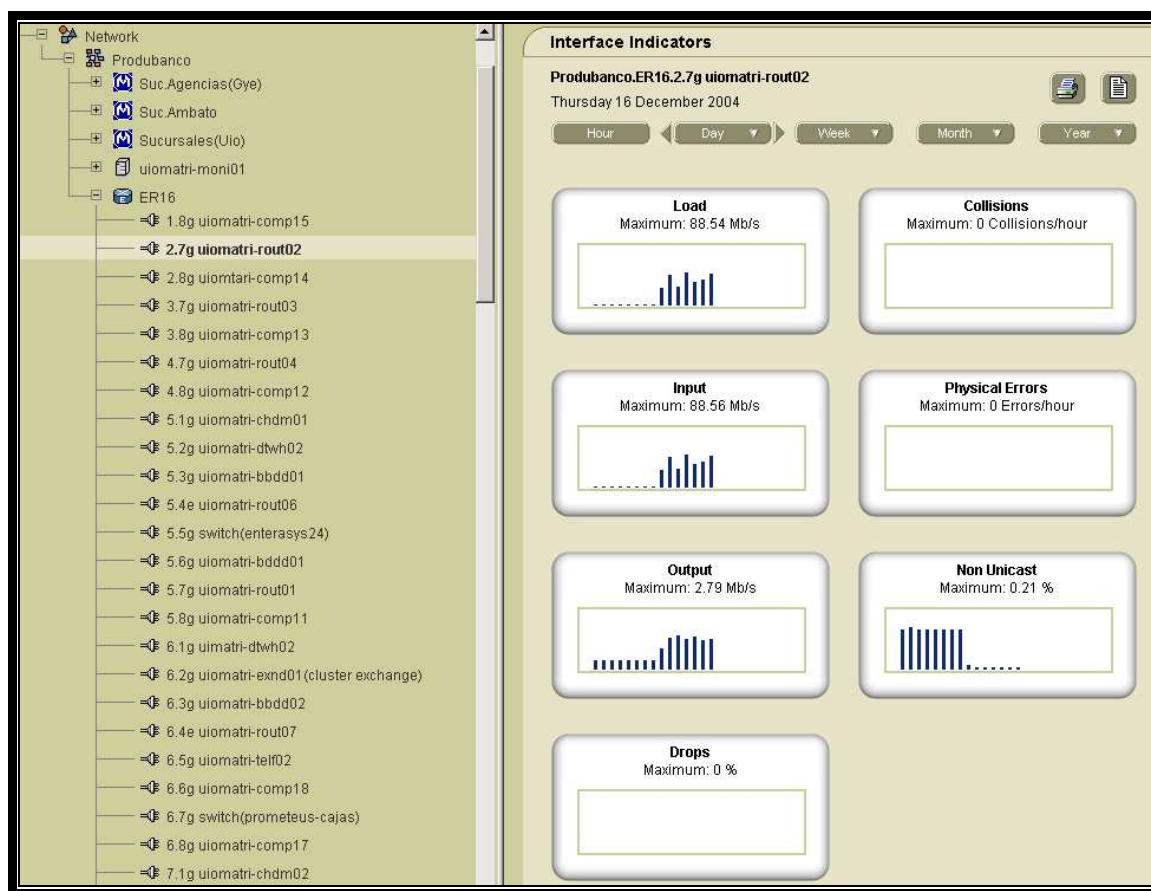


**Gráfico 84. Ejemplo de Alertas y notificaciones**

### 6.2.18 Tiempo Real

Se puede monitorear cada uno de los dispositivos en tiempo real, para poder relacionar algún evento que provoque el traspaso del límite.

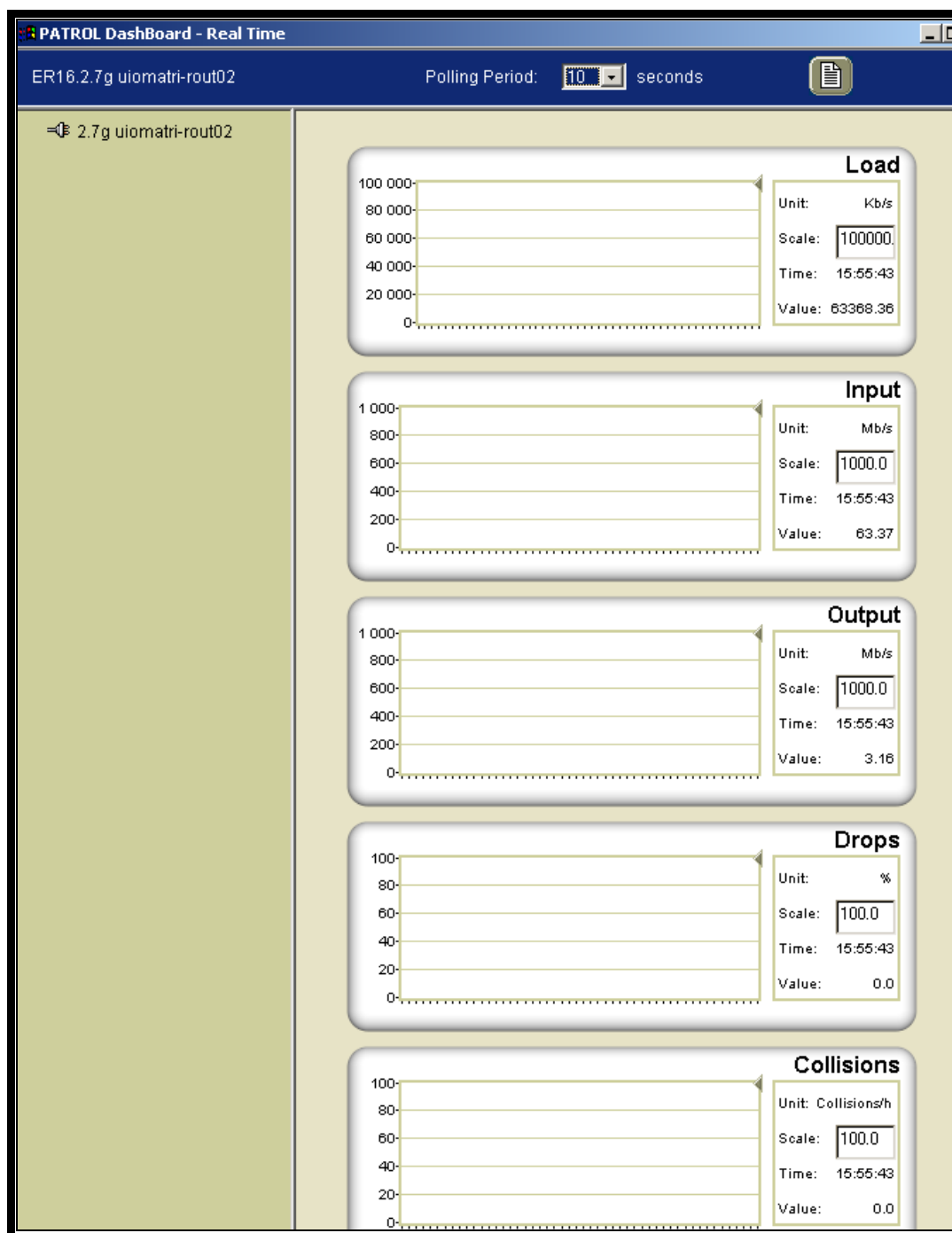


Gráfico 85. Ejemplo de un informe en tiempo real

Para ingresar un dispositivo solo es necesario la IP y el nombre de la comunidad; una vez este sea ingresado automáticamente reconoce cada uno de los puertos que posea; así como también el tipo de dispositivo que se esta ingresando.

Para el Gráfico 86 descrito abajo se puede observar un router Motorola, un ER16 y un Servidor.

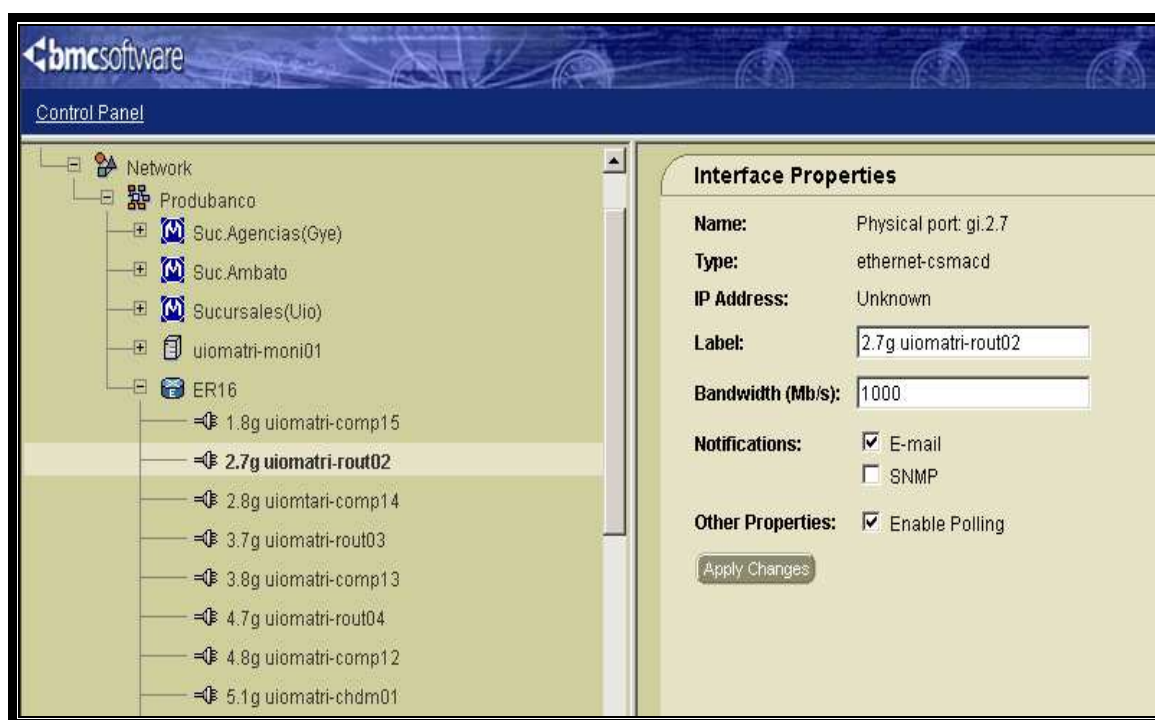


**Gráfico 86. Ejemplo de dispositivos de una red**

### **6.2.19 Alertas Escalables y Temporizador**

PATROL DashBoard le permitirá difundir diferentes tipos de alarmas a diferentes niveles de usuario. Esto significa que un evento puede disparar más de un tipo de acciones a diferentes tiempos. Por ejemplo, un tipo de alerta puede ser programado para inmediatamente ocurrido el inconveniente se envíe un mensaje en forma de anuncio en el escritorio a un administrador junior.

Otra acción puede ser un segundo mensaje 5 minutos después de ocurrido el evento en forma de SMS a un nivel superior de soporte; y otro luego de 30 minutos si el tema no ha sido resuelto (ej. E-mail a un supervisor). Esta acción, o cualquier otra, puede ser predefinida tantas veces como se desee por el usuario para continuar enviándose hasta que se solucione el inconveniente o la persona responsable tome cartas en el asunto. Las alertas pueden ser asociadas a diferentes responsabilidades entre los administradores. Por ejemplo, una persona responsable de los servidores de Windows será notificada solo si algún dispositivo de su área de responsabilidad tiene algún problema. De esta manera las alertas son asignadas de acuerdo a las áreas de responsabilidad, conocimiento o guardias.

Además, es posible asignar demoras en las notificaciones. De esta manera, NetCrunch no enviará una alerta inmediatamente después de ocurrido un evento (ej. Sistema esta down) sino que esperará un cierto tiempo para notificar esta situación, de esta manera, si el inconveniente se soluciona durante el período de tiempo especificado (ej. Sistema up

nuevamente) el administrador no será alertado innecesariamente y se evitará una falsa alarma.

Ejemplos de mail de alertas configurados para dos tipos de usuario.

Usuario1. Reporte Diario. Véase en anexos

Usuario2. Reporte de Alarmas cada 5 minutos. Véase en anexos

### 6.3 Cuadro Comparativo Patrol DashBoard y Solar Win

| <b>Características</b>                                                         | <b>Patrol Dashboard</b> | <b>Solar Win</b> |
|--------------------------------------------------------------------------------|-------------------------|------------------|
| Conocer donde están los cuellos de botella en la red                           | X                       | X                |
| Verificar el ancho de banda                                                    |                         | X                |
| Predecir posible congestiones                                                  | X                       |                  |
| Conocer que elementos se utilizan más/menos de lo debido                       | X                       |                  |
| Supervisión remota del funcionamiento de los dispositivos                      | X                       | X                |
| Permite tener varios perfiles de usuario                                       | X                       |                  |
| Predecir saturación de enlaces WAN o LAN                                       | X                       |                  |
| Monitorear y ver gráficamente en tiempo real el # de paquetes perdidos         | X                       | X                |
| Supervisar cada nodo manejado mediante SNMP                                    | X                       | X                |
| Optimizar costos de operaciones                                                | X                       |                  |
| Proveer de gráficos históricos y mapas de la utilización de la red             | X                       | X                |
| Justificar la inversión de nuevos elementos de hardware                        | X                       |                  |
| Crear una base de datos del inventario detallado de la red                     | X                       | X                |
| Anticipa pérdidas o caídas del funcionamiento de la red                        | X                       |                  |
| Genera informes sobre los dispositivos de los cuales es responsable            | X                       | X                |
| Envía alertas a correos electrónicos y teléfonos celulares (e-mail)            | X                       | X                |
| Genera reportes dependiendo del perfil de usuario                              | X                       |                  |
| Se adapta a varias plataformas                                                 | X                       |                  |
| Su uso no genera tráfico en la red                                             | X                       |                  |
| Usa arquitectura web-browser                                                   | X                       |                  |
| Permite visualizar, actualizar y realizar cambios a cualquier dispositivo SNMP | X                       | X                |
| Proporciona un histórico de eventos de los dispositivos monitoreados           | X                       |                  |

## **7 CAPITULO VII**

### **CONCLUSIONES Y RECOMENDACIONES**

#### **7.1 Conclusiones**

Al realizar el estudio de varias herramientas para la gestión de red en centros de cómputo enfocado al protocolo SNMP/RMON se concluye que PATROL DashBoard es la herramienta escogida debido a que:

1. Permite el manejo de perfiles de usuarios, lo que optimiza y centraliza la información requerida por cada usuario en forma confidencial.
2. Patrol DashBoard permite a los usuarios medir el servicio que obtienen gracias a su interfaz basada en Web-Browser.
3. Los eventos de red son trabajados en combinación con las alertas, estadísticas, reportes y tendencias que el mismo software los genera. Además recolecta y determina con exactitud la información generada y enviada por el equipo.
4. Permite justificar la adquisición de nuevo hardware mediante la información histórica que proporciona Patrol DashBoard a través de los protocolos.
5. Permite clasificar las alertas de acuerdo a las funciones o responsabilidades de cada perfil de usuario.

6. No se puede olvidar, sin embargo, que la gestión de red, es un problema que nunca estará totalmente resuelto por las herramientas, ya que éstas, sin personal cualificado o procedimientos específicos, pierden su valor.

## **7.2 Recomendaciones**

- Actualmente las redes de área extensa están evolucionando a escenarios de alta velocidad en los que se hace necesario una monitorización con alta fiabilidad. Para ello el uso de herramientas de monitoreo basadas en protocolo SNMP y RMON es imprescindible.
- Aprovechar la inversión en la herramienta de gestión para optimizar la obtención de infraestructuras, sistemas, aplicaciones y sobre todo mejorar el servicio de las empresas.
- Es importante recalcar, que la información que nos proporciona una herramienta de monitoreo debe ser utilizada para educar a los usuarios, de tal forma que utilicen los recursos de una manera óptima.
- La adquisición de una herramienta de gestión específica está justificada, puesto que ofrece soluciones a los problemas de una organización. Pero es necesario que se logre una interoperabilidad entre las distintas herramientas de gestión, para que no de lugar a visiones parciales e incompletas y a inconsistencias en la actuación frente a problemas de las organizaciones.

- El uso de Patrol DashBoard permite la visualización de estadísticas en tiempos reales e históricos, sirviendo de ayuda en la toma de decisiones.
- Patrol DashBoard es recomendable además porque a través de este se configura de manera gráfica los dispositivos de la red, lo que significa un ahorro de tiempo.

## 8 GLOSARIO DE TÉRMINOS

### A

**Administrador de red.-** es la persona responsable de supervisar y controlar el hardware y software de una red. El administrador trabaja en la detección y corrección de problemas que hacen ineficiente o imposible la comunicación y en la eliminación de las condiciones que pudieran llegar a provocar el problema nuevamente.

### **Agente**

- En general, es el software que procesa consultas y devuelve respuestas en nombre de una aplicación.
- En NMSs, es el proceso que reside en todos los dispositivos administrados, e informa los valores de variables especificadas a estaciones de gestión.
- En la arquitectura de hardware Cisco, una tarjeta de procesador individual que provee una o más interfaces de medios.

### **Alarma**

Mensaje que notifica a un operador o administrador sobre un problema de la red.

### **Ancho de banda**

Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. El término se utiliza también para describir la medida de capacidad de throughput de un medio o protocolo de red dados.

### **ANSI (American National Standards Institute)**

Instituto nacional americano de normalización. Organización voluntaria compuesta por corporaciones, el gobierno y otros miembros, que coordina actividades relacionadas con estándares, aprueba normas nacionales de EE.UU., y desarrolla posiciones para Estados Unidos en organizaciones internacionales de estándares. ANSI contribuye a desarrollar normas estadounidenses e internacionales relacionadas, entre otras cosas, con comunicaciones y networking. ANSI es miembro de IEC y de ISO.

### **API (application programming interface)**

Interfaz de programación de aplicaciones. Especificación de convenciones de llamadas de función que define una interfaz a un servicio.

### **AppleTalk**

Serie de protocolos de comunicaciones diseñada por Apple Computer. Existen dos fases actualmente. La Fase 1, la versión anterior, soporta una red física simple que puede tener solamente un número de red y estar en una zona. La Fase 2, la versión más reciente, soporta redes lógicas múltiples en una red física simple, y permite a las redes estar en más de una zona.

### **ARP (Address Resolution Protocol)**

Protocolo de resolución de direcciones. Protocolo de Internet que se utiliza para mapear una dirección IP a una dirección MAC. Definido en RFC826.

### **Arquitectura cliente-servidor**

Término utilizado para describir los sistemas de red de informática distribuida en los cuales las responsabilidades de la transacción se dividen en dos partes: cliente (frontal) y servidor (nodo). Ambos términos (cliente y servidor) pueden aplicarse a programas de software o a dispositivos reales de computación. También llamado informática distribuida.

### **ASCII (American Standard Code for Information Interchange)**

Código normalizado americano para el intercambio de información. Código de 8 bits para representación de caracteres (7 bits más paridad).

### **ASN.1 (Abstract Syntax Notation One)**

Sintaxis abstracta de notación uno. Lenguaje OSI para describir tipos de datos, independientemente de estructuras informáticas particulares y técnicas de representación. Descripta por el estándar internacional ISO 8824.

### **Agente.**

Agente que se ejecuta en cada nodo de la red y recoge información del terminal y de la red que se encuentran en el MIB.

### **Agente intermediario SNMP.**

Agente SNMP asociado con una política de acceso intermediaria.

### **APDU.**

Application Protocol Data Unit, Unidad de datos de control de aplicación.

## **B**

### **Backbone**

La parte de una red que actúa como ruta primaria para el tráfico que sale y llega de otras redes con mayor frecuencia.

### **Banda ancha**

Sistema de transmisión que multiplexa varias señales independientes en un cable. En terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que un canal con grado de voz (4 kHz). En terminología LAN, un cable coaxial sobre el cual se utiliza señalización analógica. También llamada banda amplia

### **Bridge (puente)**

Dispositivo que conecta y pasa paquetes entre dos segmentos de red que utilicen el mismo protocolo de comunicaciones. El bridge opera en la capa de enlace de datos (capa 2) del modelo de referencia OSI. En general, el bridge filtra, envía o inunda un frame entrante basándose en la dirección MAC de dicho frame.

### **Broadcast (emisión)**

Paquete de datos que se enviará a todos los nodos de una red. Los broadcasts se identifican por medio de direcciones de broadcast.

## **C**

### **Canal**

Una ruta de comunicación. En ciertos ambientes pueden multiplexarse varios canales por un cable único.

### **Cliente**

Nodo o programa de software (dispositivo frontal) que solicita servicios a un servidor.

**CMIS.** Common Management Information Services, Servicio común de gestión de información. Interfaz de servicio de administración de red OSI creado y normalizado por ISO para el monitoreo y control de redes heterogéneas.

**CMISE.** Common Management Information Service Element, Elemento de servicio de gestión de información, es el encargado de transferir la información de gestión de un sistema a otro por lo que trabaja mano a mano con CMIP. CMISE mapea todas sus acciones en operaciones CMIP sobre el terminal remoto. Es decir, es CMISE el que manda a CMIP que envíe una PDU para realizar cierta acción, y en recepción CMIP pasa el evento a CMISE el cual lo hace llegar al usuario.

**CMOT.** CMIP sobre TCP/IP.

**CCITT.** International Consultative Committee on Telegraphy and Telephony. Comité Consultivo de Telegrafía y Telefonía. Organización que establece estándares internacionales sobre telecomunicaciones.

**CGI** Common Gateway Interface. Interfaz de Acceso Común. Programas usados para hacer llamadas a rutinas o controlar otros programas o bases de datos desde una página Web. También pueden generar directamente HTML.

**CMIP** .Common Management Information Protocol, Protocolo Común de Gestión de Información, es otro protocolo de gestión sobre OSI (CMIP se encuentra en el nivel de aplicación OSI) y más complejo que SNMP.

### **Comunidades SNMP**

Sistema de autenticación que permite que un dispositivo de red inteligente valide las solicitudes SNMP de fuentes tales como el NMS.

### **Congestión**

Tráfico que excede la capacidad de una red.

**Consola** DTE a través del cual se ingresan los comandos en un host.

### **Control de errores**

Técnica utilizada para detectar y corregir errores en transmisiones de datos.

### **CPU (Central Processing Unit)**

Unidad central de procesamiento. Parte de una computadora que controla todas las partes restantes. Captura las instrucciones de la memoria y las decodifica. Esto puede hacer que transfiera datos hacia o desde la memoria o active periféricos para realizar entradas o salidas.

## **D**

### **Datagrama**

Agrupamiento lógico de información enviada como una unidad de capa de red por un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades principales de información en la Internet. Los términos frame, mensaje, paquete, y segmento también se utilizan para describir los agrupamientos lógicos de información en las diferentes capas del modelo de referencia OSI y en varios círculos de tecnología.

**Datos** Datos del protocolo de capa superior.

**Dirección de transporte.** En el servicio UDP, dirección IP seguida por un número de puerto UDP.

**DCN** Data Communication Network.

**DDP** Datagram-Delivery Protocol, Protocolo de Datagrama de Entrega

Este protocolo es responsable del zócalo a la entrega del zócalo de datagramas sobre el Internet de Appletalk.

## **Dirección**

Estructura de datos o convención lógica utilizada para identificar una entidad única, como un proceso particular o un dispositivo de red.

## **Dirección IP**

Dirección de 32 bits asignada a los hosts que utilizan TCP/IP. Una dirección IP corresponde a una de cinco clases (A, B, C, D, o E) y se escribe en forma de 4 octetos separados con puntos (formato decimal con punto). Cada dirección consiste en un número de red, un número opcional de subred, y un número de host. Los números de red y de subred se utilizan conjuntamente para el enrutamiento, mientras que el número de host se utiliza para el direccionamiento a un host individual dentro de la red o de la subred. Para extraer la información de la red y de la subred de la dirección IP se utiliza una máscara de subred. También denominada dirección de Internet.

(IP address) Comando utilizado para establecer la dirección de red lógica de esta interfaz.

## **Dirección MAC**

Dirección de la capa de enlace de datos estandarizada, necesaria para cada puerto o dispositivo conectado a una LAN. Otros dispositivos en la red utilizan estas direcciones para localizar puertos específicos en la red, y para crear y actualizar tablas de enrutamiento y estructuras de datos. Las direcciones MAC tienen una longitud de 6

bytes y son controladas por IEEE. También conocidas como dirección de hardware, dirección de capa MAC, o dirección física.

### **DNS (Domain Naming System)**

Sistema de denominación de dominio. Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones.

### **Dominio**

- En Internet, una parte del árbol de jerarquía de nombres que se refiere a los agrupamientos generales de redes basadas en tipo de organización o geografía.
- En SNA, un SSCP y los recursos que controla.
- En IS-IS, un conjunto lógico de redes.

### **Documentos RFC.**

Los documentos llamados Request for Comments o RFCs Pedido para Comentarios son las notas de trabajo del "Network Working Group" (Grupo de Trabajo de Red), que es la comunidad Internet de investigación y desarrollo. Un documento en esta serie puede tratar esencialmente sobre cualquier tema relacionado a la comunicación de computadoras, y puede ser cualquier cosa desde el informe de una reunión a la especificación de un estándar.

**Aviso: Todas las normas se publican como RFCs, pero no todos los RFCs especifican normas. Cualquiera puede presentar un documento para que sea**

**publicado como RFC. Las solicitudes deben hacerse por medio de correo electrónico al Editor de RFC.**

**E**

**Entidades de aplicación SNMP.**

Entidades en las estaciones de gestión y los elementos de red que se comunican utilizando el SNMP.

**Entidades de protocolo.**

Procesos que implementan el SNMP y por tanto soportan a las entidades de aplicaciones SNMP.

**Esquema de autenticación.**

Conjunto de reglas por las que un mensaje SNMP es reconocido como un mensaje SNMP auténtico para una cierta comunidad SNMP.

**Ethernet.**

Diseño de red de área local normalizado como IEEE 802.3. Utiliza transmisión a 10 Mbps por un bus Coaxial. Método de acceso es CSMA/CD.

**ETSI** European Telecommunication Standards Institute. Instituto Europeo de Estándares en Telecomunicaciones.

**Estación de administración**

La estación de administración es la interfaz del administrador de red al sistema de red. Posee los programas para manipular los datos y controlar la red. La estación de administración también mantiene una base de datos de información de administración (MIB) extraída de los dispositivos bajo su administración.

### **Elemento de Red (ER).**

Son diversos tipos de equipos considerados como “entes gestionados”, como son: Sistemas de transmisión, sistemas de conmutación, terminales, concentradores, servidores, encaminadores, puentes, etc.

**Elemento de Gestión (EG).**- Son elementos encargados de monitorizar, coordinar y controlar a los ER.

### **Encapsulación**

Envoltura de datos en un encabezado de protocolo particular. Por ejemplo, los datos de Ethernet se envuelven en un encabezado específico de Ethernet antes de su tránsito por la red. Además, cuando se hace bridging de redes disímiles, se coloca simplemente todo el frame de una red en el encabezado utilizado por el protocolo de la capa de enlace de datos de la otra red.

### **Encriptación**

La aplicación a los datos de un algoritmo específico para alterar la presentación de los datos al hacerlos incomprensibles para los terceros que no estén autorizados a ver la información.

## **Enlace**

Canal de comunicaciones en red que consta de un circuito o ruta de transmisión y todo el equipo relativo entre un emisor y un receptor. Se lo utiliza más frecuentemente para referirse a una conexión WAN. Algunas veces denominado línea o enlace de transmisión.

## **Enrutamiento**

Proceso que consiste en encontrar la ruta hasta el host de destino. El enrutamiento es muy complejo en las redes de grandes dimensiones debido a los diversos destinos intermedios potenciales que un paquete debe atravesar antes de llegar a su host de destino.

## **Equilibrio de la carga**

En enrutamiento, la capacidad de un router de distribuir el tráfico por todos sus puertos de red que se encuentren a la misma distancia de la dirección de destino. Los buenos algoritmos de balanceo de carga utilizan tanto la información sobre velocidad como sobre confiabilidad de la línea.

## **F**

**Fast Ethernet.** Diseño de red Ethernet, donde se alcanzan velocidades de hasta 100 Mbps, comúnmente son inteligentes y se les permite identificar los nodos que trabajarán más rápido que otros.

**FIREWALL.** Cortina de Fuego. ROUTER diseñado para proveer seguridad en la periferia de la red. Se trata de cualquier programa (Software) ó ROUTER (Hardware) que protege a una red de otra red. El FIREWALL da acceso a una maquina en una red local a Internet pero Internet no ve mas allá del FIREWALL.

### **FDDI (Fiber Distributed Data Interface)**

Interfaz de datos distribuida por fibra. Norma LAN, definida por ANSI X3T9.5, que especifica una red de token-passing de 100-Mbps que utiliza un cable de fibra óptica, con distancias de transmisión de hasta 2 km. FDDI utiliza una arquitectura de anillo doble para dar redundancia.

### **Frame Relay**

Protocolo de la capa de enlace de datos conmutados, de norma industrial, que administra varios circuitos virtuales utilizando una encapsulación HDLC entre dispositivos conectados. Frame Relay es más eficaz que X.25, el protocolo para el cual se considera por lo general un reemplazo.

### **FTP (File Transfer Protocol)**

Protocolo de transferencia de archivos. Protocolo de aplicación, parte de la pila de protocolos TCP/IP, utilizado para transferir archivos entre nodos de red. FTP está definido en RFC 959

## **G**

**Gateway.** Pasarela. Puerta de Acceso. Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red.

**Gestión de red.** Se define como el proceso o control de la información compleja que circula por la red para maximizar su eficiencia y productividad. Las áreas fundamentales en las que actúa son la gestión de fallos, gestión de la configuración, gestión de la seguridad, gestión de la ejecución y gestión de la contabilidad.

**Gestor.** Gestor que se encuentra localizado en el servidor principal de la red. Su papel principal es recorrer los agentes (agents) para pedirles información importante para la gestión de la red.

**GDMO.** Guidelines for the Definition of Managed Objects

### **Gateway**

En la comunidad IP, un término antiguo que se refiere a un dispositivo de enrutamiento. En la actualidad, se utiliza el término router para describir los nodos que realizan esta función, mientras que gateway se refiere a un dispositivo para fines especiales que convierte información de la capa de aplicación de un stack de protocolo a otro.

### **GUI (graphical user interface)**

Interfaz gráfica del usuario. Entorno de usuario que utiliza representaciones de texto y de imagen de la entrada y salida de aplicaciones así como una estructura de datos jerárquica o de otro tipo donde se almacena información. Son típicas convenciones como botones, íconos y ventanas, y se realizan muchas tareas mediante un dispositivo

de señalización (como un ratón). Microsoft Windows y Apple Macintosh son ejemplos destacados de plataformas que utilizan una GUI.

## **H**

**Hardware.** A los componentes que es posible ver y tocar se les llama en jerga computacional "hardware", palabra inglesa cuyo significado es máquina o "cosa dura".

## **Host**

Sistema de computación en una red. Similar al término nodo excepto que el host usualmente implica un sistema de computación, mientras que un nodo generalmente se aplica a cualquier sistema en red, incluyendo los servidores de acceso y routers.

## **Hub (concentrador)**

- En forma general, un término utilizado para describir un dispositivo que sirve como centro de una red de topología en estrella.
- Dispositivo de hardware o software que contiene múltiples módulos independientes pero conectados de equipo de red e internetwork. Los hubs pueden ser activos (cuando repiten señales enviadas a través de ellos) o pasivos (cuando no repiten, sino que meramente dividen las señales enviadas a través de ellos).
- En Ethernet e IEEE 802.3, un repetidor Ethernet multipuerto, algunas veces denominado como concentrador.

## **HEMS (High-Level Management System)**

## **I**

**IAB.** Internet Activities Board, Boletín de actividades de Internet.

**ICMP** Internet Control Message Protocol. Protocolo Internet de Control de Mensajes.

Protocolo de mensajes de control en Internet. Protocolo Internet de capa de red que informa errores y brinda información relativa al procesamiento de paquetes IP. Documentado en RFC 792.

**IEEE** Institute of Electrical and Electronics Engineers. Instituto de Ingenieros Eléctricos y Electrónicos. Asociación Norteamericana. IEEE 802.3 Protocolo para la red LAN de la IEEE que especifica una implementación del nivel físico y de la sub capa MAC, en la capa de enlace de datos. El IEEE 802.3 utiliza CSMA/CD a una variedad de velocidades de acceso sobre una variedad de medios físicos. Extensiones del estándar IEEE 802.3 especifica implementaciones para Fast Ethernet.

**IETF** Internet Engineering Task Force. Grupo de Tareas de Ingeniería de Internet. Asociación de técnicos que organizan las tareas de ingeniería principalmente de telecomunicaciones en Internet. Por ejemplo: mejorar protocolos o declarar obsoletos otros.

**INTERNET.** Conjunto de redes y ruteadores que utilizan el protocolo TCP/IP y que funciona como una sola gran red.

**IPX** Internet Packet Exchange. Intercambio de Paquetes entre Redes. Inicialmente protocolo de Novell para el intercambio de información entre aplicaciones en una red NETWARE.

**ISP** Internet Service Provider. Proveedor de Servicios Internet.

**ITU** International Telecommunications Union. Union Internacional de Telecomunicaciones. Forma parte de la CCITT. Organización que desarrolla estándares a nivel mundial para la tecnología de las telecomunicaciones.

**Interrupción.-** es un informe de un suceso significativo, transmitido por el agente y recibido por el nodo administrador.

### **IP (Internet Protocol)**

Protocolo Internet. Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork sin conexión. El IP tiene prestaciones para direccionamiento, especificación del tipo de servicio, fragmentación y rearmado, y seguridad. Documentado en RFC 791.

### **ISO (International Organization for Standardization)**

Organización internacional para la normalización. Organización internacional que tiene a su cargo una amplia gama de estándares, incluidos aquellos referidos a networking. ISO desarrolló el modelo de referencia OSI, un popular modelo de referencia de networking.

**ITU-T (International Telecommunication Union Telecommunication Standardization Sector)**

Unión internacional de las telecomunicaciones (ITU-T) (ex -Comité de consultoría Internacional para telefonía y telegrafía - CCITT-). Organización internacional que desarrolla estándares de comunicación

**J**

**JAVA** Lenguaje de programación orientado a objeto parecido al C++. Usado en WWW para la tele carga y telejecución de programas en el computador cliente. Desarrollado por SUN MICROSYSTEMS.

**L**

**LAN** Local Area Network. Red de Área Local. Una red de área local es un sistema de comunicación de alta velocidad de transmisión. Estos sistemas están diseñados para permitir la comunicación y transmisión de datos entre estaciones de trabajo inteligentes, comúnmente conocidas como Computadoras Personales. Todas las PCs, conectadas a una red local, pueden enviar y recibir información. Como su mismo nombre lo indica, una red local es un sistema que cubre distancias cortas. Una red local se limita a una planta o un edificio.

**Layer Capa.** En protocolos o en OSI se refiere a los distintos niveles de estructura de paquete o de enlace respectivamente.

**LCP** Link Control Protocol. Protocolo de Control de Enlace

**LINUX** Versión SHAREWARE y/o FREEWARE del conocido sistema operativo UNIX. Es un sistema multitarea multiusuario de 32 bits para PC.

## **M**

### **MAC (Media Access Control)**

Control de acceso al medio. La inferior de las dos subcapas de la capa de enlace de datos definida por IEEE. La subcapa MAC administra el acceso a medios compartidos, por ejemplo, si se utilizará token passing o contención.

**Mensaje SNMP auténtico.** Mensaje SNMP originado por una entidad de aplicación SNMP que de hecho pertenece a la comunidad SNMP denominada por el componente de comunidad de dicho mensaje.

**MIB.** Management Information Base, es una base de datos donde se guarda toda la información relativa a la gestión de la red. El MIB tiene una estructura en árbol, donde en la parte superior se encuentra la información más general sobre la red, y conforme avanzamos por las ramas se consigue información más específica y detallada. Cada nodo del árbol MIB se conoce como variable, y la parte superior del árbol MIB se denomina "Internet". Aunque la ISO ha definido un MIB modelo, cada fabricante de equipos tiene el suyo propio, e el que en general aunque las variables se denominen de diferente manera la información contenida en ellas es la misma.

**Modo de acceso SNMP .** Elemento del conjunto {READ-ONLY, READ-WRITE}.

## **Mensaje**

Agrupación lógica de información de la capa de aplicación (capa 7), a menudo compuesta por una cantidad de agrupaciones lógicas de capas inferiores, tales como paquetes. Los términos datagrama, frame, paquete, y segmento también se emplean para describir agrupaciones lógicas de información en diversas capas del modelo de referencia OSI y en diversos círculos de tecnología.

### **Modelo de referencia OSI**

Modelo de referencia de interconexión de sistemas abiertos. Modelo de arquitectura de redes desarrollado por ISO e ITU-T. El modelo consiste en siete capas, cada una de las cuales especifica funciones particulares de la red, como por ejemplo direccionamiento, control de flujo, control de errores, encapsulación y transferencia confiable de mensajes. La capa superior (capa de aplicación) es la más próxima al usuario; la capa inferior (capa física) es la más próxima a la tecnología de medios. La capa siguiente a la capa inferior está implementada en hardware y en software mientras que las cinco capas superiores están implementadas únicamente en software. El modelo de referencia OSI se utiliza mundialmente para enseñar y comprender la funcionalidad de una red. Es similar en ciertos aspectos a SNA. Véase capa de aplicación, capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión, y capa de transporte.

### **Módem**

Modulador-desmodulador. Dispositivo que convierte señales digitales y análogas. En el punto de origen, un módem convierte señales digitales a una forma apropiada para la transmisión por facilidades de comunicación análogas. En el punto de destino, las

señales análogas se recuperan a su forma digital. Los módem permiten la transmisión de datos por líneas telefónicas de grado voz.

## N

**NETBIOS** Network BIOS. Network Basic Input/Output System. BIOS de una red, es decir, Sistema Básico de Entrada / salida de red.

**NIC** Network Interface Card. Tarjeta de Red.

**Nodo.** Por definición punto donde convergen más de dos líneas. A veces se refiere a una única máquina en Internet. Normalmente se refiere a un punto de confluencia en una red. Punto de interconexión a una RED.

## **NMS (network management system)**

Sistema de gestión de la red. Sistema responsable de administrar al menos parte de una red. Un NMS es en general una computadora razonablemente potente y bien equipada, por ejemplo, una estación de trabajo de ingeniería. Los NMS se comunican con agentes para contribuir a mantener un seguimiento de recursos y estadísticas de red.

## O

**OSI.** Open Systems Interconnection. Interconexión de Sistemas Abiertos. Modelo de referencia de interconexión de sistemas abiertos propuesto por la ISO. Divide las tareas de la red en siete niveles.

**OIW.** OSI Implementors Workshop, Grupo de trabajo de implementación de OSI.

**ONMF.** OSI Network Management Forum, Foro de gestión de red de OSI.

**OID: Identificador de Objetos**, son los números de referencia numérica utilizados por el mecanismo interno de base de datos del directorio LDAP . Los nombres de atributos están ahí para tí y para mí, pero los ordenadores son más eficientes cuando tratan con números. Si estás familiarizado con DNS, el concepto es bastante similar -- la mayoría de nosotros utilizamos nombres de máquinas como `www.sendmail.net`, pero los ordenadores traducen el nombre "amigable para el humano" en direcciones IP antes de tragarse el trabajo.

## **P**

### **Paquete**

Agrupamiento lógico de información que incluye un encabezado que contiene información de control y (usualmente) datos del usuario. Los paquetes se utilizan más frecuentemente para hacer referencia a las unidades de datos de las capas de red. Los términos datagrama, frame, mensaje, y segmento también se utilizan para describir agrupamientos de información lógica en diferentes capas del modelo de referencia OSI y en varios círculos de tecnología.

### **PDU (Protocol data unit)**

Unidad de datos del protocolo. Término OSI para paquete.

## **Ping**

Comando que utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección lógica de la capa de red. Es un mecanismo de prueba muy básico.

### **Protocolo**

- Descripción formal de un conjunto de reglas y convenciones que gobiernan la forma en la que los dispositivos de una red intercambian información.
- Campo dentro de un datagrama IP que indica el protocolo de capa superior (Capa 4) que envía el datagrama.

### **Proxy**

Entidad que, a fin de lograr mayor eficiencia, esencialmente suple otra entidad.

### **Puerto**

- Interfaz en un dispositivo de internetworking (tal como un router).
- En la terminología IP, un proceso de capa superior que está recibiendo información de capas más bajas.
- Re-escribir software o microcodificar, de forma tal que correrá en una plataforma de hardware diferente o en un ambiente de software diferente para el que fue diseñado originalmente.
- Un conector hembra en un patch panel que acepta un enchufe del mismo tamaño que una ficha RJ45. Los patch cords se utilizan en estos puertos para interconectar

computadoras cableadas al patch panel. Es esta interconexión la que permite el funcionamiento de una LAN.

## **R**

**RAM** Random Access Memory. Memoria de Acceso Aleatorio. Varios son los tipos de memoria que se usa en las computadoras. La más conocida son las RAM. Se les llama así porque es posible dirigirse directamente a la célula donde se encuentra almacenada la información. Su principal característica es que la información se almacena en ellas provisoriamente, pudiendo ser grabadas una y otra vez, al igual que un CASSETTE de sonido. La memoria RAM se puede comparar a un escritorio, donde se coloca los papeles con que se va a trabajar. Mientras más grande el escritorio más papeles soporta simultáneamente para ser procesados.

**RFC** Request For Comment. Petición de comentarios. Serie de documentos iniciada en 1967 que describe el conjunto de protocolos de Internet. Los RFC son elaborados por la comunidad Internet.

## **Red**

- Conjunto de computadoras, impresoras, routers, switches, y otros dispositivos, que pueden comunicarse entre sí por algún medio de transmisión.
- (network) Comando que asigna una dirección NIC con la cual el router está conectado directamente.

- (network) Comando que especifica cualquier red conectada directamente que será incluida.

### **RMON (Remote Monitoring)**

Monitorización remota. Especificación de agente MIB descrita en RFC 1271 que define las funciones de la monitorización remota de los dispositivos de red. La especificación RMON brinda diversas prestaciones de monitorización, detección de problemas e informes.

### **Router**

Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviará el tráfico de la red. Los routers envían paquetes de una red a otra en base a la información de capa de red. Ocasionalmente llamado gateway (aunque esta definición de gateway va cayendo en desuso día a día).

**Repetidores.-** Dispositivos que generan la señal de un segmento de cable y pasan estas señales a otro segmento de cable sin variar el contenido de la señal. Son utilizados para incrementar la longitud entre conexiones en una Lan.

**Routers.-** Son dispositivos que nos permiten unir varias redes (más de dos, a diferencia de los bridge), tomando como referencia la dirección de red de cada segmento. Al igual que los bridges, los Routers restringen el tráfico local de red permitiendo el flujo de datos a través de ellos solamente cuando los datos son direccionados con esa intención.

**SMI.** Structure of Management Information, Estructura para la información de gestión.

**SGMP.** Simple Gateway Management Protocol, Protocolo Sencillo de Supervisión de Pasarelas.

**SNMP.** Simple Network Management Protocol, Protocolo simple de gestión de red, es un protocolo diseñado para dar al usuario capacidad de manejar remotamente otro ordenador, preguntándole y dándole valores y monitorizando los eventos que ocurren en la red. Está compuesto del MIB, del gestor (manager) y del agente gestionado (agent). SNMP funciona sobre TCP/IP en su nivel de aplicación. Existen dos versiones SNMPV1 y SNMPV2.

**Software.** Esta palabra inglesa que significa "cosa suave", tiene dos significados: (a) uno amplio, de "procedimientos lógicos, para la cooperación armónica de un grupo de personas y máquinas, persiguiendo un objetivo común"; (b) el otro restringido, de programas de computadora, o conjunto de instrucciones, que se pone en la memoria de una computadora para dirigir sus operaciones.

**Seguridad informática.-** son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas.

**Software de administración de red.-** permite al administrador supervisar y controlar los componentes de una red; por ejemplo, permite que el administrador investigue

dispositivos como hosts, enrutadores, conmutadores y puentes para determinar su estado y obtener estadísticas sobre las redes a las que se conectan.

**Switchs.-** Divide la LAN en varios segmentos limitando el tráfico a uno o más segmentos en vez de permitir la difusión de los paquetes por todos los puertos.

### **SMI (Structure of Management Information)**

Estructura de la información de gestión. Documento (RFC 1155) que establece las reglas que se utilizan para definir los objetos administrados en el MIB.

### **Sesión**

Conjunto relacionado de transacciones de comunicación entre dos o más dispositivos de red.

### **Subred**

- En redes IP, red que comparte una dirección de subred particular. Las subredes son redes segmentadas arbitrariamente por un administrador de red para brindar una estructura de enrutamiento multinivel, jerárquico, protegiendo a la subred de la complejidad del direccionamiento de las redes conectadas. Llamada a veces subnet.
- En las redes OSI, grupo de ES e IS bajo el control de un único dominio administrativo que utilizan un mismo protocolo de acceso a la red.

### **T**

**TMN** Telecommunications Management Network. Modelo de gestión de red para redes de telecomunicaciones

**TCP/IP** Transmission Control Protocol / Internet Protocol. Protocolo de Control de Transmisión / Protocolo Internet. Nombre común para una serie de protocolos desarrollados por DARPA en los Estados Unidos en los años 70, para dar soporte a la construcción de redes interconectadas a nivel mundial. TCP corresponde a la capa (LAYER) de transporte del model OSI y ofrece transmisión de datos. El IP corresponde a la capa de red y ofrece servicios de datagramas sin conexión. Su principal característica es comunicar sistemas diferentes. Fueron diseñados inicialmente para ambiente UNIX por Víctor G. Cerf y Robert E. Kahn. El TCP / IP son básicamente dos de los mejores protocolos conocidos.

### **Token Ring**

LAN token passing desarrollada y soportada por IBM. Token Ring corre a 4 ó 16 Mbps por una topología de anillo. Similar a IEEE 802.5.

**TFTP (Trivial File Transfer Protocol):** Versión simplificada de FTP que permite la transferencia de archivos de una computadora a otra por una red

### **TCP (Transmission Control Protocol)**

Protocolos de control de transmisión. Protocolo de la capa de transporte orientado a conexión que provee una confiable transmisión de datos full-duplex. TCP es parte del stack de protocolo TCP/IP.

## **Terminal**

Dispositivo simple donde se pueden ingresar o recuperar datos de una red. En general, las terminales tienen un monitor y un teclado, pero no tienen procesador ni unidad de disco local.

## **Trap**

Mensaje enviado por un agente SNMP a un NMS, consola, o terminal, para indicar la ocurrencia de un evento significativo, como una condición definida específicamente, o un umbral que ha sido alcanzado.

## **U**

### **UDP (User Datagram Protocol, Protocolo de Datagrama de Usuario)**

Protocolo de datagrama de usuario. Protocolo sin conexión de capa de transporte en el stack de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos. UDP se define en la RFC 768.

### **UPS (uninterruptable power supply)**

Sistema de alimentación ininterrumpida. Dispositivo de respaldo diseñado para brindar una fuente de energía sin interrupciones en caso de fallo eléctrico. Comúnmente se los instala en todos los servidores de archivos y en los hubs de cableado.

## **W**

**WAN** Wide Area Network. Red **WAN (wide-area network, Red de Area Ancha)**

Red de área amplia. Red de comunicación de datos que sirve a usuarios ubicados a través de una amplia zona geográfica y a menudo utiliza dispositivos de transmisión suministrados por portadoras comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN.

**WEB** Site. Sitio en el World Wide Web. Conjunto de páginas Web que forman una unidad de presentación, como una revista o libro. Un sitio está formado por una colección de páginas Web.

**WWW**, WEB o W3 World Wide Web. Telaraña mundial. Sistema de arquitectura cliente-servidor para distribución y obtención de información en Internet, basado en hipertexto e hipermedia. Fue creado en el Laboratorio de Física de Energía Nuclear del CERN, en Suiza, en 1991 y ha sido el elemento clave en el desarrollo y masificación del uso de Internet.

## BIBLIOGRAFÍA

### Libros

- STALLINGS William. **SNMP, SNMP v2 and RMON**. Addison Wesley, Primera edición, 1997.
- PHAAL Peter , **Lan Traffic Management**. Prentice-Hall, Primera edición, 1999.
- JAMSA Kris. **Internet Programming**. Oxford Press, Primera edición, 1999.
- MIER E., **Network World, Bell Labs Test Router's Snmp Agents**. July, 1991.
- Stallings W. **SNMP, SNMPv2 and CMIP: The Practical Guide to Network Management Standards**. Addison Wesley, 1993.
- STALLINGS, William. **SNMP, SNMPv2, and RMON : pratical network management, 2nd ed**. Massachusetts, Addison-Wesley, 1996.
- BLACK Uyles, **Network Management Standards, SNMP, CMIP, TMN, MIBs and Object Libraries**. McGraw-Hill,1995.
- FANG Leinwand. **Network Management. A practical perspective**. Addison Wesley, 1993.
- LIMONCELLI Thomas A. and HOGAN Christine. **The Practice of System and Network Administration**. Addison Wesley, 2002.

## **Capitulo II. Introducción a la Gestión En Redes**

<http://www.tid.es/presencia/publicaciones/comsid/esp/articulos/vol61/estba/estba.html>

[http://ares.unimet.edu.ve/electrica/fpie22/GLOSARIO\\_1.htm](http://ares.unimet.edu.ve/electrica/fpie22/GLOSARIO_1.htm)

<http://www.rares.com.ar/PDF/1211.pdf>

<http://www-gris.det.uvigo.es/~mramos/gprsi/gprsi3.pdf>

<http://elisoft.galeon.com/docus/rfc1780.htm>

<http://www.arg.com>

<http://informatica.uv.es/iiguia/2000/R/snmp.ppt>

[http://ciberpol.blogspot.com/2003\\_06\\_15\\_ciberpol\\_archive.html](http://ciberpol.blogspot.com/2003_06_15_ciberpol_archive.html)

<http://www.tango04.es/customerupdate/index.php?customerupdate=2>

<http://jungla.dit.upm.es/~jlopez/publicaciones/telecomid04lopezber.pdf>

## **Capitulo III SNMP**

<http://www.coit.es/publicac/publbit/bit102/quees.htm>

[http://www.zonavirus.com/Detalle\\_Noticia.asp?noticia=63](http://www.zonavirus.com/Detalle_Noticia.asp?noticia=63)

<http://www.tau.org.ar/base/computacion/gsal-19991128-htm/snmp.htm>

<http://www.arrakis.es/~tobal/snmp.htm>

<http://www.ucbcba.edu.bo/carreras/ingsis/cursos/cursodelhaire/snmp.htm>

<http://www.inei.gob.pe/biblioineipub/bancopub/Inf/Lib5009/cap0110.htm>

<http://neutron.ing.ucv.ve/revista-e/No6/Rodriguez%20Edwin/SNMPv3.html>

<http://www.arrakis.es/~gepetto/redes/rog08p1.htm>

[http://pegaso.ls.fi.upm.es/arquitectura\\_redes/transparencias/APDO\\_11\\_14/sld106.htm](http://pegaso.ls.fi.upm.es/arquitectura_redes/transparencias/APDO_11_14/sld106.htm)

<http://informatica.uv.es/iiguia/2000/R/snmp.ppt>

<http://www.snmp.com/FAQs/snmp-faq-part1.txt>

#### **Capitulo IV. RMON**

[http://www.bmas.ja.net/bandwidth\\_management/rmon\\_protocol.html](http://www.bmas.ja.net/bandwidth_management/rmon_protocol.html)

<http://www.netcraftsmen.net/welcher/papers/rmon.htm>

[http://www.eie.fceia.unr.edu.ar/~etapia/Redes2002pub/SNMP\\_RMON.PDF](http://www.eie.fceia.unr.edu.ar/~etapia/Redes2002pub/SNMP_RMON.PDF)

<http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html>

[http://web.madritel.es/personales3/edcollado/openview/OV\\_Configuracion.htm](http://web.madritel.es/personales3/edcollado/openview/OV_Configuracion.htm)

<http://www.softland.com.ar/info/nt/solarwinds/Tools/Engineer/index.htm>

#### **Capitulo V y VI. Herramientas de Monitoreo Remoto**

<http://neutron.ing.ucv.ve/revista-e/No6/Rodriguez%20Edwin/SNMPv3.html>

<http://www.matuk.com/teclado/1991/sep-30-1991.html>

<http://www.enterasys.com/la/switching/matrix/matrix.pdf>

<http://www.ebizlatam.com/noticias/wmview.php?ArtID=1770>

[http://tecun.cimex.com.cu/tecun/software/Soporte tecnico Redes/Enterasys/Generales/Netsight.pdf](http://tecun.cimex.com.cu/tecun/software/Soporte_tecnico_Redes/Enterasys/Generales/Netsight.pdf)

<http://eduangi.com/documentos/HPOpenView.pdf>

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

[http://www.bmc.com/products/proddocview/0,2832,19052 19429 2064403 9548,00.html](http://www.bmc.com/products/proddocview/0,2832,19052_19429_2064403_9548,00.html)

[http://www.bmc.com/products/proddocview/0,2832,19052 19429 26259 8475,00.html](http://www.bmc.com/products/proddocview/0,2832,19052_19429_26259_8475,00.html)

## **Glosario**

[http://ares.unimet.edu.ve/electrica/fpie22/GLOSARIO 1.htm](http://ares.unimet.edu.ve/electrica/fpie22/GLOSARIO_1.htm)

## ANEXOS

### Reporte de Alarmas cada 5 minutos

06-Jan-2005

04:25:05

Period:

4:00

to

5:00

Device

Produbanco.Sucursales(Uio):

Itf Produbanco.Sucursales(Uio).Ibarra (Bellsouth):

Output: Downward Threshold Crossing, value = 54.06 Kb/s, threshold = 76.80 Kb/s

Itf Produbanco.Sucursales(Uio).Ibarra (Porta):

Output: Downward Threshold Crossing, value = 54.2 Kb/s, threshold = 76.80 Kb/s

Itf Produbanco.Sucursales(Uio).Loja (Bellsouth):

Output: Upward Threshold Crossing, value = 52.89 Kb/s, threshold = 51.20 Kb/s

Itf Produbanco.Sucursales(Uio).Riobamba (Bellsouth):

Output: Downward Threshold Crossing, value = 49.53 Kb/s, threshold = 76.80 Kb/s

Itf Produbanco.Sucursales(Uio).Riobamba (Porta):

Output: Downward Threshold Crossing, value = 53.61 Kb/s, threshold = 76.80 Kb/s

## Reporte Diario de Novedades en Patrol DashBoard

Network

From Thu 07 Oct 2004 to Wed 05 Jan 2005

Devices: Workload IP No Route Drops CPU load Memory usage Volume In  
Volume Out Non Unicast Unavailability Unreachability

Servers: Server CPU load Server VRAM Server Disk Usage

Interfaces: Volume In Volume Out Input Utilization Output Utilization  
CommunicationTime Drops Collisions Errors Physical Errors CRC Errors\_LAN  
CRC Errors\_WAN Non Unicast Unavailability

Dlcis: Volume In Volume Out Input Utilization Output Utilization Congestion  
Unavailability

|                                     |             |                |                 |                              |                                                |   |
|-------------------------------------|-------------|----------------|-----------------|------------------------------|------------------------------------------------|---|
| Top                                 |             |                |                 |                              |                                                |   |
| Workload                            | Devices     |                |                 |                              |                                                |   |
|                                     | Volumes     |                |                 | Trends                       |                                                |   |
|                                     | Daily Value | Weekly Average | Monthly Average | Short Term (Trends by Month) | Long Term (Trends by Month, Time to Threshold) |   |
| Objects                             |             |                |                 |                              |                                                |   |
| <u>Produbanco.ER16</u>              | 20695pps    | 15429pps       | 17131pps        |                              | —                                              | — |
| <u>Produbanco.Sucursales(Uio)</u>   | 804pps      | 537pps         | 570pps          |                              | —                                              | — |
| <u>Produbanco.Suc.Agencias(Gye)</u> | 587pps      | 385pps         | 369pps          |                              | —                                              | — |
| <u>Produbanco.Suc.Ambato</u>        | 76pps       | 50pps          | 48pps           |                              | —                                              | — |
| Top                                 |             |                |                 |                              |                                                |   |
| IP No Route                         | Devices     |                |                 |                              |                                                |   |
|                                     | Volumes     |                |                 | Trends                       |                                                |   |
|                                     | Daily Value | Weekly Average | Monthly Average | Short Term (Trends by Month) | Long Term (Trends by Month, Time to Threshold) |   |
| Objects                             |             |                |                 |                              |                                                |   |
| <u>Produbanco.Sucursales(Uio)</u>   | 0%          | 0%             | 0%              | —                            | —                                              | — |
| <u>Produbanco.Suc.Ambato</u>        | 0%          | 0%             | 0.01%           |                              | —                                              | — |
| <u>Produbanco.Suc.Agencias(Gye)</u> | 0%          | 0%             | 0.01%           | —                            | —                                              | — |

| Top                                 |             |                |                 |                              |                                                |   |
|-------------------------------------|-------------|----------------|-----------------|------------------------------|------------------------------------------------|---|
| Drops                               |             | Devices        |                 |                              |                                                |   |
| Objects                             | Volumes     |                |                 | Trends                       |                                                |   |
|                                     | Daily Value | Weekly Average | Monthly Average | Short Term (Trends by Month) | Long Term (Trends by Month, Time to Threshold) |   |
| <u>Produbanco.ER16</u>              | 0%          | 0%             | 0%              | —                            | —                                              | — |
| <u>Produbanco.Sucursales(Uio)</u>   | 0%          | 0%             | 0%              | —                            | —                                              | — |
| <u>Produbanco.Suc.Ambato</u>        | 0%          | 0%             | 0%              | —                            | —                                              | — |
| <u>Produbanco.Suc.Agencias(Gye)</u> | 0%          | 0%             | 0%              | —                            | —                                              | — |

| Top                                 |             |                |                 |                                                                                       |                                                |   |
|-------------------------------------|-------------|----------------|-----------------|---------------------------------------------------------------------------------------|------------------------------------------------|---|
| CPU load                            |             | Devices        |                 |                                                                                       |                                                |   |
| Objects                             | Volumes     |                |                 | Trends                                                                                |                                                |   |
|                                     | Daily Value | Weekly Average | Monthly Average | Short Term (Trends by Month)                                                          | Long Term (Trends by Month, Time to Threshold) |   |
| <u>Produbanco.ER16</u>              | 7.25%       | 6.41%          | 6.60%           |  | —                                              | — |
| <u>Produbanco.Sucursales(Uio)</u>   | 0%          | 0%             | 1.03%           | —                                                                                     | —                                              | — |
| <u>Produbanco.Suc.Ambato</u>        | 0%          | 0%             | 0%              | —                                                                                     | —                                              | — |
| <u>Produbanco.Suc.Agencias(Gye)</u> | 0%          | 0%             | 0.19%           | —                                                                                     | —                                              | — |

| Top                                 |             |                |                 |                                                                                       |                                                |   |
|-------------------------------------|-------------|----------------|-----------------|---------------------------------------------------------------------------------------|------------------------------------------------|---|
| Memory usage                        |             | Devices        |                 |                                                                                       |                                                |   |
| Objects                             | Volumes     |                |                 | Trends                                                                                |                                                |   |
|                                     | Daily Value | Weekly Average | Monthly Average | Short Term (Trends by Month)                                                          | Long Term (Trends by Month, Time to Threshold) |   |
| <u>Produbanco.ER16</u>              | 17.41%      | 17.35%         | 17.34%          |  | —                                              | — |
| <u>Produbanco.Sucursales(Uio)</u>   | 5.95%       | 5.73%          | 5.67%           |  | —                                              | — |
| <u>Produbanco.Suc.Agencias(Gye)</u> | 5.05%       | 4.82%          | 4.79%           |  | —                                              | — |
| <u>Produbanco.Suc.Ambato</u>        | 3.63%       | 3.60%          | 3.60%           |  | —                                              | — |

| Top                               |             |                |                 |                                                                                       |                                                |   |
|-----------------------------------|-------------|----------------|-----------------|---------------------------------------------------------------------------------------|------------------------------------------------|---|
| Server CPU load                   |             | Servers        |                 |                                                                                       |                                                |   |
| Objects                           | Volumes     |                |                 | Trends                                                                                |                                                |   |
|                                   | Daily Value | Weekly Average | Monthly Average | Short Term (Trends by Month)                                                          | Long Term (Trends by Month, Time to Threshold) |   |
| <u>Produbanco.uiomatri-moni01</u> | 46.59%      | 46.69%         | 42.97%          |  | —                                              | — |
| <u>Produbanco.uiomatri-mana01</u> | 7.27%       | 4.04%          | 4.04%           | —                                                                                     | —                                              | — |
| <u>Produbanco.uiomatri-bach01</u> | 5.19%       | 4.12%          | 4.65%           | —                                                                                     | —                                              | — |

| Server VRAM                         |             | Servers        |                 |            |             |    |  |
|-------------------------------------|-------------|----------------|-----------------|------------|-------------|----|--|
| Objects                             | Volumes     |                |                 | Trends     |             |    |  |
|                                     |             |                |                 | Short Term | Long Term   |    |  |
|                                     |             |                |                 | (Trends    | (Trends     | by |  |
|                                     |             |                |                 | Month)     | Month, Time | to |  |
|                                     | Daily Value | Weekly Average | Monthly Average | by         | Threshold)  |    |  |
| <u>Produbanco.uiomatri-moni01</u>   | 0%          | 0%             | 0.01%           | —          | —           |    |  |
| <u>Produbanco.uiomatri-mana01</u>   | 0%          | 0%             | 0%              | —          | —           |    |  |
| <u>Produbanco.uiomatri-bach01</u>   | 0%          | 0%             | 0%              | —          | —           |    |  |
| Top                                 |             |                |                 |            |             |    |  |
| Server Disk Usage                   |             | Servers        |                 |            |             |    |  |
| Objects                             | Volumes     |                |                 | Trends     |             |    |  |
|                                     |             |                |                 | Short Term | Long Term   |    |  |
|                                     |             |                |                 | (Trends    | (Trends     | by |  |
|                                     |             |                |                 | Month)     | Month, Time | to |  |
|                                     | Daily Value | Weekly Average | Monthly Average | by         | Threshold)  |    |  |
| <u>Produbanco.uiomatri-mana01</u>   | 66%         | 66.01%         | 66.01%          | —          | —           |    |  |
| <u>Produbanco.uiomatri-bach01</u>   | 21%         | 20.74%         | 20.37%          | —          | —           |    |  |
| <u>Produbanco.uiomatri-moni01</u>   | 20%         | 20%            | 20%             | →          | —           |    |  |
| Top                                 |             |                |                 |            |             |    |  |
| Volume In                           |             | Devices        |                 |            |             |    |  |
| Objects                             | Volumes     |                |                 | Trends     |             |    |  |
|                                     |             |                |                 | Short Term | Long Term   |    |  |
|                                     |             |                |                 | (Trends    | (Trends     | by |  |
|                                     |             |                |                 | Month)     | Month, Time | to |  |
|                                     | Daily Value | Weekly Average | Monthly Average | by         | Threshold)  |    |  |
| <u>Produbanco.ER16</u>              | 1321GB      | 844GB          | 957GB           | ↓          | —           |    |  |
| <u>Produbanco.Sucursales(Uio)</u>   | 14.68GB     | 10.42GB        | 33.58GB         | ↗          | —           |    |  |
| <u>Produbanco.Suc.Agencias(Gye)</u> | 9.55GB      | 7.89GB         | 6.47GB          | ↑          | —           |    |  |
| <u>Produbanco.Suc.Ambato</u>        | 1.20GB      | 1.43GB         | 1.02GB          | ↑          | —           |    |  |
| Top                                 |             |                |                 |            |             |    |  |
| Volume Out                          |             | Devices        |                 |            |             |    |  |
| Objects                             | Volumes     |                |                 | Trends     |             |    |  |
|                                     |             |                |                 | Short Term | Long Term   |    |  |
|                                     |             |                |                 | (Trends    | (Trends     | by |  |
|                                     |             |                |                 | Month)     | Month, Time | to |  |
|                                     | Daily Value | Weekly Average | Monthly Average | by         | Threshold)  |    |  |
| <u>Produbanco.ER16</u>              | 1331GB      | 920GB          | 1019GB          | ↘          | —           |    |  |
| <u>Produbanco.Sucursales(Uio)</u>   | 14.65GB     | 10.38GB        | 32.51GB         | ↗          | —           |    |  |
| <u>Produbanco.Suc.Agencias(Gye)</u> | 9.59GB      | 8.46GB         | 6.61GB          | ↑          | —           |    |  |
| <u>Produbanco.Suc.Ambato</u>        | 1.20GB      | 1.77GB         | 1.11GB          | ↑          | —           |    |  |

## Legend

**Label** The label of the object (Network, Domain or Device) on which the report is done

**Daily Report** The date when the trends report is generated  
**Period** The period used to compute trends

**Short term calculation** 2 weeks trend calculation period  
**Short term delta** The monthly delta value relative to the short term trend value  
**Short Time to threshold** Forecast: time when threshold be crossed (relative to short term trend value)

**Long term calculation** 13 weeks trend calculation period  
**Long term delta** The monthly delta value relative to the long term trend value  
**Long Time to threshold** Forecast: time when threshold be crossed (relative to long term trend value)

**Blue color values** Aggregated values (domain or device)  
**Salmon color values** Values used to sort an Indicator results table

**Trends by month**  : more than 45%

 : between 15% and 45%

 : between 5% and 15%

 : between -5% and 5%

 : between -50% and -5%

 : less than -50%