VNIVERSIDAD NACIONAL AVTNOMA DE MEXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

SISTEMA DE MONITOREO DEL ORACLE SUN BLADE 6000 MEDIANTE EL PROTOCOLO SNMP Y LA HERRAMIENTA MRTG.

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERA EN COMPUTACIÓN

PRESENTA

ELIZABETH RUBIO MEJÍA

ASESORA

ING. MA. ALEJANDRA ZÚÑIGA MEDEL

SINODALES

M.C. MA. JAQUELINA LÓPEZ BARRIENTOS

M.C. CINTIA QUEZADA REYES

DRA. ANA MARÍA VAZQUEZ VARGAS

ING. TANYA ITZEL ARTEAGA RICCI

MÉXICO DF ABRIL 2012

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS.

Agradezco a Dios por permitirme llegar a este inicio de mi vida profesional, por darme la fortaleza durante la elaboración de este proyecto y por poner a mi lado a personas tan valiosas que me brindaron su apoyo y conocimiento.

Estoy infinitamente agradecida con mis padres: el MVZ Omar Rubio Roa y la Sra. Olga Mejía Velázquez por todo el apoyo, paciencia, tiempo, comprensión, dinero y esperanza que pusieron en mi, me considero bendecida por tener unos padres como ustedes que inculcaron en mi cualidades como la perseverancia y la paciencia.

A mis hermanas Adalyz, Edith y Olga Rubio Mejía, les doy las gracias por creer en mí, por permanecer siempre a mi lado y apoyarme en todo lo que se necesitara. Gracias por escucharme, aconsejarme, regañarme, exigirme a lo largo de toda mi vida para ser una mejor persona cada día.

Mil gracias a José Antonio Trujillo González quien fue mi compañero y confidente a lo largo de la carrera, agradezco su apoyo incondicional para lograr que este sueño se hiciera realidad.

Todo este trabajo no hubiera sido posible sin la dirección de una excelente Ingeniera en Computación de nombre Alejandra Zúniga Medel, gracias por darme el honor de ser su primera tesista, por la confianza y paciencia que me brindó y por pemitirme vivir toda esta experiencia a su lado.

Agradezco a mis sinodales y maestras: M.C. Ma. Jaquelina López Barrientos, M.C. Cintia Quezada Reyes, Ing. Tanya Itzel Arteaga Ricci y la Dra. Ana María Vázquez Vargas, quienes tienen una enorme pasión por su carrera y sobre todo una gran vocación por la enseñanza.

Quiero hacer una mención especial al Centro Nacional de Prevención de Desastres, organismo que me dió todo el apoyo para realizar la tesis, permitiéndome el acceso a sus instalaciones y a sus equipos, mediante el privilegio de ser su tesista.

Por ultimo y no menos importante gracias a la Universidad Nacional Autónoma de México por ser mi máxima casa de estudios, pero en especial gracias a la Facultad de Ingeniería por darme el privilegio de pertenecer a ella y vivir una de las experiencias más grande, satisfactoria y alegre de mi vida.

ÍNDICE

ÍNDICE DE FIGURAS.

ÍNDICE DE TABLAS

INTRODUCCIÓN

INTRODUCCIÓN

El Centro Nacional de Prevención de Desastres (CENAPRED) realiza actividades de investigación, capacitación, instrumentación y difusión acerca de fenómenos naturales y antropogénicos que pueden originar situaciones de desastre, así como acciones para reducir y mitigar los efectos negativos de tales fenómenos, para coadyuvar a una mejor preparación de la población para enfrentarlos. [35]

Dentro de la organización y estructura del CENAPRED se encuentra el área de Sistemas de Información Sobre Riesgo, encargada de colaborar en la generación de información geoespacial sobre peligros, vulnerabilidad y riesgos que se origina en el CENAPRED con el fin de integrar el Atlas Nacional de Riesgos (ANR), mediante un Sistema Integral de Información sobre Riesgo de Desastre (Siiride) cuyos resultados ayuden a las autoridades de Protección Civil a establecer políticas efectivas de prevención y mitigación. [34]

El área de Sistemas de Información Sobre Riesgo cuenta con el servidor ORACLE-SUN Blade 6000, donde se almacena la siguiente información:

- Base de datos que contiene capas de información sobre los peligros hidrometeorológicos, geológicos y químicos.
- Información sobre indicadores socioeconómicos e imágenes satelitales con diferentes coberturas a nivel nacional
- Portal web del Atlas Nacional de Riesgos.
- SAVER (Sistema de Análisis y Visualización de Escenarios de Riesgo), el cual es de suma importancia para el análisis de los diferentes escenarios de sismos, inundaciones, trayectorias de ciclones, entre otros y su afectación a diferentes sistemas expuestos (infraestructura de vivienda, población, carreteras, presas, puentes, infraestructura económica.) para la toma de decisiones de diferentes niveles políticos, así como diversos sistemas en colaboración con otras instituciones como CONABIO (Comisión Nacional para el Conocimiento y Uso de la Biodiversidad), INFONAVIT (Instituto del Fondo Nacional de la Vivienda para los Trabajadores), INE (Instituto Nacional de Ecología) e IMTA (Instituto Mexicano de Tecnología del Agua).

Debido a la importancia de la información que resguarda el servidor ORACLE-SUN Blade 6000, es necesario tener un sistema de monitoreo que sea capaz de mostrar datos gráficos referentes al hardware y software de dicho dispositivo, algunos ejemplos son: el tráfico que circula por las tarjetas de red, el número de peticiones recibidas y contestadas, el uso de memoria RAM, el tráfico web, entre otras.

Este sistema también debe contar con la habilidad de poder enviar alertas vía mail con el fin de prevenir al administrador sobre algún evento inesperado en el servidor.

Con el sistema de monitoreo se obtendrían los siguientes beneficios:

- Prevenir, detectar y corregir errores que se pudiesen presentar.
- Analizar el comportamiento del servidor a través del tiempo.

- Controlar el ORACLE-SUN Blade y la infraestructura física que lo soporta.
- Recibir informes sobre el estado del servidor en cualquier parte del mundo.

A grandes rasgos lo que se pretende es generar un sistema de monitoreo económico, eficiente, de fácil interpretación y manejo simple.

Por razones de seguridad, en el presente trabajo se modificaron los nombres y las direcciones IP de los servidores.

OBJETIVOS

OBJETIVOS

Objetivo general

Planear, organizar, integrar, dirigir y controlar un sistema de monitoreo del servidor ORACLE-SUN Blade 6000, a través del protocolo SNMP y la herramienta MRTG, con el fin de solucionar problemas de red, problemas de software y/o problemas de hardware que se presenten, permitiendo tomar las medidas necesarias para disminuir el impacto en caso de falla de los sistemas, así como reducir el tiempo de localización de errores.

Objetivos específicos

- Crear un sistema de monitoreo gráfico, amigable y fácil de interpretar.
- Graficar el comportamiento de la temperatura de los procesadores, el tráfico web, la carga del CPU, la memoria RAM y el tráfico en las tarjetas de red.
- Montar el sistema de monitoreo en una página web, donde se pueda observar el comportamiento de las variables de hardware y software que se mencionaron en el punto anterior.
- Enviar alertas SNMP a cualquier correo electrónico que se desee cuando ocurran eventos inesperados en el servidor ORACLE-SUN Blade 6000.

CAPÍTULO 1.

Conceptos básicos de redes de datos

1. CONCEPTOS BÁSICOS DE REDES DE DATOS

En este capítulo se narra brevemente la historia de las redes de datos y las aportaciones más importantes dentro del mundo de telecomunicaciones que causaron un gran avance y cambio en la humanidad.

Por otra parte, se dan a conocer las definiciones fundamentales dentro de las redes de datos, se describirá la forma en que se comunican y los elementos necesarios para que la comunicación se pueda lograr.

Una red crea múltiples beneficios en la vida actual, éste tema también será abordado en este capítulo, así como las diversas clasificaciones que se tienen de las redes según su topología, su cobertura geográfica, tecnología de transmisión, entre otras.

Las redes, al igual que todo lo creado por el ser humano están regidas por organismos de estandarización, los cuales permiten que equipos con diferente hardware y software puedan comunicarse entre sí.

Además de los organismos de estandarización, existen dos tipos básicos de modelos para las comunicaciones de red, los cuales son: modelos de protocolo y modelos de referencia. Sin embargo, antes de describir su funcionamiento, se debe comenzar con el proceso de comunicación.

1.1. Breve historia de las redes de datos

La historia de la red comienza a principios del siglo XIX en Suecia y Francia, donde se realizó el primer intento de establecer una red que cumpliera con dos requisitos fundamentales: abarcar al menos un territorio nacional y ser estable. A esta red se le denominó telégrafo óptico y consistía en torres, similares a los molinos, con una serie de brazos que codificaban la información según las distintas posiciones que adoptaban. El sistema se basaba en colocar varias torres en cadena de manera que cada torre repitiera el mensaje de la anterior, haciendo la entrega más veloz que si se hubiese enviado mediante un mensajero a caballo. [24]

Estos telégrafos ópticos fueron la base de algunas técnicas que posteriormente se utilizaron en transmisiones digitales y analógicas como la recuperación de errores, compresión de información, técnicas de cifrado, entre otras.

El siguiente invento que impresionó a la humanidad y dio un giro positivo a las comunicaciones fue el teléfono, inventado por Antonio Meucci alrededor del año 1854. Meucci construyó el teléfono al que llamó teletrófono con el fin de cubrir la necesidad de comunicarse desde su oficina al dormitorio de su esposa debido a que ella padecía de reumatismo. Antonio carecía del dinero suficiente para patentar su invento, por lo que decidió presentárselo a una empresa donde no le dieron importancia alguna, sin embargo, se quedaron con su material. Aún no se sabe exactamente cómo fue que la documentación del teléfono llegó a manos de Alexander Graham Bell, quien registró la patente del teléfono en 1876, razón por la cual se creía que él lo había inventado. Fue hasta el 11 de junio del 2002 cuando el Boletín Oficial de la Cámara de

Representantes de los EE.UU. publicó la Resolución Nº 269 en la que se reconoce que fue Meucci antes que Graham Bell quien inventó el teléfono.

Con la creación de este invento se logró establecer la primera red telefónica en los alrededores de Boston, su primer éxito fue cuando, tras un choque de trenes, se utilizó el teléfono para reportar el accidente y llamar a algunos doctores que acudieron inmediatamente.

El método de telefonía más habitual es la conmutación de circuitos, donde se establece un circuito físico entre los habitantes. Además de éste tipo de conmutación, existe la conmutación de paquetes, la cual permite a varios usuarios compartir la misma conexión. Estos dos tipos de conmutaciones se explican a detalle más adelante en el tema 1.7.1.

El establecimiento de las redes de conmutación de paquetes en los 60´s llegó a marcar la historia de las redes porque era un método que permitía fragmentar los mensajes en paquetes, los encaminaba hacia su destino, y los ensamblaba una vez que llegan a este.

La primera red experimental de conmutación de paquetes se usó en el Reino Unido en los NPL (National Physics Laboratories, Laboratorios Nacionales de Física) fue hasta el año de 1969 que llegó a los EE.UU, donde fue utilizada por la ARPA (Advanced Research Projects Agency, Agencia de Investigación de Proyectos Avanzados), organismo creado en 1957, afiliado al departamento de defensa para impulsar el desarrollo tecnológico.

ARPA estaba interesada en la tecnología desde el punto de vista de la defensa nacional, deseaba crear un sistema de comunicaciones donde no hubiera ningún punto central de mando y control, es decir un sistema donde ningún punto fuera indispensable para la red, obteniendo como beneficio una red totalmente independiente, si algún nodo cayera, esto no afectaría a la red. La corporación Rand aconsejó la creación de esta red en 1962.

En 1967 La ARPA convoca una reunión en Michigan en la que se debate por primera vez las características sobre la futura red ARPANET (Advanced Research Projects Agency Network, Red de la Agencia de Investigación de Proyectos Avanzados), donde se acordó convocar a empresas y universidades para que propusieran diseños para construir una red. La universidad de California ganó la propuesta del centro de administración de red y la empresa Bolt Beraneck and Newman Inc. ganó el concurso de adjudicación para el desarrollo de la tecnología de conmutación de paquetes mediante la implementación de IMP (Interface Message Processor, Procesador de la interfaz de mensaje), los cuales implementaban la técnica de almacenar y reenviar, utilizando un modem telefónico para poder conectarse a otros equipos.

La primera red de computadoras de la historia denominada ARPANET se construyó en 1969, la cual estaba compuesta por cuatro nodos situados en la UCLA (Universidad de California Los Ángeles), SRI (Instituto de Investigación de Stanford),la UCBS (Universidad de California de Santa Bárbara) y El Departamento Gráfico de la Universidad de Utah. La primera comunicación se produjo entre UCLA e SRI el 20 de octubre de 1969, Ese mismo año la Universidad de Michigan creo una red basada en conmutación de paquetes con un protocolo llamado X.35, el objetivo de esta red era mantener la comunicación entre profesores y alumnos. También se empezaron a editar los primeros RFC (Peticiones de comentarios), que son un conjunto de documentos que

describen, especifican y asisten en la implementación, estandarización y discusión de las redes en general. [24]

ARPANET utilizaba el protocolo Host-to-Host, al cual se le denominada NCP (Network Control Protocol, Protocolo de Control de Redes), creado en 1970. NCP fue utilizado durante los años setenta en Internet y es el predecesor del protocolo TCP/IP que es el que actualmente se utiliza en toda la red.

A principios de la década de los 70´s, además del gran logro de crear la red ARPANET, se crearon las primeras LAN propietarias. [71]

En el año de 1973 se realizó la primera conexión internacional de la ARPANET con el colegio universitario de Londres. A mediados de 1973 la universidad de Stanford comenzó a emitir noticias a través de la ARPANET de manera permanente.

La publicación de la propuesta del protocolo de comunicación TCP/IP fue realizada en 1974, pero no fue hasta el 1 de enero de 1983 que todas las máquinas vinculadas con ARPANET utilizaron el TCP/IP. De esta manera se estandariza la comunicación entre las máquinas y todos los equipos que se conecten lo pueden hacer con la garantía de que su compatibilidad será total.

A finales de los años setenta, la NSF (National Science Foundation, Fundación Nacional de Ciencia) se interesó por ARPANET. La NSF se percató del importante potencial que la red tenía para la investigación científica y actuó en dos líneas: de un lado, proporcionar conexión a Internet a todas las universidades, y, en segundo lugar, a mediados de los ochenta constituyó un centro con cinco supercomputadoras interconectadas que sirvieron para construir lo que se conoce como el backbone, la espina dorsal de Internet. [71]

La llegada de las primeras tecnologías estándares de LAN fue en 1980 con Ethernet y en 1985 con Token Ring y FDDI (Fiber Distribute Data Interface, Interfaz de Datos Distribuidos por Fibra). [71]

El año de 1990 dejó marcado la historia de las redes ya que ARPANET dejó de existir debido a que Internet se consolidó y definió como una Red de redes, llegando a obtener más de 200 millones de usuarios en el año de 1999.

Desde ese entonces se han creado una infinidad de aplicaciones para utilizar en la red con el fin de mejorar la calidad de vida del ser humano. Durante los años 2000-2012 se ha visto un gigantesco crecimiento en las redes de datos y en las tecnologías de la información en general.

Actualmente la tecnología de la información se ha convertido en una forma de vida para el humano mediante la cual puede realizar diferentes actividades como por ejemplo: comunicarse con otra persona a través de texto, audio o video, vigilar su economía mediante la consulta, transferencia o retiro de dinero, consultar libros, revistas, periódicos, entre otras.

1.2. Comunicación de redes de datos

La comunicación sostiene y anima la vida, es el motor y expresión de la actividad social y de la civilización, ha llevado a los pueblos desde el instinto hasta la inspiración, a través de una serie de procesos y sistemas de información, impulsos y control. Desde los tiempos remotos, el hombre

sintió la necesidad de comunicarse y transponer fronteras; por eso surgen: la hoguera en la cima de la montaña, los tambores, las señales óptico-acústicas, los juglares, los narradores, la imprenta, el telégrafo, la radio, el radar, la televisión, la prensa y actualmente la internet. [54]

El concepto de comunicación en su sentido más amplio, se refiere al hecho fundamental del encuentro de los seres vivientes con su medio ambiente o entorno, en otras palabras, los seres vivos se comunican cuando son capaces de recibir información sobre el mundo, la cual provoca una reacción sobre ellos. La comunicación así comprendida constituye una condición de la vida misma, por eso se dice que incomunicarse es morir.

Previo a comenzar cualquier tipo de comunicación se deben de establecer reglas o acuerdos para lograr que el mensaje se envíe y comprenda correctamente. A continuación se muestra una lista de algunas reglas para lograr una buena comunicación, no es necesario que existan todas: [11]

- Emisor y receptor identificados
- Método de comunicación consensuado
- Idioma y gramática comunes
- Velocidad y puntualidad en la entrega de mensaje
- Requisitos de confirmación o acuse de recibo.

1.3. Elementos de la comunicación

El objetivo principal de todo sistema de comunicaciones es intercambiar información entre dos entidades por ejemplo, una llamada telefónica, una carta, mensajería instantánea, una entrevista de trabajo, entre otros.

Todos los métodos de comunicación tienen en común tres elementos. El primer elemento es el emisor o también conocido como origen del mensaje, el cual es el encargado de enviar los mensajes a personas o dispositivos. El segundo elemento de la comunicación es el destino o receptor del mensaje, su función es recibir e interpretar el mensaje que le ha sido enviado. Un tercer elemento llamado canal, está conformado por los medios que proporcionan el camino por el que viaja la información. [15]

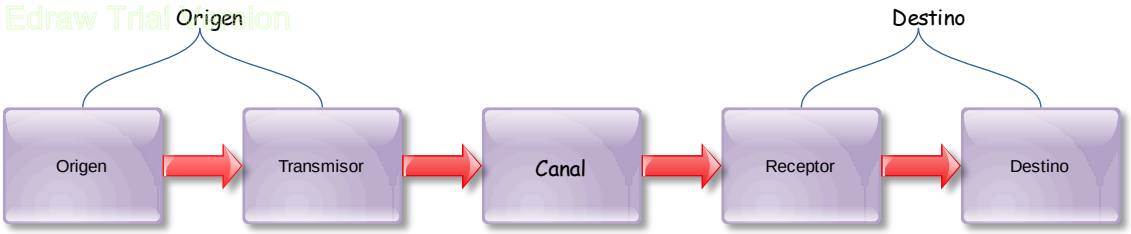


Figura No.1.1-Elementos de la comunicación

En la figura anterior (Ver Figura No.1.1) se muestran dos componentes extras que pertenecen al sistema origen y al destino que son el transmisor y el receptor respectivamente. El transmisor transforma y codifica la información, ya que generalmente esta no se transmite directamente tal y como es generada. Por otro lado el receptor es el que acepta la señal proveniente del canal y la transforma para que pueda ser manejada e interpretada por el destino. [15]

Con esta información se podría concluir que una comunicación simple como un video musical podría enviarse a través de la red desde un origen hacia un destino a través de un canal como un flujo de bits masivo y continuo, sin embargo, esto sería inconveniente e ineficiente ya que provocaría inmensos retrasos en la red y una sobresaturación debido a que ningún otro dispositivo podría enviar o recibir mensajes en la misma red mientras la transferencia estuviese en progreso, en caso de existiera alguna falla en la red, el mensaje se perdería totalmente y se tendría que retransmitir.

La solución al problema anterior es la segmentación, la cual consiste en dividir los datos en partes pequeñas y manejables. Sus principales beneficios son: [11]

- Una red multiuso, lo que significa que se pueden entrelazar diversas conversaciones en la red, a este proceso se le denomina multiplexación.
- El aumento de la confiabilidad de las comunicaciones de red. No es necesario que las partes separadas del mensaje viajen por la misma ruta, se podría decir que cada parte es independiente y busca su mejor ruta, en caso de que alguna ruta falle o se sature, sólo se retransmitirán las partes faltantes.

1.4. Elementos básicos de una red [11]

El término red se refiere a una interconexión de computadoras para compartir información, recursos y servicios, generalmente una red consta de muchas piezas complejas de hardware y software que son coordinadas y controladas por protocolos de red.

Se llama protocolo al conjunto de reglas para el intercambio de información dentro de una red. El protocolo debe permitir:

- Establecer la conexión
- Mantener la conexión
- Iniciar y finalizar el coloquio
- Transferir la información
- Controlar los errores y recuperar los datos.

Los protocolos o reglas, medios, dispositivos y mensajes son los elementos que existen dentro de una red de datos típica tal como lo muestra el diagrama de la Figura No. 1.2.

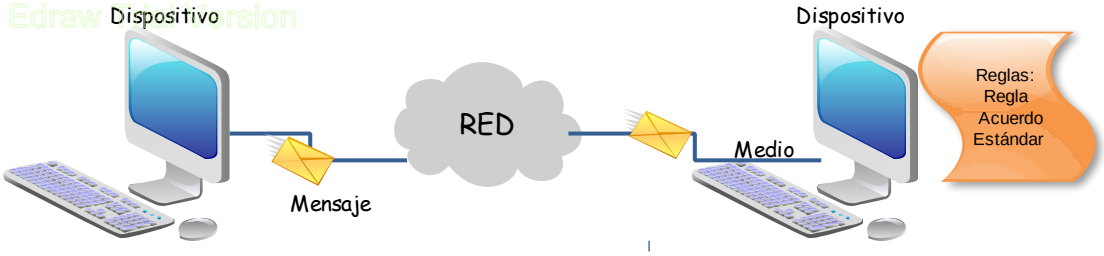


Figura No.1.2-Elementos básicos de una red

Dónde:

Los mensajes refieren a la información que se desee enviar o recibir tales como: páginas webs, e-mails, entre otras formas de comunicación permitidas en internet.

Los dispositivos generalmente son aquellos que originan mensajes que constituyen la comunicación, algunos ejemplos son las computadoras, servidores, teléfonos, routers, entre otros.

Los medios interconectan a los dispositivos ya sea por cable o inalámbricamente. En las conexiones con cables el medio puede ser cobre o fibra óptica. Por otro lado en las conexiones inalámbricas, el medio es la atmósfera de la tierra o espacio.

El último elemento de la red son las reglas o protocolos, que se encargan de gobernar a los dispositivos interconectados a través de medios para proporcionar servicios, con el fin de poderse comunicar entre sí.

1.5. Beneficios y uso de las redes locales

Las redes de datos respaldan la forma en que la humanidad vive, aprende, trabaja y juega, ya que proporciona una plataforma para los servicios que permite conectar en forma local y global, a las familias y amigos, así como también a los integrantes de una empresa.

Es sorprendente la importancia que tienen las redes de datos en la vida diaria, las cuales fueron creadas principalmente para uso militar, posteriormente fueron el transporte de información entre negocios. Actualmente las redes de datos mejoran la calidad de vida de todas las personas ayudándolas en diferentes campos como:

- Consultar el clima
- Buscar la mejor ruta para su destino ya sea en transporte público, caminando o en automóvil, un claro ejemplo es google maps
- Recibir y enviar información mediante correos electrónicos
- Descargar recetas de cocina
- Unir familias que se encuentran en diferentes países mediante la mensajería instantánea (Messenger), redes sociales (Facebook y Twitter) o videollamadas (Skype).
- Transacciones bancarias
- Cajeros automáticos

Las redes de datos renovaron el mundo de la educación con la introducción de cursos en línea, material didáctico, foros de discusión, entre otros. Los métodos de aprendizaje tradicionales proporcionan dos fuentes de conocimiento: el libro de texto y el instructor. Estas fuentes están limitadas tanto en el formato como en la disponibilidad del instructor, es decir, un instructor no está todo el tiempo disponible para resolver los cuestionamientos del alumno. Por el contrario, los cursos en línea cubrieron este tipo de deficiencias en el medio educativo de tal manera que siempre se encuentran disponibles en la red a cualquier hora y en todo lugar, el formato de los libros o dinámicas es mucho más amigable y puede contener voz, video y datos. [11]

En el campo laboral la mayoría de las organizaciones tiene una cantidad significativa de computadoras en operación, las cuales generalmente se encuentran a una distancia considerable, lo que implica que cada computadora debe estar conectada a una misma red con la finalidad de compartir datos y recursos, por ejemplo, llevar un mejor control de inventarios, vigilar la productividad, pagar nóminas, entre otros.

En términos generales, una meta de las redes dentro del campo laboral, es hacer que todos los programas, el equipo y los datos estén disponibles para cualquiera en la red, sin importar la localización física de los recursos y de los usuarios. Otra meta a conseguir es la confiabilidad al contar con fuentes alternativas de suministro, es decir, respaldar la información en dos o tres máquinas diferentes, así, si una no está disponible, podrían usarse las otras copias de la información. [11]

En la actualidad, las redes ofrecen una mayor integración entre funciones y organizaciones relacionadas que la que era posible en el pasado.

Las redes como medio de entretenimiento han tenido un éxito total, lo que a su vez ha provocado que la sociedad interactúe menos entre sí, también ha ocasionado que los niños dejen juegos deportivos por juegos en la red perjudicando su salud y su agilidad física. Por esta razón, hoy en día se han creado consolas de videojuegos que obligan al usuario a moverse físicamente con el fin de que ejercite su cuerpo.

La idea original de las redes como medio de entretenimiento era mejorar la posibilidad de disfrutar y compartir diferentes formas de recreación, sin importar la ubicación.

Internet se utiliza para formas tradicionales de entretenimiento, escuchar artistas grabados, ver avances de películas, leer libros o descargar software son algunas de las acciones que se pueden realizar gracias a internet.

1.6. Topologías de redes

El arreglo físico o lógico en el cual los nodos de una red se interconectan entre sí sobre un medio de comunicación se le llama topología de una red.

La topología de una red define la distribución de cable, es decir, es el mapa de distribución de los medios de interconexión que forman la intranet. [52]

La topología física se refiere al diseño actual del medio de transmisión de la red, la manera en que los nodos están conectados unos con otros. [52]

Por otro lado la topología lógica es el método que se usa para comunicarse con los demás nodos, es decir, la forma de cómo la red reconoce a cada conexión de estación de trabajo.

Las redes de datos se pueden clasificar respecto a su topología, ya sea lógica o física, donde las más comunes son:

1.6.1. Topología Bus

Esta estructura está basada en un canal central único a lo largo del cual se conectan las computadoras que forman la red local (Ver Figura No. 1.3). Este sistema permite la transmisión de datos de una computadora a la vez, estos datos son escuchados por todas las computadoras conectadas al canal central, pero sólo el receptor designado los utiliza. [65]

Ventajas de la topología bus.

- Fácil instalación y extensión.
- Costo más económico de todas las topologías

Desventajas de la topología bus

- Vulnerabilidad a quebraduras de cable, conectores y cortos en el cable muy difíciles de localizar.
- Sólo una computadora a la vez puede transmitir datos por la red.

Edraw Trial Version

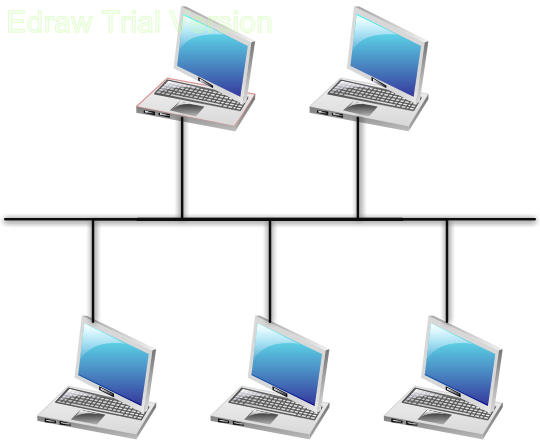


Figura No.1.3-Red en bus

1.6.2. Topología estrella

En esta topología todas las computadoras o estaciones están conectadas a un dispositivo central (Ver Figura No. 1.4), por el cual debe pasar obligatoriamente toda la información de la red, ya que de este dispositivo depende la comunicación entre las estaciones y es el controlador del flujo de datos. [41]

Ventajas de la topología estrella.

- Fácil escalabilidad, lo que significa que la red se puede expandir fácilmente, esto depende del número de puertos disponibles en el dispositivo central.
- En caso de que una estación falle, la red sigue funcionando

Desventajas de la topología estrella.

- En caso de que el dispositivo central falle, toda la red se desconecta

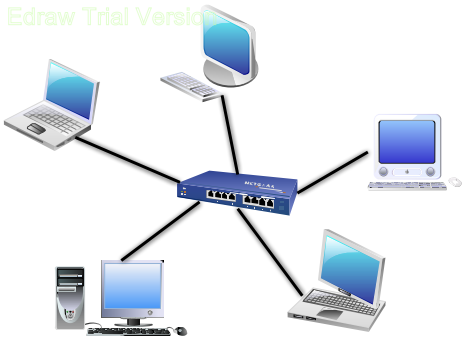


Figura No.1.4-Red en estrella

1.6.3. Topología Anillo

Topología que consiste en la conexión de dispositivos de red uno tras otro sobre el cable en un círculo físico (Ver Figura No. 1.5), es decir, todas las estaciones se conectan a un canal común que se cierra en forma de anillo, de ahí el nombre de topología de anillo. [41]

El funcionamiento de esta topología se basa en que cada computadora retransmite los paquetes que reciben y los envían a la siguiente computadora en red. Cada mensaje enviado por una estación pasa por todas las estaciones que se encuentren entre el emisor y el receptor. Para evitar las colisiones, así como lograr un uso correcto y ordenado del canal se requiere de un token el cual otorga el turno a las computadoras para transmitir datos. El token circula alrededor del anillo, cuando una computadora desea enviar datos, espera al token y se apodera de él para poder transmitir su mensaje. [65]

Ventajas de la topología anillo.

- No existen colisiones debido al control de acceso a los medios que se tiene.
- Permite verificar si se ha recibido un mensaje.

Desventajas de la topología anillo.

- Si una estación o computadora falla, afecta a toda la red.
- Su costo es elevado.

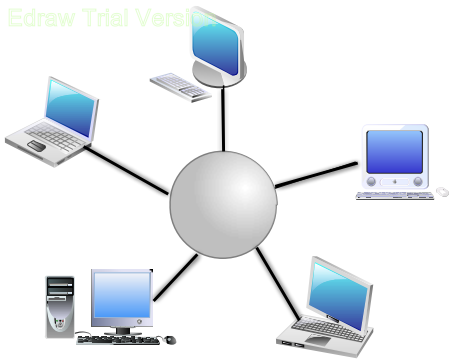


Figura No. 1.5-Red en anillo.

1.6.4. Topología Árbol

Es una topología de red en la que los nodos están colocados en forma de árbol (Ver Figura No. 1.6). Esta topología es similar a una serie de topologías en estrella interconectadas, la diferencia radica en que no existe un nodo central, sin embargo, existe un nodo troncal desde el que se ramifican los demás nodos. [70]

Ventajas de la topología árbol.

- Es muy fácil de expandir
- Mayor alcance de señal

Desventajas de la topología árbol

- Si el nodo troncal se cae, la red se pierde
- La configuración es compleja y difícil.

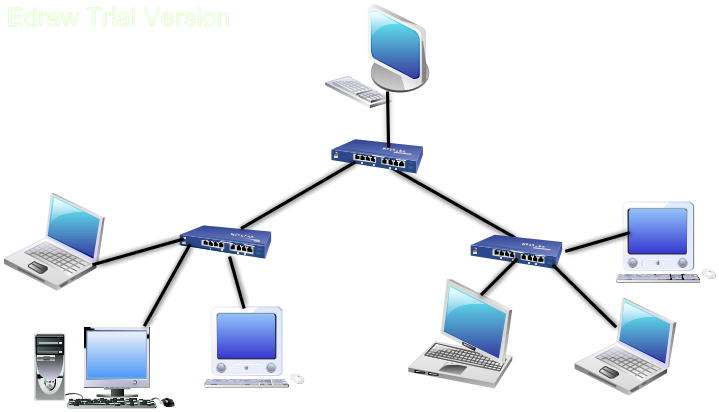


Figura No. 1.6-Topología de árbol

1.6.5. Topología Malla

Una topología de malla conecta cada dispositivo de una red a muchos dispositivos de la red (Ver Figura No. 1.7), ocasionando que los datos desplazados en la red sigan distintas trayectorias a su destino. Estas trayectorias de datos redundantes hacen muy robusta a una red de malla. [70]

Ventajas de la red en malla

- Los mensajes pueden tomar caminos diferentes a su destino
- Si falla un cable, otro cable se hace cargo del tráfico
- Ningún nodo es indispensable para la red
- No existe un nodo central lo que reduce el mantenimiento.

Desventajas de la red en malla

- Es más costosa porque se requiere más cable.
- Sólo funciona con una pequeña cantidad de nodos debido a la gran cantidad de medios necesarios para los enlaces y la cantidad de conexiones con los enlaces.

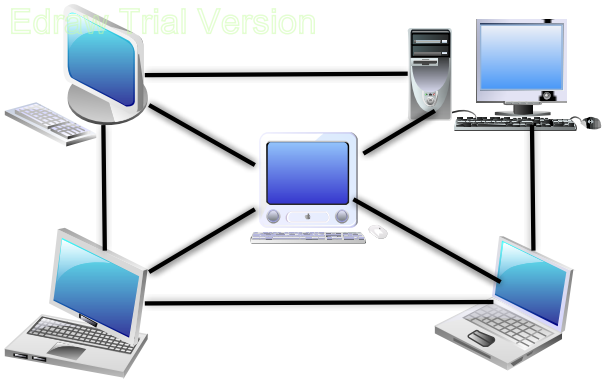

Edraw Trial Version

Figura No. 1.7-Topología de malla

Además de la clasificación de las redes respecto a su topología, existen otras clasificaciones según el área geográfica que abarquen, el tipo de conmutación que utilicen, su velocidad de transmisión, entre otras.

1.7. Evolución de las redes de datos. Principales características: cobertura geográfica, velocidad, redes conmutadas y no conmutadas

A través del tiempo, las redes han evolucionado positivamente, creando un medio de comunicación estable, confiable e íntegro para el ser humano. Dentro de las redes se tienen diferentes tipos de redes de datos, para saber cuál se debe utilizar o qué tipo de red se está empleando, se deben conocer las clasificaciones existentes. Algunas de ellas son las siguientes.

1.7.1 Redes conmutadas y no conmutadas

En una red conmutada, el enlace entre dos terminales de usuario se puede establecer haciendo una solicitud de enlace, tal como lo hace la telefonía clásica. En las redes no conmutadas el enlace es permanente y es alquilado por la empresa ya sea pública o privada. Este tipo de enlaces son de gran utilidad para los usuarios que no pueden aceptar el retardo que lleva establecer una conexión o el bloqueo que puede aparecer si todas las líneas están ocupadas. [18]

Las principales ventajas de una red conmutada son la flexibilidad y el bajo costo de esta, siempre y cuando el volumen de tráfico sea pequeño. Las desventajas de este tipo de red son: baja calidad, tiempo de respuesta largo y pueden llegar a bloquearse. [18]

En el caso de las redes no conmutadas se tienen como beneficios la posibilidad de obtener una red de mayor calidad y libre de bloqueos, así como soportar un mayor volumen de tráfico. El problema con este tipo de redes es que el costo se eleva si se tiene un tráfico pequeño.

Las redes conmutadas pueden utilizar tres técnicas distintas para el establecimiento de los enlaces: la conmutación de circuitos, conmutación de paquetes o conmutación de celdas.

Las redes con conmutación de circuito (RCC) establecen una conexión entre dos equipos terminales de datos. [8] Cada conexión se establecerá durante el tiempo que dialoguen las terminales para intercambiar información mediante una trayectoria bien definida. Cuando la transmisión de datos concluye, la conexión se libera y puede atender nuevas solicitudes de conexión (Ver Figura No. 1.8).

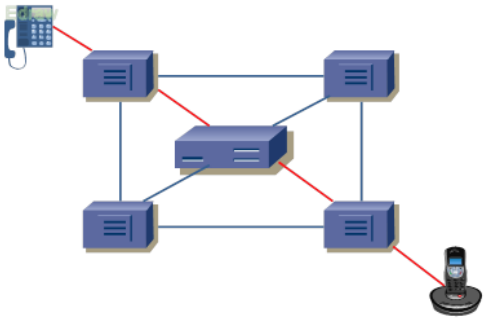


Figura No. 1.8-Ilustración de RCC

La conmutación de paquetes es un método más eficiente de envío de datos ya que las RCC no son capaces de proporcionar conexiones con ancho de banda variable, lo que provoca un uso ineficiente de recursos cuando se requiere un ancho de banda estrecho o la aparición de retardos en la transmisión de datos cuando se necesitan ráfagas de ancho de banda grande. [8]

En la conmutación de paquetes, regularmente no se establece una trayectoria física completa desde el origen hasta el destino en cualquier momento durante la comunicación. Se le llama conmutación de paquetes porque la información total a transmitir se separa en cierto número de paquetes, los cuales esperan su turno para ser enviados (Ver Figura No.1.9). Cada paquete de datos se rotula con la dirección de su destino y la secuencia antes de ser enviado. El extremo receptor se encarga de reensamblar los paquetes en el orden apropiado con ayuda de la secuencia.

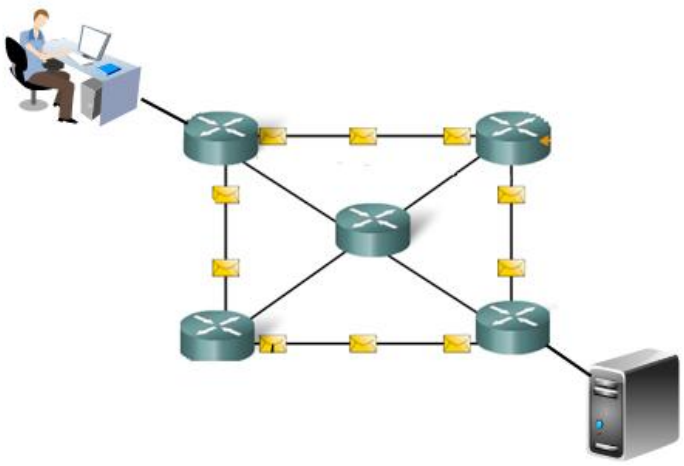


Figura No. 1.9-Conmutación de paquetes.

Existen dos grandes familias dentro de la conmutación de paquetes clásica: [18]

1. Conmutación de paquetes en modo "circuito virtual": El camino que siguen todos los paquetes pertenecientes a una comunicación se determina en su inicio y no varía a los largo de la comunicación tal como en la conmutación de circuitos. [18] Es importante destacar que sólo se determina el camino, no se hace una reserva de recursos como sucedía en la conmutación de circuitos.
2. Conmutación de paquetes en modo "datagrama": El camino que sigue cualquier paquete se determina individualmente, lo que significa que se elige en el momento en que un paquete llega a un nodo intermedio y solamente tiene validez para ese paquete. [16] En otras palabras, cada paquete constituye en sí una comunicación.

La conmutación de celdas consiste en paquetes de longitud pequeña y fija llamados celdas. Debido a su pequeña longitud, permiten un buen aprovechamiento del ancho de banda. Por otro lado, el tamaño fijo de las celdas facilita el uso de técnicas de conmutación muy rápidas. [18]

A continuación se muestra una tabla comparativa con algunas características y diferencias de los distintos tipos de conmutación de red (Ver Tabla No.1.1). [18]

Tabla No.1.1- Comparación de la conmutación de redes

Conmutación de circuitos	**Conmutación de paquetes modo "datagrama"**	**Conmutación de paquetes modo "circuito virtual"**
Circuito dedicado en exclusiva	Circuito compartido	Circuito no dedicado (compartido)
Ancho de banda fijo	Uso dinámico del ancho de banda	Uso dinámico del ancho de banda
Retardo de establecimiento de la conexión	No hay retardo de establecimiento de la conexión	Retardo de establecimiento de la conexión
Retardo bajo y fijo (no hay almacenamiento sólo propagación)	Retardo mayor y variable debido al almacenamiento y conmutación	Retardo mayor y variable.
Ruta establecida inicialmente e invariable	Ruta establecida para cada paquete	Ruta establecida inicialmente e invariable
Fiabilidad alta (sólo desconexiones imprevistas)	Fiabilidad baja (posibles pérdida y desordenamientos de paquetes)	Fiabilidad alta
No existen cabeceras de red durante la conexión	Cabeceras de red grandes en cada paquete	Cabeceras de red más pequeñas en cada paquete
Para tráfico continuo	Para tráfico discontinuo (a ráfagas)	Para tráfico discontinuo

1.7.2. Clasificación de las redes según su tecnología de transmisión

En un sentido amplio, existen dos tipos de tecnologías de transmisión que se utilizan de manera extensa:

1. Las redes de difusión (broadcast) tienen un solo canal de comunicación, por lo tanto, todas las máquinas de la red lo comparten. En el caso de que una estación decida enviar un mensaje, este será recibido por todas las estaciones que se encuentren dentro de la misma red. Cuando una estación recibe un paquete, verifica el campo de dirección en el cual se especifica el destinatario, y si el paquete va destinado hacia esa estación, esta lo procesa, si va destinado a alguna otra, esta lo ignora. Algunos sistemas de difusión también soportan la transmisión a un subconjunto de máquinas, algo conocido como multidifusión (multicasting). [65]
2. Las redes punto a punto constan de muchas conexiones entre pares individuales de estaciones de trabajo. Para ir del origen al destino, un paquete podría tener que visitar primero una o más máquinas intermedias. La transmisión de punto a punto con un emisor y un receptor se conoce como unidifusión (unicasting). [65]

1.7.3. Clasificación de redes según su cobertura

Otra forma de clasificar las redes es mediante su escala. Los sistemas de procesadores múltiples son clasificados por su tamaño físico (Ver Tabla No. 1.2). En la parte superior de la Tabla No.1.2 se muestran las redes de área personal, que están destinadas para una sola persona. Posteriormente se encuentran redes más grandes, las cuales se pueden dividir en redes de área local, de área metropolitana y de área amplia. Por último, la conexión de dos o más redes se conoce como interred.

La Tabla No.1.2 sólo da una idea general de los valores teóricos que deben existir entre los procesadores de una red, sin embargo, en la práctica los valores de distancias son diferentes.

Tabla No. 1.2- Clasificación de procesadores interconectados por escala

Distancia entre procesadores	**Procesadores ubicados en el mismo**	**Ejemplo**
1 m	Metro cuadrado	Red de área personal
10 m	Cuarto	Red de área local
100 m	Edificio	Red de área local
1 km	Campus	Red de área local
10 km	Ciudad	Red de área metropolitana
100 km	País	Red de área amplia
1,000 km	Continente	Red de área amplia
10,000 km	Planeta	Internet

1.7.3.1. LAN (Local Área Network, Red de Área Local)

Una red de área local está constituida por un hardware (cables, terminales, servidores) y un software (acceso al medio, administración de recursos, intercomunicación) que se distribuyen por una extensión limitada (planta, edificio, grupo de edificios) en la que existen una serie de recursos compatibles, a los que tienen acceso los usuarios para compartir información (Ver Figura No. 1.10). [51]

Una red LAN se distingue de otras redes de datos por características como la restricción a un área geográfica limitada, la capacidad que tienen de depender de un canal físico de comunicaciones con una velocidad binaria alta y su reducida tasa de errores.[32]

Además de la cobertura que tiene una LAN, existen otras características importantes tales como: [51]

- La velocidad de transmisión de los datos es elevada, varía de 10 Mbit/s – 10 Gbit/s.
- Su tasa de error de transmisión de datos reducida tiene un orden de 1 bit erróneo por cada 100 millones de bits transmitidos.
- El propietario de la LAN es el encargado de gestionar la red o se puede contratar a un tercero.

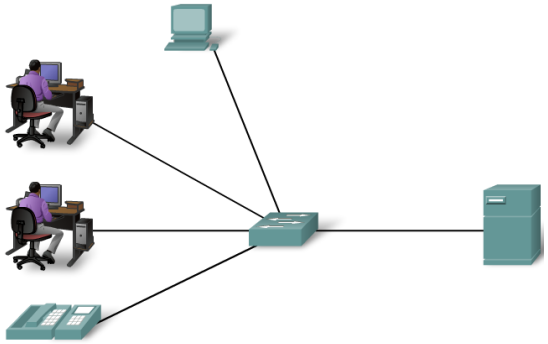


Figura No. 1.10-Red de Área Local (LAN)

1.7.3.2. MAN (Metropolitan Area Network, Red de Área Metropolitana)

Este tipo de redes abarcan una ciudad. (Ver Figura No. 1.11). Una red MAN es una red intermedia entre una LAN y una WAN. Estas redes aparecieron en la década de 1990, eran tecnológicamente avanzadas. El ejemplo más conocido son las redes de televisión por cable disponibles en muchas ciudades. Sus características principales son: [17]

- En sus inicios tenía velocidades de acceso de 30 a 150 Mbit/s, actualmente alcanza hasta los 10Gbit/s.
- Cobertura mediana de 10 a 50 km.
- Las dos tecnologías más empleadas son SMDS (Switched Multi-Megabit Data Service, Servicio de datos conmutado multimegabits) y FDDI (Fiber Distribute Data Interface, Interfaz de Datos Distribuidos por Fibra).

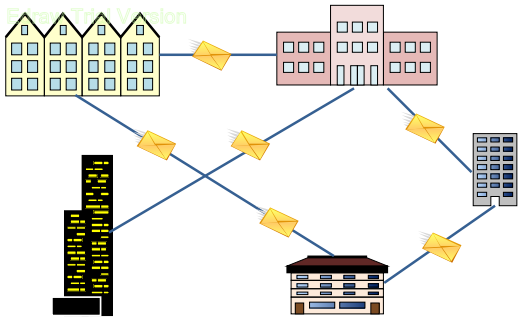


Figura No.1.11-Red de Área Metropolitana (MAN)

1.7.3.3. WAN (Wide Area Network, Red de Área Amplia)

Cuando la cobertura de la red no tiene un límite predefinido, se está hablando de una red de área extendida o WAN, la cual puede llegar a ser tan extensa como sea necesario. Una WAN interconecta redes de área local o metropolitana con el fin de disponer de una alta capacidad de transferencia de datos para que la comunicación entre usuarios sea rápida (Ver Figura No. 1.12). [11]

Las características generales de una WAN son:

- Distancia de cobertura de 100 a 20,000 km.
- La red telefónica tradicional es un claro ejemplo de una red WAN, al igual que Internet.

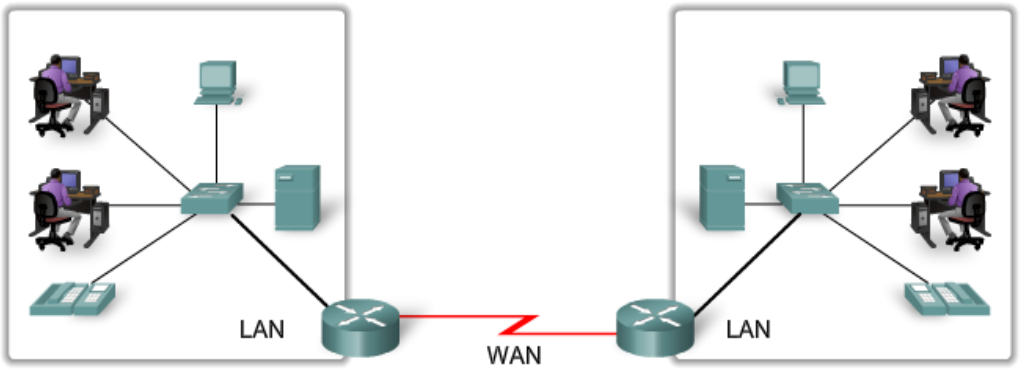


Figura No. 1.12-Red de Área Extendida (WAN)

1.7.4. Redes con procesamiento centralizado, descentralizado y distribuido

Otro aspecto importante de una red de cómputo es el tipo de procesamiento que se maneja en los sistemas que la integran. El tipo de procesamiento influirá principalmente sobre el tipo de tecnología que se utilizará para la implementación de la red. De acuerdo con el tipo de procesamiento las redes pueden ser de procesamiento centralizado, descentralizado o distribuido. [17]

1. Procesamiento centralizado: En una red con este tipo de procesamiento se emplea un sistema de cómputo central, el cual es el encargado de atender todos los requerimientos de las terminales mediante programas de aplicación que este posea. Este procesamiento

ofrece el más alto grado de control, pero tiene como desventaja la degradación de servicio cuando aumenta el número de terminales conectadas al sistema. [17]

2. Procesamiento descentralizado: Los dispositivos de procesamiento se colocan en diversas ubicaciones lejanas. Los sistemas de computación individuales están aislados y no se comunican entre sí. Estos sistemas son convenientes para compañías que tienen divisiones operativas independientes. [66]
3. Procesamiento distribuido: las computadoras se ubican en sitios lejanos pero se conectan entre sí a través de dispositivos de telecomunicaciones. Un beneficio de dicho procesamiento es que la actividad de procesamiento se puede asignar a la ubicación o ubicaciones donde sea posible realizarlo con más eficiencia. [17]

Cualquiera que sea el caso del tipo de red en uso, ésta debe estar regida por organismos que regulen el funcionamiento y el proceso de comunicación de la red.

1.8. Organismos de estandarización

Existen diversos fabricantes y proveedores de redes, cada una con sus propias ideas, si no existiera la coordinación sería un caos total y los usuarios no podrían conseguir nada. La solución a este problema es el acuerdo de la adopción de algunos estándares para las redes.

Los estándares permiten que computadoras diferentes se comuniquen e incrementan el mercado de productos que se ajustan a los estándares.

Existen dos tipos de estándares: [65]

- De facto: Son estándares con gran aceptación en el mercado, establecidos normalmente por grupos de empresas y organizaciones, pero que aún no son oficiales.
- De iure: Son estándares definidos por organizaciones o grupos oficiales.

Los estándares también pueden ser clasificados en dos tipos: abiertos y cerrados. Dentro de los abiertos se encuentran los estándares de facto e iure, ya que pueden ser consultados por cualquiera. No obstante existen organismos que cobran cuota por acceder a sus estándares prohibiendo su distribución. A este tipo de estándares se les denomina estándares de distribución restringida. En el otro extremo se sitúan los estándares cerrados, también denominados propietarios, que representan normas únicamente accesibles para los miembros de la empresa propietaria. [65]

Los estándares abiertos pueden ser definidos por consorcios de fabricantes o por organismos oficiales. [65]

Los consorcios de fabricantes están formados por grupos de empresas que cooperan para establecer acuerdos y reglas que permitan obtener la interoperabilidad de sus productos empleando una tecnología determinada. [65]

Por otra parte, los organismos oficiales están formados por consultores independientes, miembros de los departamentos o secretarías de estado de diferentes países y otros miembros. Los más destacados son los que enseguida se presentan (Ver Figura No. 1.13). [65]

ISO (International Organization for Standardization, Organización Internacional para la Estandarización) es una agencia internacional sin ánimo de lucro cuyo objetivo es el desarrollo de normalizaciones que abarcan un amplio abanico de materias.[9] Esta organización ha definido multitud de estándares de diferentes temáticas, que van desde el paso de los tornillos, hasta arquitecturas de comunicaciones para la interconexión de sistemas. ISO está formada por organismos de estandarización de 162 países y por un grupo de organizaciones observadoras que no poseen la capacidad de votar. A pesar de ser una organización no gubernamental, la mayoría de sus miembros son instituciones gubernamentales. [42]

ITU (International Telecommunication Union), en español Union Internacional de Telecomunicaciones (UIT) es la organización más importante de las Naciones Unidas en lo que concierne a las tecnologías de la información. Esta organización representa un foco global para los gobiernos y el sector privado en el desarrollo de redes y servicios. La UIT coordina el uso del espectro radioeléctrico, promoviendo la cooperación internacional para la asignación de órbitas de satélites, trabajando para mejorar las infraestructuras de comunicación mundiales, estableciendo estándares para la interconexión de un enorme rango de sistemas de comunicación, haciendo frente a problemas actuales como el cambio climático y la seguridad en el ciberespacio.[9] Su sede está en Ginebra (Suiza) y está formada por 191 países y más de 700 entidades del sector privado e instituciones académicas. [19]

Esta organización está compuesta por tres sectores o comités: ITU-R (antes CCIR, Comité Consultivo Internacional de Radiocomunicaciones), que se encarga de promulgar estándares de comunicaciones que emplea el espectro electromagnético. Por otro lado la ITU-D se encarga de la organización, coordinación técnica y actividades de asistencia. El tercer sector es la ITU-T (antes CCITT, Comité Consultivo Internacional de Telegrafía y Telefonía), encargada de desarrollar estándares para la telefonía, la telegrafía, interfaces, redes y otros aspectos de las telecomunicaciones. [65]

IEEE (Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Electricistas y Electrónicos), es la mayor asociación profesional para el avance de la innovación y la excelencia tecnológica en busca del beneficio de la humanidad. IEEE y sus miembros inspiran a una comunidad global que innove hacia un mejor mañana a través de sus publicaciones enormemente citadas, conferencias, estándares tecnológicos, y actividades profesionales y educativas. Fue fundada en 1884 y desde entonces desarrolla estándares para las industrias eléctricas y electrónicas. Desde el punto de vista de las redes de datos son muy interesantes los trabajos del comité 802, que desarrolla estándares de protocolos de comunicaciones para la interfaz física de las conexiones de las redes locales de datos. [65]

ANSI (American National Standars Institute, Instituto Nacional de Normalización Estadounidense) es una organización privada sin fines lucrativos que administra y coordina la normalización voluntaria y las actividades relacionadas a la evaluación de conformidad en los Estados Unidos, la cual fue fundada el 19 de octubre de 1918. La misión del Instituto es mejorar tanto la competitividad mundial de las empresas estadounidenses, así como la calidad de vida estadounidense, promoviendo y facilitando normas voluntarias de consenso y sistemas de evaluación de conformidad, protegiendo su integridad. [33]

ETSI (European Telecommunications Standards Insitute, Instituto Europeo de Normas de Telecomunicaciones), es una organización internacional sin ánimo de lucro abierta, lo que implica que cualquier persona puede participar, su objetivo es contribuir a la ingeniería de Internet, en especial en el transporte, el encaminamiento y la seguridad. Para saber sobre algún tipo de protocolo o servicio de Internet se debe consultar los imprescindibles RFC (Request For Comments). Por ejemplo los RFC para los protocolos de SMTP, MIME, HTTP, HTTPS, POP3, entre otros. [40]

IETF (Internet Engineering Task Force, Fuerza de Trabajo para la Ingeniería de Internet) es una gran comunidad internacional abierta de diseñadores de redes, operadores, vendedores, e investigadores preocupados por la evolución de la arquitectura de internet y su forma de operar. Está compuesto por grupos de trabajos organizados por temas en varias áreas como enrutamiento, transporte y seguridad. Las áreas son gestionadas por los directores de área (AD), que son miembros del grupo IESG (Internet Engineering Steering Group, Grupo de Dirección de Ingeniería de Internet). IANA (Internet Assigned Numbers Authority, Agencia de Asignación de Número de Internet) es el coordinador central para la asignación unívoca de valores a los parámetros de los protocolos de Internet. [65]

Por su parte, México cuenta con la Norma Oficial Mexicana conocida como NOM, la cual se encarga de regular las especificaciones, atributos, características o prescripciones aplicables a un producto, sistema, proceso, instalación, servicio o actividad. Estas normas son de uso obligatorio para quien cae dentro del alcance de la aplicación de las mismas y cuando los productos se hagan durante la vigencia de la misma. [39]

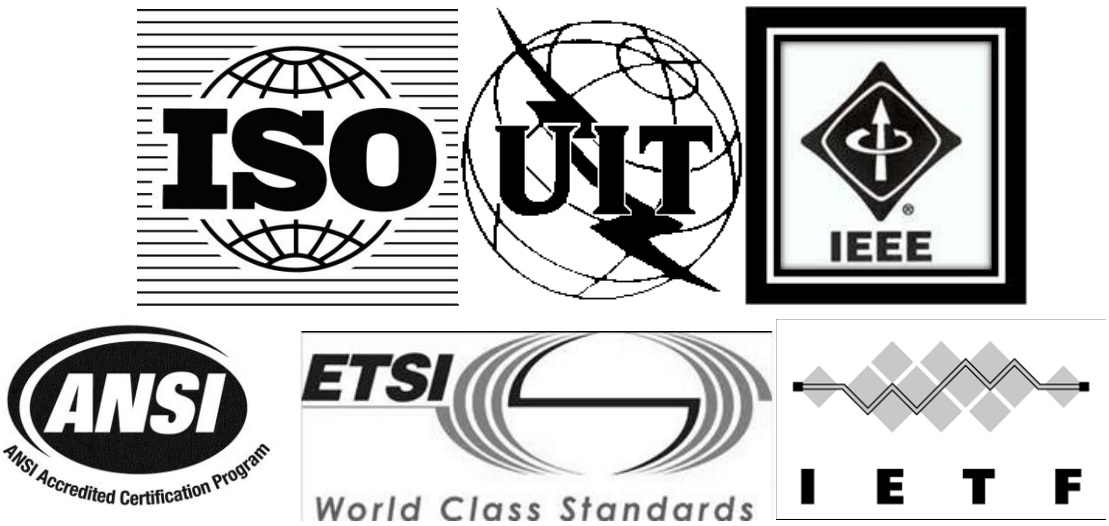


Figura No.1.13- Organismos de estandarización

Dentro de los organismos de estandarización antes mencionados, se encuentra ISO, organización que creo el modelo de red descriptivo llamado OSI. Las características del modelo OSI se describirán en el siguiente tema.

1.9. Modelo de referencia OSI

Toda comunicación, está regida por reglas predeterminadas denominadas protocolos. Estos protocolos son específicos de las características de conversación.

Para obtener una comunicación exitosa entre los hosts de una red, se requiere de la interacción de una gran cantidad de protocolos diferentes. Se denomina suite o conjunto de protocolos a un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación. [11]

Los conjuntos de protocolos de redes describen procesos como los siguientes: [11]

- El formato o estructura del mensaje
- El método por el cual los dispositivos de redes comparten información de rutas con otras redes.
- Inicio y terminación de las sesiones de transferencia de datos.

Los protocolos individuales de un conjunto de protocolos pueden ser específicos de un fabricante o de propiedad exclusiva.

Una de las mejores formas de visualizar de qué manera todos los protocolos interactúan en un host es verlo como una pila (stack). Una pila de protocolos muestra como los protocolos individuales de la suite se implementan en el host. Los protocolos se muestran como una jerarquía en capas, donde cada servicio de nivel superior depende de la funcionalidad definida por los protocolos que se muestran en los niveles inferiores. Por su parte, las capas inferiores de la pila competen a los movimientos de datos por la red y a la provisión de servicios a las capas superiores, concentrados en el contenido del mensaje que se está enviando y en la interfaz de usuario.

Existen dos tipos básicos de modelos para las comunicaciones de red, los cuales son: modelos de protocolo y modelos de referencia. En este tema sólo se interesa describir el modelo de referencia, sin embargo, el modelo de protocolo se explica en el tema 1.10. [11]

Un modelo de referencia proporciona una referencia común para mantener consistencia en todos los tipos de protocolos y servicios de red. Este modelo no está pensado para ser una especificación de implementación, ni para proporcionar un nivel de detalle suficiente para definir de forma precisa los servicios de la arquitectura de red. Su propósito principal es asistir en la comprensión más clara de las funciones y los procesos involucrados. [11]

El modelo de interconexión de sistema abierto (OSI) es el modelo de referencia para las comunicaciones de red más conocido. Se utiliza para el diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas.

Inicialmente, el modelo OSI fue diseñado por la ISO en 1984 para proporcionar un marco sobre el cual crear un conjunto de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas propietarios. Lamentablemente, la velocidad a la que fue adoptada la Internet y la proporción en

la que se expandió ocasionaron que el desarrollo y la aceptación del modelo OSI se quedaran atrás. [11]

El objetivo primordial del modelo OSI es acelerar el desarrollo de futuros productos de una red. Aunque existen otros modelos de referencia, la mayoría de los actuales fabricantes relacionan sus productos con el modelo de referencia OSI, ya que lo consideran la mejor herramienta disponible para enseñar cómo se envían y reciben datos en la red. [70]

OSI fue diseñado para describir las funciones que cualquier sistema de redes debe ofrecer en términos de capas o niveles, donde cada capa se construye sobre la base de la inmediata inferior. El modelo de referencia OSI es una especificación de servicios de comunicación; cada nivel ofrece una clase particular de servicios al nivel superior y espera un servicio de la capa inferior. El modelo OSI divide los procesos de la comunicación en una pila de 7 capas o niveles: Física, Enlace de datos, Red, Transporte, Sesión, Presentación y Aplicación. [70]

Para proporcionar servicios de comunicación, cada nivel se debe comunicar con su capa subsecuente. Las comunicaciones requieren protocolos y éstos son especificaciones o reglas que gobiernan las transacciones de la comunicación entre las capas del modelo. Las funciones se dividieron en el principio divide y vencerás, el cual indica que dividir una tarea en tareas más pequeñas y manejables, ayudará a conquistarlas. [70]

Las capas 1-Física, 2-Enlace de datos y 3-Red, se definen como orientadas a la red, debido a que se usan para comunicar computadoras, mientras que las capas 5-Sesión, 6-Presentación y 7-Aplicación, están orientadas a las aplicaciones, porque ellas se concentran en la tarea de comunicación entre procesos, por último, la capa cuatro esconde detalles de las capas orientadas a la red y de las capas orientadas a las aplicaciones. [70]

En el siguiente modelo ilustrativo se mencionan y describen brevemente las capas del modelo OSI (Ver Figura No.1.14): [11]

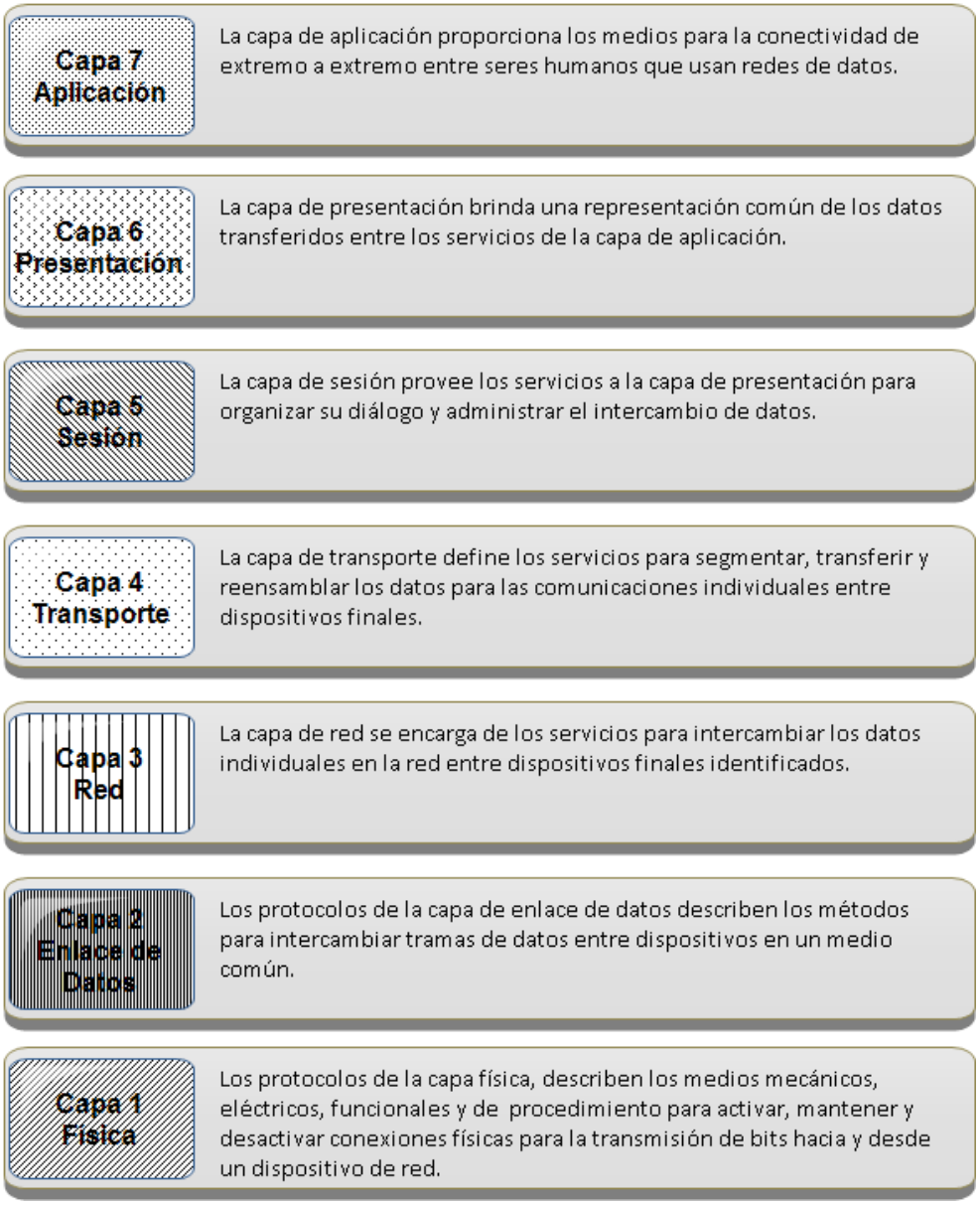


Figura No. 1.14-Modelo OSI en forma de pila

1.9.1. Capas del modelo de referencia OSI

Capa 1. Física.

Se ocupa de la transmisión de la información en forma de bits (unidad básica de información) a lo largo de un canal de comunicación. Su diseño debe asegurar que cuando un extremo envía un bit con cierto valor, éste se reciba como un bit con exactamente el mismo valor en el otro extremo. [70]. Las limitaciones del nivel físico (equipos de transmisión y recepción, medios de transmisión, amplificadores, entre otros.) imponen otras al resto del sistema, por un lado, limitan la velocidad de transmisión y, por otro, hacen aparecer una probabilidad de error: el porcentaje de bits erróneos que llegan al destino.

El envío de tramas a través de medios de transmisión requiere de los siguientes elementos de la capa física: [11]

- Medios físicos y conectores asociados.
- Una representación de los bits en los medios
- Codificación de los datos y de la información de control
- Sistema de circuitos del receptor y transmisor en los dispositivos de la red.

El objetivo de la capa física es crear la señal que representa a los bits en cada trama y su función es recuperar las señales individuales desde los medios, restaurarlas para sus representaciones de bit y enviar los bits hacia la capa de Enlace de datos como una trama completa. [11]

Para transmitir las señales, existen dos tipos básicos de medios de red: [11]

- Alámbricos
- Inalámbricos

La presentación de los bits depende del tipo de medio. Para los medios alámbricos de cobre, las señales son patrones de pulsos eléctricos. Para los medios de fibra, las señales son patrones de luz. Para los medios inalámbricos, las señales son patrones de transmisiones de radio, microondas o infrarrojo. [11]

Debido al uso de conectores, medios y circuitos electrónicos en la capa física, las principales organizaciones especializadas en ingeniería eléctrica y en comunicaciones (ISO, IEEE, ANSI, ITU, EIA/TIA, entre otros) definen los estándares que rigen al hardware antes mencionado. Por otro lado, las operaciones y los protocolos de las capas superiores de OSI se llevan a cabo mediante un software y están diseñados por especialistas informáticos e ingenieros de software. [11]

Resumiendo, la capa física se encarga de la conexión física de la red, de las reglas de codificación de transmisión, así como de las especificaciones mecánicas y eléctricas para el medio de transmisión (Ver Figura No. 1.15).

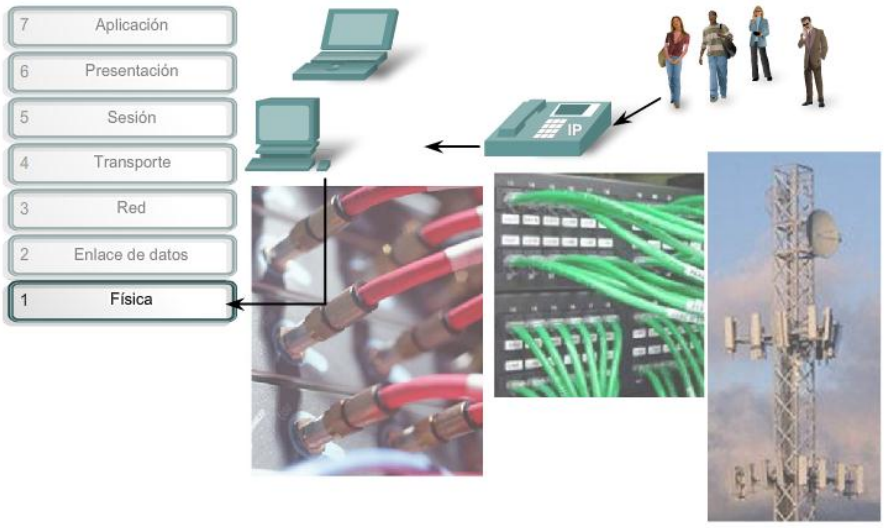


Figura No. 1.15-Capa Física

Capa 2. Enlace de datos.

La capa de enlace de datos proporciona un medio para intercambiar datos a través de medios locales comunes. [11]

Los principales servicios de la capa de enlace son: [11]

- Permitir a las capas superiores acceder a los medios usando técnicas como tramas.
- Controlar la forma en que se ubican los datos en los medios y la manera en que son recibidos desde los medios usando técnicas como el control de acceso a los medios y detección de errores.

Un modelo de red permite que cada capa funcione con un mínimo interés por los papeles de las otras capas. La capa de enlace de datos releva a las capas superiores de la responsabilidad de colocar y recibir datos. Esta capa proporciona servicios para soportar los procesos de comunicación para cada medio por el cual se transmitirán los datos. [11]

Los métodos de control de acceso al medio definen los procesos por los cuales los dispositivos de red pueden acceder a los medios de red y transmitir datos en diferentes entornos de red.[6]

Para sostener una gran variedad de funciones, la capa de enlace de datos generalmente se divide en dos subcapas comunes de tecnologías LAN, las cuales son (Ver Figura No. 1.16): [70]

LLC (Logical Link Control, Control de enlace lógico): Se encarga de colocar la información en la trama que identifica qué protocolo de la capa de red está siendo utilizado por la trama. Esta información permite que varios protocolos de la capa 3 utilicen la misma interfaz de red y los mismos medios. [70]

MAC (Media Access Control, Control de acceso al medio): Tiene el control sobre la manera en que los dispositivos de red, tienen permitido acceder al medio. Es responsable de etiquetar y leer el origen y el destino físico o dirección MAC (Identificador único de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red) asociada con la trama. [11]

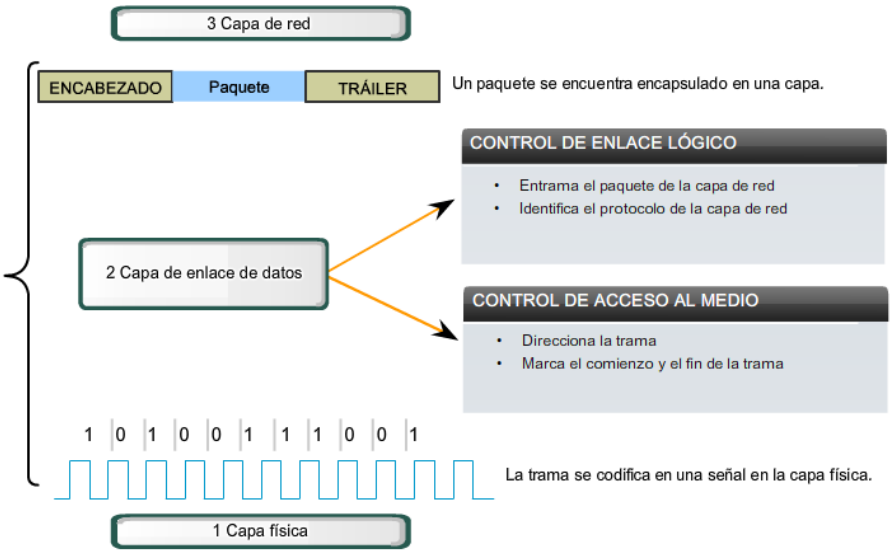


Figura No. 1.16-Subcapas de enlace de datos

Capa 3. Red

La capa de red provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados (Ver Figura No. 1.17). Para lograr dicho intercambio de datos, se puede basar en dos tipos de tablas: estáticas y dinámicas. [11]

Las tablas estáticas se encuentran predefinidas, difícilmente pueden cambiarse y, se pueden determinar al inicio de cada conversación.

Por otro lado, las de tipo dinámico se determinan de forma diferente para cada paquete, reflejando la carga de la red. Si en cierto momento existen demasiados paquetes presentes en la subred, ellos mismos congestionarán la red, dando lugar a un cuello de botella. [70] El control de tal problema dependerá de la capa de red, así como el direccionamiento, la encapsulación, el enrutamiento y la desencapsulación. [11]

Resumiendo, la capa de red tiene tres funciones principales: [70]

- Organizar los mensajes en grupos lógicos llamados paquetes.
- Encaminar paquetes hacia sus correspondientes redes destinos.
- Establecer las direcciones IP en los ruteadores.

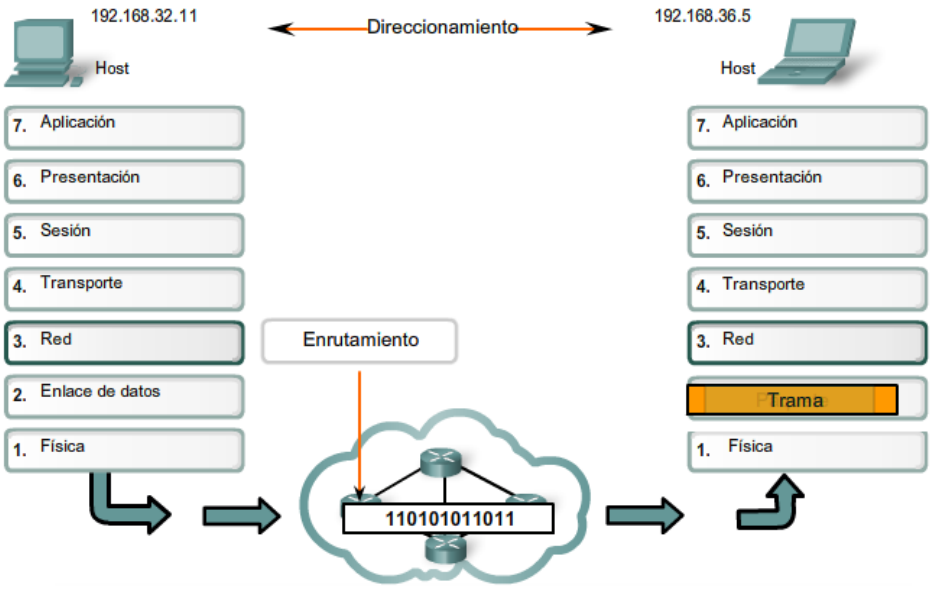


Figura No. 1.17-Capa de red

Capa 4. Transporte

La capa de transporte prepara los datos de la aplicación para el viaje a través de la red y procesa los datos de la red para su utilización por parte de las aplicaciones. Permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos flujos de datos de comunicación. Las responsabilidades principales que debe cumplir son: [11]

- Dar el seguimiento de la comunicación individual entre aplicaciones en los hosts origen y destino.
- Segmentar los datos y administrar cada porción.
- Reensamblar los segmentos en flujos de datos de aplicación.
- Identificar las diferentes aplicaciones.

La función principal de la capa de transporte es aceptar los datos de la capa de sesión y dividirlos siempre que sea necesario en unidades más pequeñas, pasarlos a la capa de red y asegurar que todos ellos lleguen correctamente al otro extremo. [70]

Bajo condiciones normales, la capa de transporte establece el acceso a los servicios de red. Si los datos transportados necesitan un gran canal para la transmisión de la información, ésta puede dividir los datos entre las conexiones de red (segmentación) con el objeto de mejorar la utilización del medio de transmisión. Por otra parte, si la creación o mantenimiento de la conexión de una red resulta costosa, la capa de transporte podría combinar los datos de varias conexiones (multiplexación) sobre la misma conexión de red para reducir dicho costo (Ver Figura No. 1.18). [70]

El tipo más popular de conexión al nivel de capa de transporte corresponde a la comunicación punto a punto sin error, en la cual se entregan los mensajes en el mismo orden en que fueron enviados, ayudándose de reglas de comunicación. Sin embargo, existe la opción de transportar mensajes aislados sin garantizar el orden de distribución y la entrega confiable del mensaje. [70]

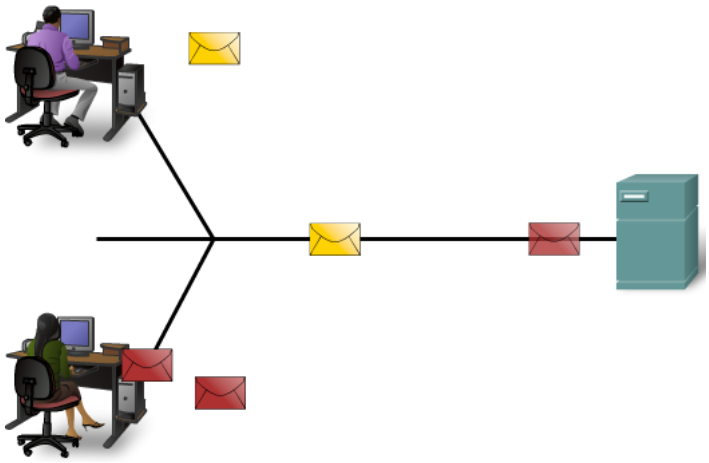


Figura No. 1.18-Segmentación y multiplexación

Capa 5. Sesión

La capa de sesión permite que los usuarios puedan establecer sesiones de trabajo con los proveedores de servicios de red. Se encarga del establecimiento, sincronización, sostenimiento y liberación de la conexión. Cuando se establece una sesión se permite acceder a un sistema de tiempo compartido a distancia o transferir un archivo entre dos hosts. Otra función de esta capa es administrar la manera en que se llevará a cabo el diálogo para la comunicación de los datos, esta puede ser: Simplex-Transmisión unidireccional, un solo sentido; Half Dúplex-

Transmisión en ambas direcciones, pero sólo una a la vez; o Full Dúplex-Transmisión en ambos sentidos al mismo tiempo. [70]

En caso de que existiera un error y se abortara la transferencia de un archivo, ésta tendría que iniciarse de nuevo y probablemente se encontraría con otra caída de red. Para eliminar este problema, la capa de sesión proporciona una forma para insertar puntos de verificación en el flujo de datos, con el objetivo de que después de cada caída, solamente tengan que repetirse los datos que se encuentren después del último punto de verificación. [70]

Capa 6. Presentación

La capa de presentación realiza funciones que se necesitan a menudo para buscar una solución general cuando se tienen máquinas con diferentes formatos de presentación de la información. Se ocupa de los aspectos de sintaxis y semántica de la información que se transmite. [11]Sus tres funciones primarias son: [11]

- Codificar y convertir los datos de la capa de aplicación para garantizar que los datos del dispositivo de origen puedan ser interpretados por la aplicación adecuada en el dispositivo de destino.
- Comprimir los datos de forma que puedan ser descomprimidos por el dispositivo de destino.
- Cifrar los datos para su transmisión y descifrar los datos cuando se reciben en el destino.

Las implementaciones de la capa de presentación generalmente no se vinculan con una pila de protocolos determinada. Los estándares para videos y gráficos son algunos ejemplos. [70]

Capa 7. Aplicación

La capa de aplicación es la capa superior del modelo OSI. Ésta capa proporciona la interfaz entre las aplicaciones que se utilizan para comunicar a los usuarios con la red subyacente en la cual se transmiten los mensajes (Ver Figura No. 1.19). [11]

La capa siete contiene una variedad de reglas, las cuales se encargan de validar el acceso y la implementación de los servicios de red. Los protocolos más conocidos en esta capa son aquellos que proporcionan información del usuario. Estos protocolos especifican la información de control y formato necesario para muchas funciones de comunicación de internet. [70]

Las funciones asociadas con los protocolos de la capa Aplicación permiten a la red humana comunicarse con la red de datos subyacente. Cuando se abre un explorador web o una ventana de mensajería instantánea, se inicia una aplicación, y el programa se coloca en la memoria del dispositivo donde se ejecuta. Cada programa ejecutable cargado a un dispositivo se denomina proceso. [11]

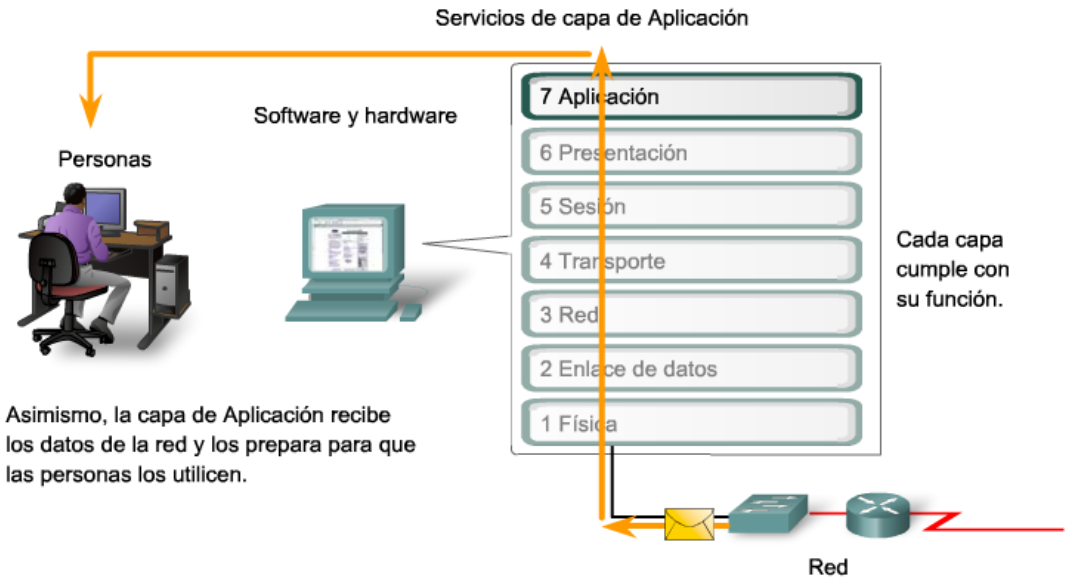


Figura No. 1.19-Funcionamiento de la capa de Aplicación

Con esta última capa se concluye la descripción de las funciones de cada una de las capas del modelo de referencia OSI y de su utilización para lograr la comunicación de red. Además de los modelos de referencia, existen otros tipos modelos para las comunicaciones de red, denominados modelos de protocolos.

1.10. Modelo de protocolos TCP/IP

Un modelo de protocolo proporciona un modelo que coincide fielmente con la estructura de una suite de protocolos en particular. El conjunto jerárquico de protocolos relacionados en una suite representa típicamente toda la funcionalidad requerida para interconectar la red humana con la red de datos. El modelo TCP/IP es un modelo de protocolo ya que describe las funciones que se producen en cada capa de los protocolos dentro del conjunto TCP/IP. [11]

Esta tecnología tiene su origen a principio de la década de los setentas en el departamento de Defensa (DoD) de los Estados Unidos de América, quienes deseaban que su Internet tuviera una rápida proliferación de las computadoras y otros elementos de procesamiento de señales dentro de la milicia, además de la necesidad de conectar equipos de diferentes fabricantes. [70]

La principal ventaja de TCP/IP, estriba en que está diseñado para enlazar computadoras de diferentes tipos, incluyendo computadoras personales, minicomputadoras o mainframes, que ejecuten sistemas operativos distintos sobre LAN y WAN, y por lo tanto, permite la conexión de equipos distantes geográficamente. [70]

TCP/IP es una colección de protocolos. Su nombre proviene de sus dos protocolos más conocidos: TCP, el cual corresponde a la capa 4 del modelo de referencia OSI (capa de transporte) y ofrece transmisión confiable de datos, e IP que trabaja en la capa 3 del modelo de referencia OSI (capa de enlace de red) y ofrece el servicio de datagramas sin conexión. [70]

La arquitectura TCP/IP transfiere datos mediante el ensamble de datos de paquetes. Cada paquete comienza con una cabecera que contiene información de control seguida de datos. [70]

El modelo de protocolos TCP/IP se divide en 4 capas: Capa 4-Aplicación, Capa 3-Transporte, Capa 2-Internet, Capa 1-Acceso a la red (Ver Figura No. 1.20). [11]

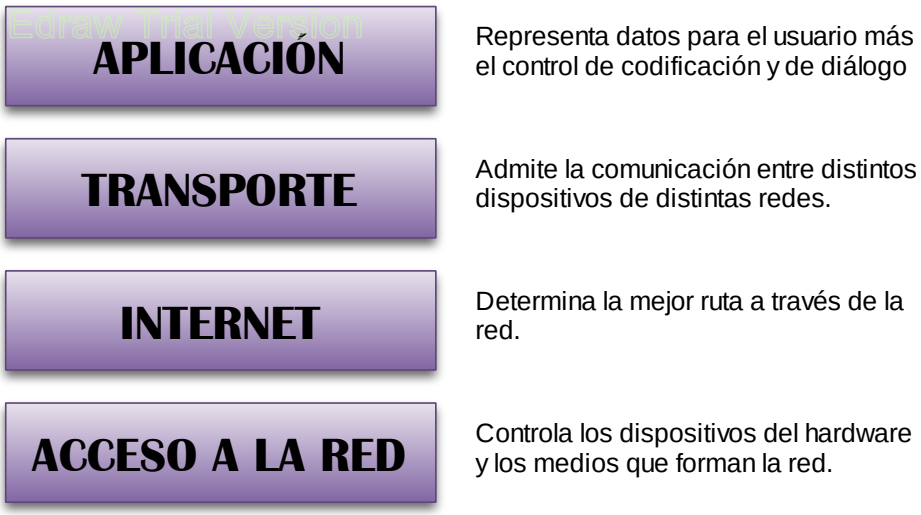


Figura No. 1.20-Protocolo TCP/IP

Un ejemplo del uso del protocolo TCP/IP, es la interacción entre un servidor Web y un explorador Web. Esta interacción utiliza una cantidad de protocolos y estándares en el proceso de intercambio de información entre ellos. Los distintos protocolos trabajan en conjunto para asegurar que ambas partes reciban y entiendan los mensajes. Algunos ejemplos de estos protocolos son: [11]

a) Protocolos de aplicación:

Protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol) es un protocolo común que regula la forma en que interactúan un servidor Web y un cliente Web. HTTP define el contenido y el formato de las solicitudes y respuestas intercambiadas entre el cliente y el servidor. Tanto el cliente como el software del servidor Web implementan el HTTP como parte de la aplicación. El protocolo HTTP se basa en otros protocolos para regir de qué manera se transportan los mensajes entre el cliente y el servidor. [11]

El protocolo HTTP se utilizó con el fin de ejemplificar la interacción entre un servidor Web y un explorador Web, sin embargo dentro de esta capa también se encuentran otros protocolos, donde los más conocidos son: [70]

- Telnet (Telecommunication Network, Red de Telecomunicaciones).
- FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos).
- SNMP (Simple Network Management Protocol, Protocolo Simple de Administración de Redes)
- DNS (Domain Name System, Sistema de Nombres de Dominio)
- SMTP (Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo).

b) Protocolos de transporte:

TCP (Transmission Control Protocol, Protocolo de control de transmisión) es el protocolo de transporte que administra las conversaciones individuales entre servidores Web y clientes Web. TCP divide los mensajes HTTP en segmentos, para enviarlos al cliente destino. También es el responsable de controlar el tamaño y los intervalos a los que se intercambian los mensajes entre el servidor y el cliente. [11]

Además del protocolo TCP existe el protocolo UDP (User Datagram Protocol, Protocolo de Datagrama de Usuario), el cual se basa en el intercambio de datagramas. Su principal característica es permitir el envío de datagramas a través de la red sin que se haya establecido una conexión. Sin embargo la desventaja que se tiene es que no existe confirmación ni control de flujo. [70]

c) Protocolos de internet:

El protocolo de internet más conocido es IP (Internet Protocol, Protocolo de Internet), el cual es responsable de tomar los segmentos formateados del TCP, encapsularlos en paquetes, asignarles las direcciones correctas y seleccionar la mejor ruta hacia su destino. [11]

Otro protocolo perteneciente a la capa de internet es el ICMP (Internet Control Message Protocol, Protocolo de Mensajes de Control de Internet), el cual es utilizado por los gateways y hosts para evaluar las condiciones de funcionamiento de los servicios IP. Su objetivo principal es proporcionar la información de error o control entre nodos. [70]

d) Protocolos de acceso a la red.

El propósito de estos protocolos es describir dos funciones principales: la administración de enlace de datos y la transmisión física de datos en los medios. Los protocolos de administración de enlace de datos toman los paquetes IP y los formatean para transmitirlos por los medios. Los estándares y protocolos de los medios físicos rigen de qué manera se envían las señales por los medios y como las interpretan los clientes que las reciben. Los transceptores (convertidores de señales digitales a señales eléctricas u ópticas) de las tarjetas de interfaz de red implementan los estándares apropiados para los medios que se utilizan. [11]

Algunos ejemplos de protocolos pertenecientes a esta capa son: [70]

- **Ethernet**. Protocolo de redes LAN para computadoras con acceso al medio CSMA/CD (Carrier Sense Multiple Access with Collision Detection, Acceso Múltiple por Detección de Portadora con Detección de Colisiones). Se refiere solo a las primeras dos capas del modelo OSI.
- **Token Ring**. Protocolo utilizado en redes con topología física en anillo para acceder al medio.
- **FDDI** (Fiber Distribute Data Interface, Interfaz de Datos Distribuidos por Fibra), protocolo usado para la transmisión de datos en redes tipo LAN mediante cable de fibra óptica.
- **Frame Relay**. Método de comunicación orientado a paquetes para la conexión de sistemas informáticos. Un frame tiene la característica de ser de tamaño variable.

Con la explicación de los modelos de las comunicaciones de red, es posible conocer cuál es el proceso que siguen las redes para poder transmitir información. Hasta este punto se conoce como se comunica una red, sus elementos y sus ventajas, sin embargo, el mantenimiento, gestión, control y mejora de la red está a cargo de la administración de redes.

CAPÍTULO 2.

Conceptos básicos de administración de redes

2. CONCEPTOS BÁSICOS DE ADMINISTRACIÓN DE REDES

Una red es extremadamente importante, sin embargo ésta no se crea, diseña, implementa, dirige y controla sola, es necesario que exista un administrador de red, el cuál será el encargado de mantener la red funcionando correctamente.

En este capítulo se abordan los conceptos fundamentales, objetivos y elementos de la administración de redes.

2.1. Definición de administración de redes

En el ámbito empresarial, la administración de redes es un instrumento vital en la planeación, organización, integración, dirección y control de los elementos de la comunicación, para garantizar un adecuado nivel de servicio, de acuerdo a un costo determinado. Al igual que las arquitecturas de redes, los sistemas de administración de redes no son idénticos, por esta razón el administrador de red tiene que encontrar el equilibrio entre los tipos de servicios que se ofrecen a los usuarios, la calidad de estos, y los medios que se deben implementar con el fin de lograr el nivel de calidad deseado. Un servicio de red es un producto que es consumido por el usuario o cliente, que goza de derechos y cumple las obligaciones que se estipulan en el contrato del servicio.

Desde el punto de vista del usuario, la arquitectura, el funcionamiento y la administración de la red debe de ser totalmente transparente. De acuerdo a sus condiciones de suscripción, los usuarios tienen el derecho de tener una conexión inmediata en cualquier momento del día o de la noche, y en cualquier época del año. La red debe satisfacer sus necesidades, proporcionando una transmisión fiable de información, sin pérdida ni errores, y con un tiempo de respuesta satisfactorio. Cualquier sistema de administración de red debe gestionar y controlar la red, independientemente de la arquitectura de la red y la complejidad, de tal manera que las necesidades de los usuarios y operadores sean plenamente cubiertas, para lograrlo, es necesario que el administrador de red cumpla con los siguientes puntos en la realización de sus actividades: [56]

- Planeación: Debe considerar la infraestructura del sistema de la que depende la vida futura de la red, las políticas y la ética que rige el cómputo.
- Organización: Implementar los modelos de la administración de redes para su mejor desempeño y utilizar modelos para la administración de los protocolos utilizados en las redes de datos.
- Integración: El administrador debe reunir e implementar las tecnologías actuales para la adecuada función de la red.
- Dirección: Adquirir o desarrollar la capacidad de liderazgo que le permita interactuar con el equipo de trabajo, con el objetivo de conjuntar esfuerzos en beneficio de la red.
- Control: Monitorear la red para optimizar el rendimiento, disponibilidad y funcionalidad de esta, manejando estándares para la medición, ejecución, acciones preventivas y correctivas.

2.2. Objetivos de la administración de red

La administración de redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada, con una planeación adecuada y propiamente documentada. Los principales objetivos de la administración de redes son: [49]

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control, monitoreo, detección de errores y suministro de recursos.
- Utilizar los recursos correctamente para una mejor eficiencia.
- Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.
- Fortalecer la red, usando métodos de seguridad efectivos
- Controlar cambios y actualizaciones en la red sin atentar contra la disponibilidad de esta.
- Crear redes convergentes (voz, datos y video)
- Interconectar redes LAN, MAN, WAN, utilizando diferentes medios de comunicación como par trenzado, cable coaxial, fibra óptica, satelital, entre otros.

El diseño de las redes, es una parte de la administración de redes que debe cubrir las siguientes especificaciones: [56]

- La información debe entregarse de manera confiable, sin ningún daño en los datos, y debe ser consistente.
- Cada computadora en la red debe ser capaz de identificar a todas las demás computadoras y a sí misma a través de lo largo de la red
- Debe existir una forma estándar de nombrar e identificar las partes de una red.

El modelo OSI considera que las cinco funciones de administración básicas son: [56]

- Configuración
- Errores
- Contabilidad
- Comportamiento
- Seguridad

2.3. Elementos de la administración de red [56]

La administración de red requiere de la habilidad de supervisar, comprobar, sondear, configurar y controlar los componentes hardware y software de una red. Dado que los dispositivos de red son distribuidos, el administrador debe ser capaz de recopilar datos, para la supervisión de entidades remotas, así como realizar cambios sobre ellas, para controlarlas. Con el fin de realizar las actividades mencionadas se hace uso de una arquitectura de sistemas de administración de redes, la cual se compone de los siguientes elementos (Ver Figura No. 2.1):

- Entidad administradora: Consiste en una aplicación con control humano que se ejecuta en una estación centralizada de administración de red en el Centro de Operaciones de Red (NOC, Network Operations Centers). En el NOC se realiza la actividad de la administración

de la red, se controla la recolección, procesamiento, análisis o visualización de la información de la administración, así como la iniciación de las acciones que controlan el comportamiento de la red, y la interacción del administrador de red con los dispositivos que la conforman.

- Dispositivo administrado: Parte del equipamiento de la red, incluido el software, que se localiza en la red administrada. Un dispositivo administrado puede ser desde un host hasta una impresora o un modem. Dentro del dispositivo existen varios objetos administrados, como el hardware o la tarjeta de red.
- Base de información de administración: Lugar donde se almacenan los datos referentes a los objetos administrados.
- Agente de administración de red: Proceso que se ejecuta en cada dispositivo administrado y que se comunica con la entidad administradora, realizando acciones locales bajo el control de los comandos de la entidad administradora.
- Protocolo de administración de red: Permite a la entidad administradora consultar el estado de los dispositivos, e indirectamente realizar acciones en dichos dispositivos a través de los agentes.

Los agentes pueden utilizar el protocolo de administración de red para informar a la entidad administradora de eventos excepcionales, tales como el fallo de componentes.

El protocolo de administración proporciona una herramienta que ayuda al administrador de red a cumplir sus funciones.

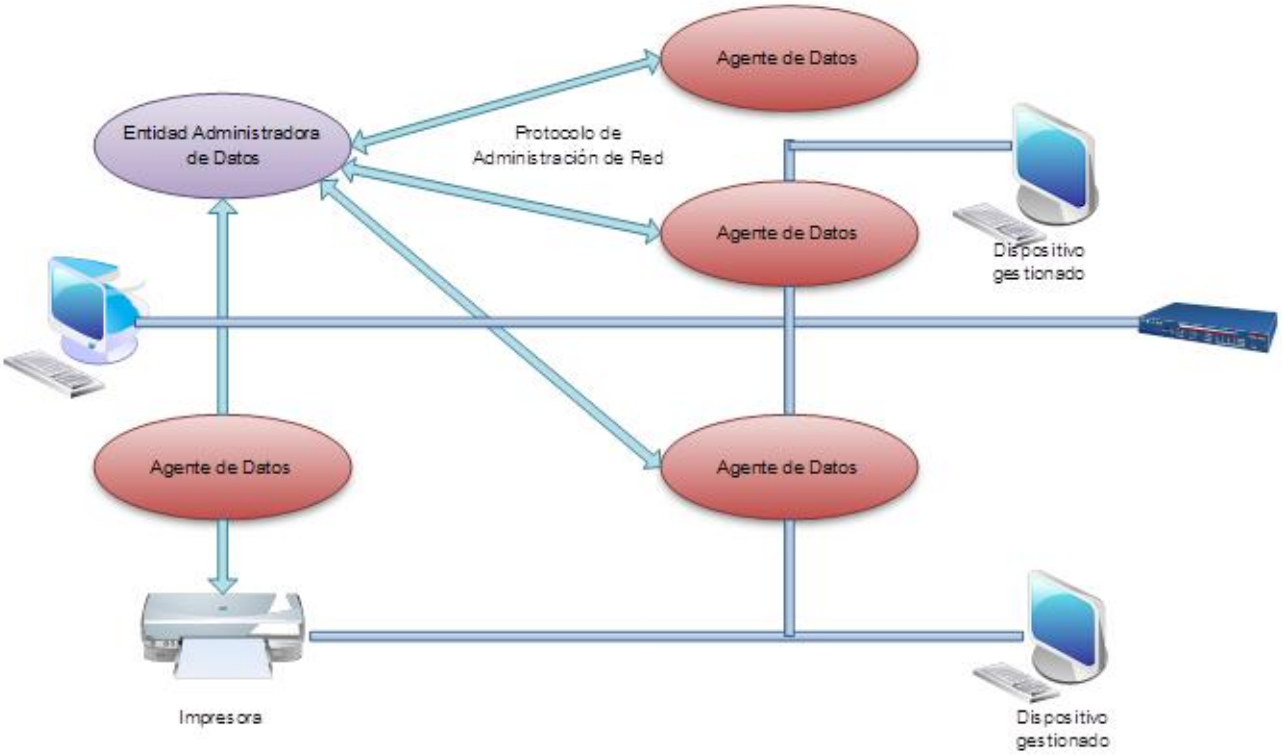


Figura No. 2.1-Infraestructura de administración de redes.

2.4. Ciclo de la administración de red

El administrador de red debe de seguir un ciclo de administración para crear una red eficiente con el menor costo posible. El ciclo de la administración se conforma de cinco elementos: Planeación, Organización, Integración, Dirección y Control.

2.4.1. Planeación

La planeación consiste en la determinación de los objetivos y en elegir el futuro curso de acción para lograrlos.

El primer paso de la etapa de planeación es el diseño de la red, donde los elementos que se deben considerar son: [56]

- Aspectos físicos, tales como la ubicación geográfica de los dispositivos, el tráfico esperado y el costo de los niveles de servicio a proveer.
- Parámetros de rendimiento, por ejemplo, la confiabilidad de la red, velocidad estimada, velocidad esperada de transferencia y la capacidad para el procesamiento del tráfico.
- Variables de red como lo son la topología de red y los medios de transmisión.

Para que las redes cumplan con sus objetivos se debe seguir una metodología del diseño de redes la cual se muestra en la Figura No.2.2. [56]

El proceso inicia con el análisis de los requerimientos y el presupuesto donde se considera la infraestructura actual del hardware, el nivel de conocimiento de los usuarios, el tipo de información que circulará por la red, las aplicaciones propietarias y no propietarias a usar y el crecimiento esperado a corto y mediano plazo. Dentro de esta etapa también se debe realizar un inventario de hardware y software, el perfil de usuario medio de la red, las definiciones de niveles de servicio y el reporte de adquisiciones requeridas. [56]

Posteriormente se debe seleccionar las topologías de acuerdo a los requisitos de la red. Además de la elección de topologías y medios de conexión, se deben prevenir los cuellos de botellas o sobresaturación de la red que podrían atentar contra la disponibilidad.

Con la red implementada, se deben realizar pruebas de estrés que servirán para observar el comportamiento de la red cuando existe la demanda. En caso de existir fallas, o que la red no funcione como se esperaba, se debe rediseñar la red con el fin de que cumpla con los requisitos establecidos. Después de las mejoras, se debe volver al punto donde se analiza la carga de la red, de nuevo se realiza el proceso de crear carga en la red y se realizan las pruebas de estrés, esperando que la red funcione correctamente.

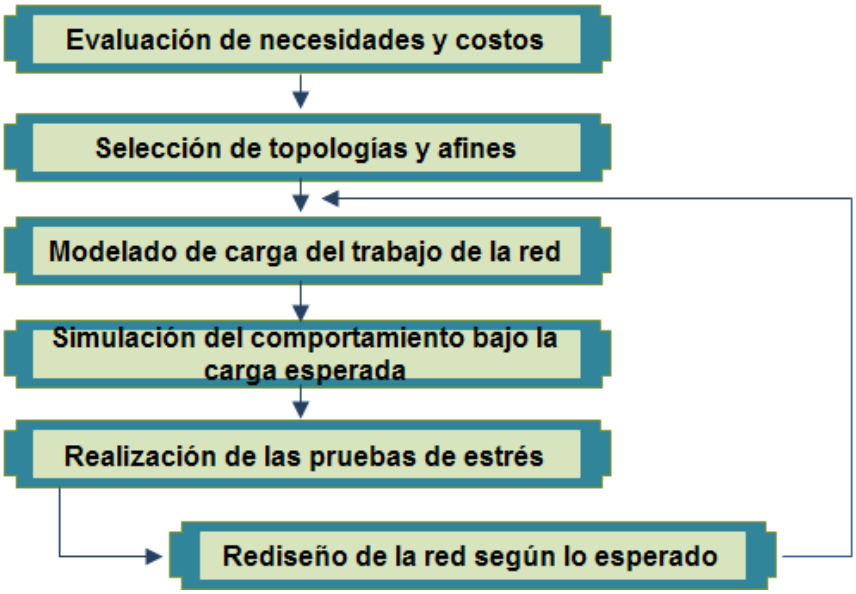


Figura No.2.2 Metodología del diseño de una red

La planeación requiere de un análisis de requerimientos de hardware, el cual consiste en: [56]

- Crear un inventario del hardware que indique el equipo y las interfaces de red que se utilizarán, la marca, el modelo, cantidad de memoria RAM y la carga de trabajo.
- Descubrimiento de la red el cual muestra un panorama global de la infraestructura física, obteniendo como beneficio analizar los cambios que se pudieran realizar.
- Análisis de modelado actual del tráfico de la red, donde se detecta la existencia de dispositivos que están dedicados a un tipo de tráfico y se evalúa la necesidad de utilizar diferentes segmentos de red para cada tipo de tráfico.
- Determinación de los niveles de confianza respecto a la funcionalidad, disponibilidad y seguridad de la red, el nivel puede ser alto, medio o bajo.
- Considerar si el equipo es capaz de soportar las tecnologías y la carga de trabajo que requiere el tráfico de la red.
- Las consideraciones de implementación son las que clasifican al equipo en dispositivos sobreusados, incompatibles, mal configurados o con direccionamiento lógico incorrecto.
- Costos de adquisición y mejora del equipo.

Una vez analizado el hardware se debe analizar la red a nivel software, por ejemplo los protocolos de red, servicios especiales, herramientas de monitoreo, entre otros.

Los principales tipos de software son los sistemas operativos, el software de servicio, los lenguajes de programación y el software de aplicación, de estos debe elegirse el más conveniente según las necesidades de la red. [56]

El siguiente paso que se debe incluir en la etapa de la planeación de la red es el análisis de direccionamiento lógico, el cual define las direcciones MAC y las direcciones IP que la red utilizará.

La dirección IP es asignada por el administrador de red, el rango de direcciones IPv4 expresado en formato decimal punteado es de 0.0.0.0 a 255.255.255.255. Dentro de este rango de direcciones se encuentran: [70]

- Direcciones específicas denominadas direcciones experimentales, de multicast y de host. Abarcan de la dirección 240.0.0.0 a la 255.255.255.254 y se reservaron con el fin de ser utilizadas en un futuro según el RFC 3330.
- Direcciones de multicast que engloban desde la dirección 224.0.0.0 a 239.255.255.255, las cuales a su vez se dividen en direcciones de enlace locales reservadas, direcciones agrupadas globalmente y direcciones agrupadas administrativamente.
- Direcciones de hosts las cuales comprenden de la dirección 0.0.0.0 a la 223.255.255.255 y se usan con los hosts IPv4. Sin embargo, dentro de este rango existen direcciones reservadas para fines específicos.

Las direcciones de host, pueden ser subdivididas en clases A, B y C (Ver Tabla No.2.1) [11]

Tabla No. 2.1- Clasificación de redes por clase

Clase	Rango	No. De Redes	No. De Hosts por Red	Máscara de Red	Broadcast ID
A	1.0.0.0-127.255.255.255	128	16,777,214	255.0.0.0	x.255.255.255
B	128.0.0.0-191.255.255.255	16,384	65,534	255.255.0.0	x.x.255.255
C	192.0.0.0-223.255.255.255	2,097,152	254	255.255.255.0	x.x.x.255

Hay ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan privadas ya que son utilizadas por los hosts que usan NAT (Network Address Translation, Traducción de Dirección de Red) para conectarse a una red pública o por los hosts que no se conectan a internet. Las direcciones privadas son: [11]

Clase A: 10.0.0.0-10.255.255.255 (10.0.0.0/8)
Clase B: 172.16.0.0-172.31.255.255 (172.16.0.0/12), usadas en universidades y grandes empresas.
Clase C: 192.168.0.0-192.168.255.255 (192.168.0.0/16) empleadas en compañías pequeñas y medianas, además de proveedores de internet.

La dirección 0.0.0.0 está reservada según la IANA (Internet Assigned Numbers Authority, Agencia de Asignación de Número de Internet) para identificación local y las direcciones 127.x.x.x se reservan para designar la propia máquina, se denomina dirección de bucle local o loopback. [11]

Un sistema basado en clases tiene muchas limitaciones como el desperdicio de direcciones IP, lo cual agotó la disponibilidad de direcciones IPv4. La solución al agotamiento y/o desperdicio de direcciones IP son las Máscaras de subred o Subnetting, las máscaras de subred de tamaño variable (VLSM, Variable Length Subnet Mask) y el encaminamiento entre dominios sin clase (CIDR, Classless Inter-Domain Routing).

El subnetting es una colección de direcciones IP que permiten definir el número de redes y de hosts que se desean utilizar en una subred determinada; VLSM es una técnica que permite dividir subredes en redes más pequeñas que se ajusten a las necesidades reales de la red, obteniendo como beneficio el máximo aprovechamiento de direcciones; finalmente el CIDR utiliza la técnica VLSM para hacer posible la asignación de prefijos de longitud arbitraria. [56]

Una vez definidos los métodos de asignación de direcciones IP's, el administrador de red debe asignar el espacio de direcciones de la capa de red dentro de la red corporativa, es importante que el administrador no seleccione de forma aleatoria las direcciones utilizadas en las redes con el fin de que no existan duplicaciones de direcciones.

La asignación de direcciones debe ser planificada con el fin de proveer y controlar el acceso a la red, ya que algunos hosts ofrecen recursos tanto para la red interna como para la red externa. Dentro de una red existen diferentes tipos de hosts, algunos ejemplos son: dispositivos finales para usuario, servidores, periféricos, dispositivos intermediarios, entre otros. [11]

Con las direcciones IP asignadas, las conexiones realizadas, el software elegido, se tiene una red que se debe proteger de amenazas que pueden atentar contra su integridad, confidencialidad o disponibilidad.

Una forma de proteger la red, es mediante la definición de las políticas de cómputo, que son un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, resguardar, y distribuir recursos en una organización. Las políticas deben especificar las propiedades del sistema y las responsabilidades de las personas. [55]

Otra característica de las políticas de seguridad es que deben estar en un lenguaje claro, de tal forma que todas las personas dentro de la organización sean capaces de comprenderlas, se deben considerar todos los peligros a los que las redes están expuestas y la manera de contrarrestarlos.

Los principios fundamentales que se aplican en general en las políticas de seguridad son: [55]

- Responsabilidad individual. Se refiere a la responsabilidad de los actos de cada individuo. Las personas deben estar conscientes de sus actividades, debido a que sus acciones son registradas, guardadas y examinadas.
- Autorización. Establece claramente quien y de qué manera puede utilizar los recursos.
- Mínimo privilegio. Las personas dentro de la empresa deben tener acceso exclusivamente a lo que requiera su trabajo.
- Separación de obligaciones. Las funciones deben ser divididas entre las personas relacionadas a la misma actividad, obteniendo como beneficio la anulación de fraudes o ataques.
- Auditoría. Es importante tener control sobre el trabajo y los resultados para conocer las acciones de cada individuo.
- Redundancia. Debe existir un respaldo de registros en diferentes lugares con el fin de prevenir pérdidas de información.

- Reducción de riesgo. Esta estrategia debe reducir el riesgo a un nivel aceptable, haciendo que el costo de la aplicación sea proporcional al riesgo.

Dentro de las políticas de seguridad existen roles con diferentes funciones, para documentos realizados en papel, se aplican los siguientes roles: Originador (autor), autorizador, custodio y usuario. Cuando se trata de una transacción comercial, se anexan el creador, cliente, ejecutor y supervisor. [55]

Las políticas de seguridad deben enfocarse en la protección de la información recabada, procesada y distribuida mediante sus recursos; sin embargo, también se deben emitir políticas para todos los rubros, incluyendo facilidades, aplicaciones, instalaciones y equipos.

Los encargados de definir los requisitos de seguridad, identificar y priorizar la importancia de los distintos elementos son los directivos junto con los expertos en tecnologías de información. Algunas reglas que se deben considerar para establecer una política de seguridad son: [47]

- Toda política debe cubrir todos los aspectos relacionados con el sistema.
- La política debe proteger el sistema en los niveles físico, humano, lógico y logístico.
- Se debe considerar el hardware, software, entorno físico, usuarios y la interacción entre estos.
- Tomar en cuenta el tipo de compañía o entidad (comercial, bancaria, educativa).
- Se debe adecuar a las necesidades y recursos, el valor de estos, y el uso que se hace del sistema en todos los departamentos.
- Evaluar los riesgos, así como el valor del sistema protegido y el costo de ser atacado.
- Debe adoptar el modelo permisivo: “Todo lo que no esté específicamente prohibido está permitido” o el modelo prohibitivo: “Todo está prohibido excepto lo que esté específicamente permitido”.

Es importante destacar que al momento de establecer una política de seguridad se deben formular las tres preguntas siguientes: ¿Qué se necesita proteger?, ¿De qué se necesita proteger? y ¿Cómo se va a proteger? [11]

Terminadas las políticas de seguridad, se concluye con la etapa de planeación de la red, el siguiente paso y elemento del ciclo de la administración a realizar es la organización.

2.4.2. Organización

Desde un punto de vista empresarial, la definición de organización es la aplicación de un conjunto de técnicas conducentes para obtener una empresa estructurada, de tal forma que con la correspondiente división de actividades y la debida coordinación de éstas, se obtenga la máxima rentabilidad. La organización es la base de la labor del administrador que tiende a adecuar los recursos previstos en la planificación para conseguir sus objetivos. [29]

Conforme una red crece, se convierte en un recurso vital que requiere ser administrado de una manera eficiente. Administrar una red implica definir la mejor topología para un adecuado comportamiento, con base a los objetivos de la organización y a las tecnologías disponibles, además de tener conocimiento y control sobre los eventos que permitan realizar proyecciones en el futuro. [56]

El administrador de red debe lograr que la red sea extensible, transparente, eficiente y confiable, sus principales tareas son el monitoreo de la disponibilidad de la red, la mejora de la automatización, vigilar el tiempo de respuesta, la seguridad, redireccionar el tráfico, entre otras. [11]

Todas las funciones antes citadas, se pueden realizar con ayuda de las arquitecturas de administración de red, de las cuales, las tres principales son:

2.4.2.1Modelo OSI (Open System Interconnection, Interconexión de Sistemas Abiertos)

Define una arquitectura de administración de red basada en cinco áreas funcionales o servicios de gestión: [12]

- Administración de configuración. Realiza las funciones de iniciación, desactivación, definición o cambio de parámetros de configuración, denominación de los elementos de la red, recopilación de información sobre versiones de software y hardware.
- Administración de errores. Detecta, diagnostica, registra, notifica y corrige los errores de la red, incluye sondeos periódicos en busca de errores y establece alarmas.
- Administración de prestaciones. Evalúa el comportamiento global de la red y comprueba si se mantienen los niveles normales.
- Administración de contabilidad. Realiza estadísticas sobre el uso de recursos para realizar ajustes o regulaciones.
- Administración de seguridad. Controla el acceso a los recursos, administra las contraseñas, firewalls y crea históricos de seguridad.

Dentro de esta arquitectura se denominan operaciones de administración cuando el administrador solicita datos al objeto o cuando desea actuar sobre él. Por otro lado cuando ocurre un suceso en el objeto, este envía datos al administrador denominadas operaciones de notificación. [12]

La arquitectura OSI incorpora los siguientes componentes: [12]

- SMI (Structure of Management Information, Estructura de la Información de Administración). Define la estructura lógica de la información, las reglas para nombrar los objetos y sus atributos, subclases de atributos, entre otros.
- MIB (Management Information Base, Base de Información de Administración). Conoce todos los objetos y sus atributos, además representa la información que se está manejando en los atributos de administración OSI.
- CMIS (Common Management Information Services, Servicios de Información de Administración Común). El conjunto de reglas que definen la estructura de la información que se intercambia entre las aplicaciones para describir el entorno.

2.4.2.2. Modelo TMN (Telecommunications Management Network, Red de Administración de las Telecomunicaciones)

Proporciona funciones de administración y comunicaciones para la operación, administración y mantenimiento de una red de telecomunicaciones y sus servicios en un entorno de múltiples fabricantes. [5]

TMN introduce una red separada para el transporte de la información de administración que define las siguientes funcionalidades: el intercambio de información entre la red administrada-TMN y entre dos redes TNM; la conversión de formatos, transferencias entre dos puntos de una red TMN, el análisis de la información de administración, la presentación al usuario y el acceso a dicha información. [12]

Las recomendaciones que regulan la TMN son las de la serie M.3XXX de la ITU-T. En esas recomendaciones se definen los siguientes modelos y arquitecturas: [6]

- Arquitectura funcional. Define los bloques funcionales de una TMN y sus puntos de referencia, estos bloques representan funciones apropiadas requeridas por TMN y que son ejecutadas por elementos de la arquitectura física de TMN (Ver Figura No.2.3). Existen 5 bloques funcionales definidos en el estándar M3010: [56]
    - Función de operación de sistemas (OSF): Encargada de procesar la información relativa a la administración de la red para el control y el monitoreo.
    - Función de estación de trabajo (WSF): Permite al usuario el acceso a la información administrada por la TMN.
    - Función de elemento de red (NEF): Administra el intercambio de datos entre los usuarios.
    - Adaptadores Q (QAF): Permiten la integración de elementos que no soporten los puntos de referencia estándar.
    - Función de mediación (MF): Garantiza que durante el intercambio de información entre bloques OSF y NEF cada uno cumpla los requisitos necesarios.
    -

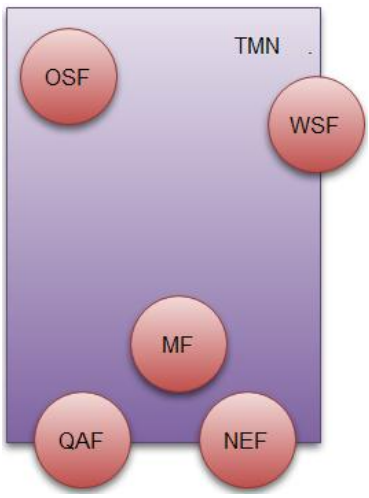


Figura No.2.3-Bloques de la arquitectura funcional.

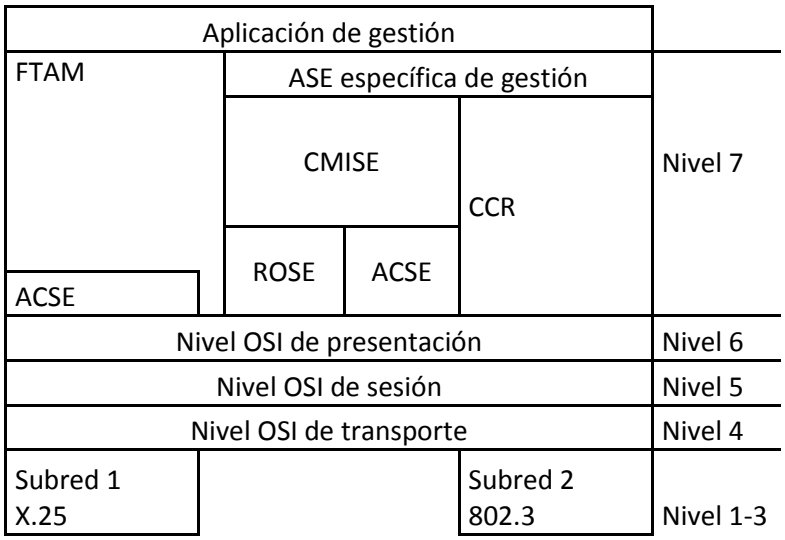
- Arquitectura física. Encargada de describir la estructura física de los bloques funcionales, su implementación y la de los puntos de referencia en interfaces. Esta arquitectura se conforma de bloques de construcción, los cuales pueden intervenir en uno o más bloques funcionales. Los bloques de construcción son: [56]
    - Elemento de red (NE)
    - Dispositivo de mediación (MD)
    - Adaptador Q (QA)
    - Sistema de operaciones (OS)
    - Red de comunicación de datos (DCN)
    - Estación de trabajo (WS)

- Arquitectura de información. La información de administración se modela con base en objetos administrados. Los objetos administrados se definen como abstracciones de los recursos físicos o lógicos a ser administrados, con el objetivo de monitorear la red y prevenir errores en su operación.

Las características principales de un objeto son sus atributos, las operaciones que realiza, el comportamiento que presenta y las notificaciones que emite, tal como lo muestra la Figura No.2.4. [56]

Figura No.2.4-Características de un objeto.

El modelo de información utilizado en TMN es el definido por el interfaz Q3 en la semántica de datos (MIBs GDMO-Guías para la Definición de Objetos de Administración). A continuación se muestra en la Figura No.2.5 un esquema con los niveles de estructura del protocolo del punto de referencia Q3. [6]



- ❖ CMISE: Protocolo de información de gestión común
- ❖ FTAM: Transferencia, acceso y administración de archivos
- ❖ ROSE: Elemento de servicio de operaciones remotas
- ❖ ACSE: Elemento de servicio de control de asociaciones
- ❖ CRR: Recuperación, concurrencia y entrega

Figura No.2.5-Esquema de capas de interfaz Q3.

- Arquitectura lógica en capas. Las áreas de administración TMN siguen el modelo FCPAS de la organización OSI, como se muestra a continuación: [56]
  - Administración de fallos.
  - Administración de configuración.
  - Administración de factibilidad.
  - Administración de prestaciones.
  - Administración de seguridad

Estas funciones pueden ser estructuradas en capas lógicas que corresponden a diferentes niveles de abstracción, los cuales se representan generalmente a través de una pirámide, así como se muestra en la Figura No.2.6. [56]

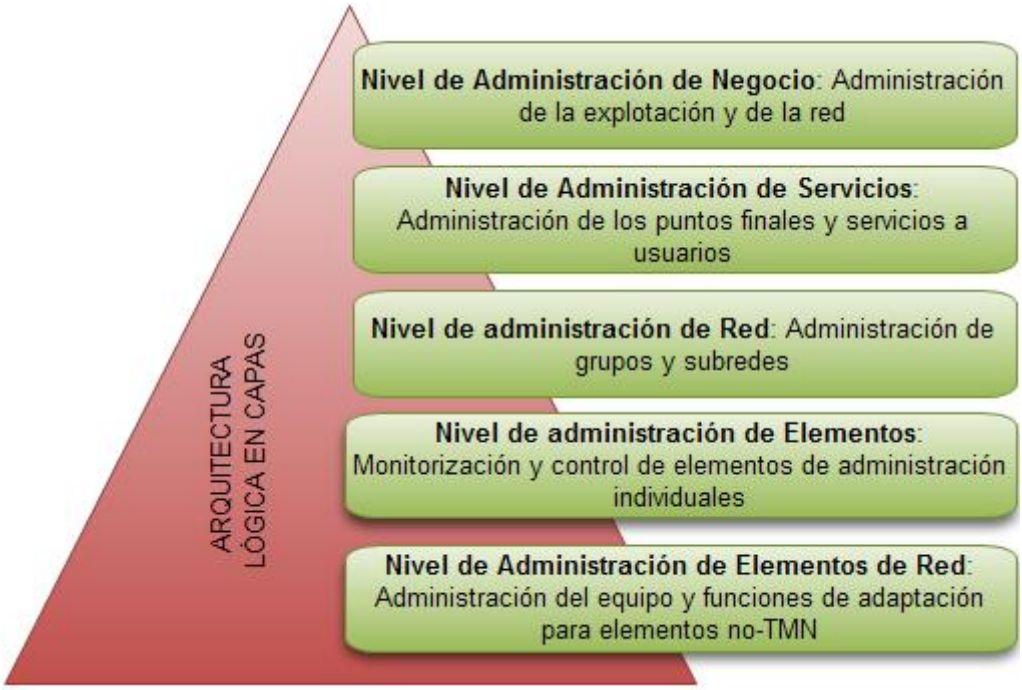


Figura No.2.6-Niveles de abstracción de la arquitectura lógica en capas.

2.4.2.3. Protocolos de administración de red

Dentro de la administración de redes existen herramientas de software diseñadas para supervisar nodos, niveles de tráfico, vigilar cuellos de botella, entre otras funciones. Estas herramientas requieren de un medio de comunicación común que les permita interactuar sin problemas, por lo tanto existe la necesidad de crear protocolos de administración normalizados. [56]

La ISO desarrolló dos estándares para la administración de redes: CMIS (Common Management Information Service, Servicios de Información de Administración Común) y CMIP (Common Management Information Protocol, Protocolo de Información de Gestión Común), que se ubican en la capa de aplicación del modelo OSI. Por su parte en TCP/IP se desarrolló un estándar que provee una funcionalidad similar a CMIP, sencillo y popular llamado SNMP (Protocolo Simple de Administración de Red). SNMP se utiliza en entornos locales y CMIP se utiliza a nivel de red de área amplia. [56]

Además de SNMP y CMIP, el Grupo de Administración de Objetos (OMG, Object Management Group) desarrolló CORBA (Common Object Request Broker Architecture, Arquitectura de Intermediación de Petición de Objetos Comunes), un protocolo que ofrece interoperabilidad y portabilidad entre diferentes lenguajes de programación, plataformas de hardware y sistemas operativos. [46]

A continuación se describirán las características principales de los protocolos de administración de red CMIP y CORBA, se omitirá SNMP ya que este se verá detenidamente en el siguiente capítulo.

2.4.2.3.1. CMIP Protocolo de Información Común (Common Management Information Protocol) [57]

Considerado como una arquitectura de administración de red basada en los servicios CMIS, que provee mecanismos de intercambio de información entre un administrador y elementos remotos de red.

Las principales características de CMIP son:

- Se basa en el paradigma administrador-agente y una base de información.
- CMIS/CMIP hacen un gran uso de recursos tales como memoria y procesador.
- Genera cabeceras complicadas en los mensajes de los protocolos.
- Las especificaciones son problemáticas de realizar y difíciles de implementar en aplicaciones.
- La comunicación con los agentes está orientada a conexión.
- Utiliza estructura de funcionamiento distribuida.
- Permite una jerarquía de sistemas de operación.

Los servicios empleados por CMIP son los CMIS, los cuales definen su implementación en el protocolo CMIP y son invocados mediante un conjunto de primitivas relacionados con uno o varios objetos. Algunos ejemplos de estas primitivas son: M-GET, M-SET, M-ACTION, entre otras.

En CMIP se ocupan los protocolos de aplicación CMISE, ACSE (Association Control Service Element) y ROSE (Remote Operation Service Element), donde ACSE último es el protocolo encargado de establecer y liberar asociaciones entre entidades de aplicación, mientras que ROSE se encarga de las llamadas de procedimientos remotos. Por su parte CMISE proporciona los servicios básicos de administración y genera requerimientos, además, hace uso de los servicios proporcionados por ACSE y ROSE como se muestra en la Figura No.2.7.

CMIP ofrece el servicio de manejo de datos, el cual es utilizado por el administrador para solicitar y modificar información de los recursos del agente, también brinda el servicio de informe de sucesos que es empleado por el agente para informar al administrador y por último se encuentra el servicio de control directo que utiliza el administrador para la ejecución de diversas acciones en el agente.

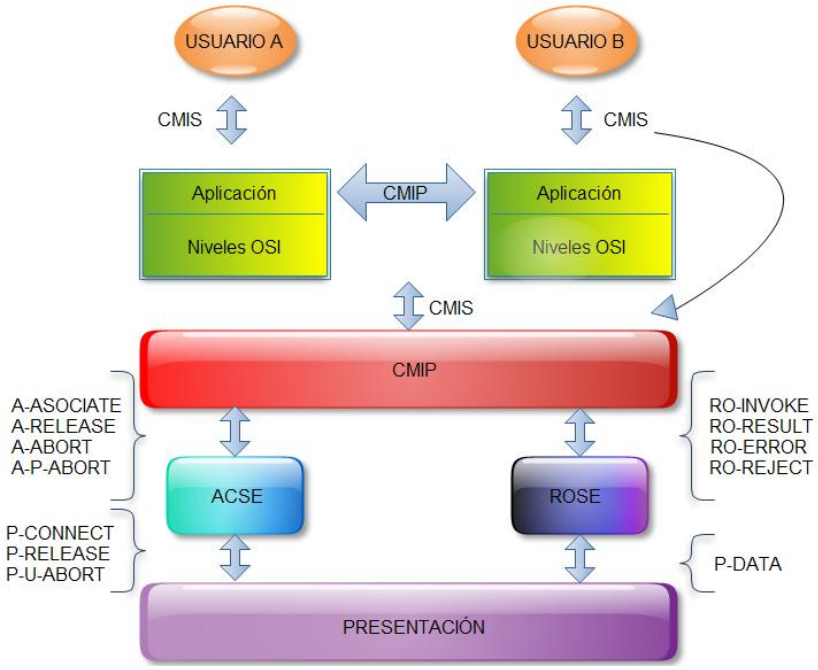


Figura No.2.7-Protocolos que integran a CMIP

2.4.2.3.2. CORBA (Common Object Request Broker Architecture, Arquitectura de Intermediación de Petición de Objetos Comunes).

Arquitectura definida y controlada por el OMG (Object Management Group, Grupo de Administración de Objetos), que define las API´s (Application Programming Interface, Interfaz de programación de aplicaciones), el protocolo de comunicaciones y los mecanismos que permiten la interoperabilidad entre diferentes aplicaciones escritas en diferentes lenguajes y ejecutadas en diferentes plataformas. CORBA mejora la flexibilidad y portabilidad de las aplicaciones. [57]

CORBA surge de la necesidad de buscar mecanismos simples y uniformes para administrar las redes modernas complejas de telecomunicaciones. Se utiliza como un mecanismo de computación distribuida por proveedor de servicios del dominio de las telecomunicaciones. [57]

El funcionamiento de CORBA es “envolver" el código escrito en otro lenguaje en un paquete que tiene información adicional sobre las capacidades del código y cómo llamar a sus métodos. Los objetos que resultan posteriormente puede ser invocados desde otro programa u objeto CORBA en la red. [30]

Algunas de las funciones principales de CORBA son tareas habituales en sistemas distribuidos tales como: registro de objetos, localización de objetos y activación de objetos. [57]

ELEMENTOS DE CORBA

Los elementos y el funcionamiento de CORBA se muestran en la Figura No.2.8, he aquí una breve descripción de cada elemento. [26]

- IDL (Interface Definition Language, Lenguaje de definición de interfaz). Sirve para especificar las interfaces con los servicios que los objetos ofrecerán, éste lenguaje proporciona un mecanismo neutral al lenguaje que permite definir interfaces de objetos distribuidos.
- ORB (Object Request Broker, Intermediación de Petición de Objetos). Administra la transferencia de mensajes desde un programa hacia un objeto localizado en un servidor en una red remota, ocultando al programador la complejidad de las comunicaciones en las redes, el ORB es considerado el núcleo de CORBA.
- DII (Dynamic Invocation Interface, Interfaz de invocación dinámica). Permite la construcción dinámica de peticiones para un determinado objeto. Una invocación dinámica está compuesta por una referencia al objeto, una operación y una lista de parámetros, todos estos obtenidos del Repositorio de Interfaces (IR).
- IR (Interface Repository, Repositorio de Interfaz). Servicio que ofrece objetos persistentes que representan la información IDL de las interfaces disponibles en CORBA de una forma accesible en tiempo de ejecución.
- GIOP (General Inter-ORB Protocol, Protocolo Inter-ORB General). Es un protocolo general. El estándar CORBA también determina protocolos adicionales, que especializan a GIOP para utilizar un protocolo de transporte en particular. El protocolo basado en GIOP más importante es el destinado a redes TCP/IP, conocido como IIOP (Internet Inter-ORB Protocol)

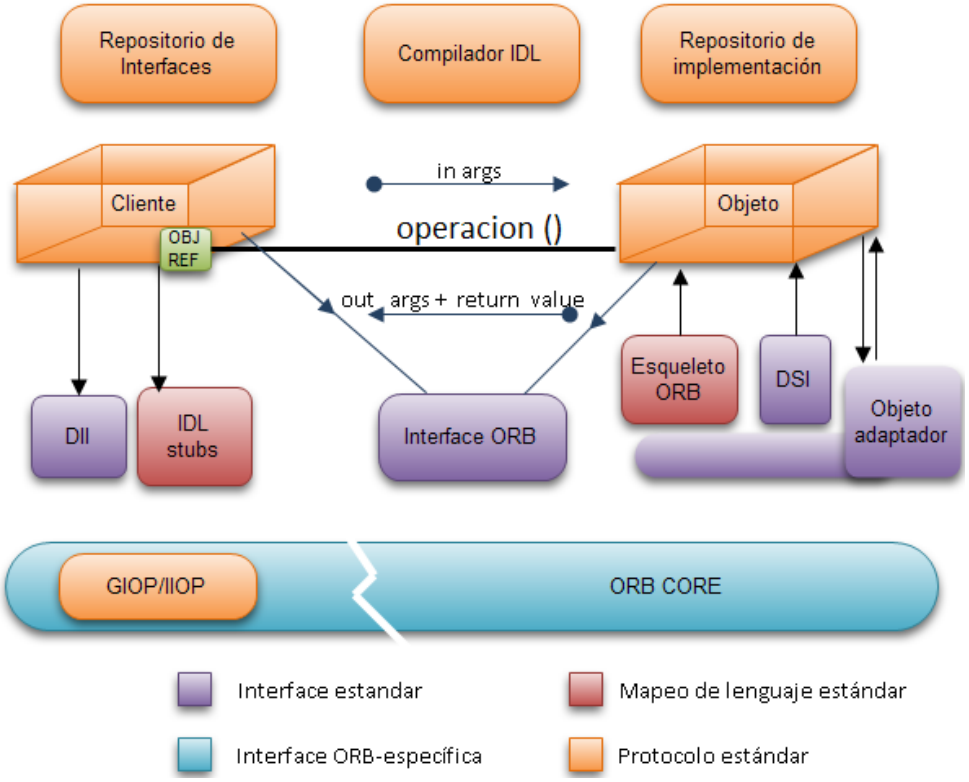


Figura No.2.8- Funcionamiento de CORBA

Con este último protocolo de administración de red se finaliza el elemento del ciclo administrativo denominado organización. Es tiempo de poner a funcionar todo lo diseñado en la parte de la planeación, sin olvidar que se realizará según lo estipulado en la etapa de organización.

2.4.3. Integración

En la etapa de integración se debe determinar el tipo de tecnología que se empleará según las necesidades de la red y lo establecido en la etapa de planeación y organización, además se deben integrar las soluciones para un óptimo funcionamiento de la red.

2.4.3.1. Tecnologías de telecomunicaciones

A continuación se presentan de forma sistemática algunas las tecnologías de telecomunicaciones más importantes que se emplean actualmente, tales como PDH (Plesiochronous Digital Hierarchy), SDH (Synchronous Digital Hierarchy) y la DWDM (Dense Wavelength Division Multiplexing), con el fin de seleccionar la tecnología que mejor se integre en la red.

2.4.3.1.1. PDH (Plesiochronous Digital Hierarchy, Jerarquía Digital Plesiócrona)

La jerarquía digital plesiócrona o PDH surge a finales de la década de los 60 del siglo XX. Hasta ese momento la transmisión telefónica era de naturaleza analógica, fue entonces cuando se comienzan los primeros esfuerzos para digitalizar el canal de voz de 4 KHz que cristalizan la aparición de PDH como una tecnología capaz de transmitir de forma simultánea múltiples canales telefónicos digitales. [61]

PDH es una tecnología usada en telecomunicaciones para transportar grandes cantidades de información mediante equipos digitales de transmisión que funcionan sobre fibra óptica, cable coaxial o radio de microondas, usando técnicas de multiplexación por división de tiempo. [56]

El término plesiócrono se deriva del griego *plesio*, cercano y *chronos*, tiempo, y se refiere al suceso de que las redes PDH funcionan en un estado donde las diferentes partes de la red están casi sincronizadas. [22]

PDH se basa en canales de 64kbps. En cada nivel de multiplexación se van aumentando el número de canales sobre el medio físico. Debido a este aumento de canales, las tramas de cada nivel tienen una estructura y duración diferentes. Además de los canales de voz, en cada trama viaja información de control que se añade en cada nivel de multiplexación, por lo que el número de canales transportados en niveles superiores es múltiplo del transportado en niveles inferiores. [61]

Existen tres jerarquías PDH, las cuales son: europea, norteamericana y japonesa. La europea usa la trama descrita en la norma G.732 de la UIT-T mientras que la norteamericana y la japonesa se basan en la trama descrita en G.733. Al ser tramas diferentes habrá casos en los que para poder unir dos enlaces que usan diferente norma, se deberá adaptar uno al otro, generalmente se convierte al formato de la jerarquía europea. [61]

T1, E1 y J1 son estándares de la jerarquía digital plesiócrona. El primero define el estándar PDH de Norteamérica, el cual consiste en 24 canales de 64 kbps dando una capacidad total de 1.544 Mbps. Por su parte E1 define el estándar PDH europeo que se conforma de 30 canales de 64 kbps y 2 canales reservados para la señalización y sincronía, dando como resultado una capacidad total de 2.048 Mbps. Finalmente el estándar J1 define el estándar PHD japonés para una velocidad de transmisión de 1.544 Mbps a través de 24 canales de 64kbps. [61]

La velocidad de transmisión de los estándares depende del número de canales y la tasa de tramas transmitidas por segundo, por ejemplo la trama del estándar J1 es de 193 ya que existen 24 canales capaces de transmitir 8 bits, multiplicando los canales por los bits se obtiene un resultado de 194, sin embargo existe un bit de sincronización el cual se ignora en la longitud de la trama. Posteriormente para obtener la velocidad de transmisión se toma en cuenta que la transmisión es de 8000 tramas por segundo, así 193 bits/trama multiplicados por 8000 tramas/segundo dan el resultado de 1, 544, 000 bps o 1.544 Mbps. [56]

En la Tabla No. 2.2 se muestran los distintos niveles de multiplexación PDH utilizados en Norteamérica, Europa y Japón.

Tabla No.2.2-Niveles de multiplexación PDH.

Nivel	Norteamérica			Europa			Japón		
	Circuitos	Kbit/s	Denominación	Circuitos	Kbit/s	Denominación	Circuitos	Kbit/s	Denominación
1	24	1,544	(T1)	30	2,048	(E1)	24	1,544	(J1)
2	96	6,312	(T2)	120	8,448	(E2)	96	6,312	(J2)
3	672	44,736	(T3)	480	34,368	(E3)	480	32,064	(J3)
4	4032	274,176	(T4)	1920	139,264	(E4)	1440	97,728	(J4)

2.4.3.1.2. SDH (Synchronous Digital Hierarchy, Jerarquía Digital Síncrona).

El desarrollo de los sistemas SDH comenzó en junio de 1986 en el seno del Grupo de Estudio VXIII de la UIT-T, el objetivo principal que se fijó este grupo fue producir una norma de alcance mundial que permitiera estandarizar los sistemas de transmisión sincrónos, obteniendo como beneficio un direccionamiento flexible y de bajo costo en la red. [16]

Algunas características de los sistemas de Jerarquía Digital Síncrona son las siguientes: [9]

- Es una jerarquía síncrona, lo que implica que el sistema funciona con un reloj maestro donde los bits son enviados en intervalos muy precisos, controlados por este reloj.
- Unifica los sistemas digitales estadounidenses, europeos y japoneses.

- Proporciona un sistema para multiplexar varios canales digitales y permite el transporte de muchos tipos de tráfico.
- Permite administrar el ancho de banda eficientemente, detecta errores y recupera de ellos la transmisión en forma transparente para las capas superiores.

SDH puede ser representada en un modelo abstracto de capas de la red de transporte en la forma en que se muestra en la Figura No.2.9, en donde se ilustra la correspondencia entre las capas de SDH y las capas de dicho modelo. [56]

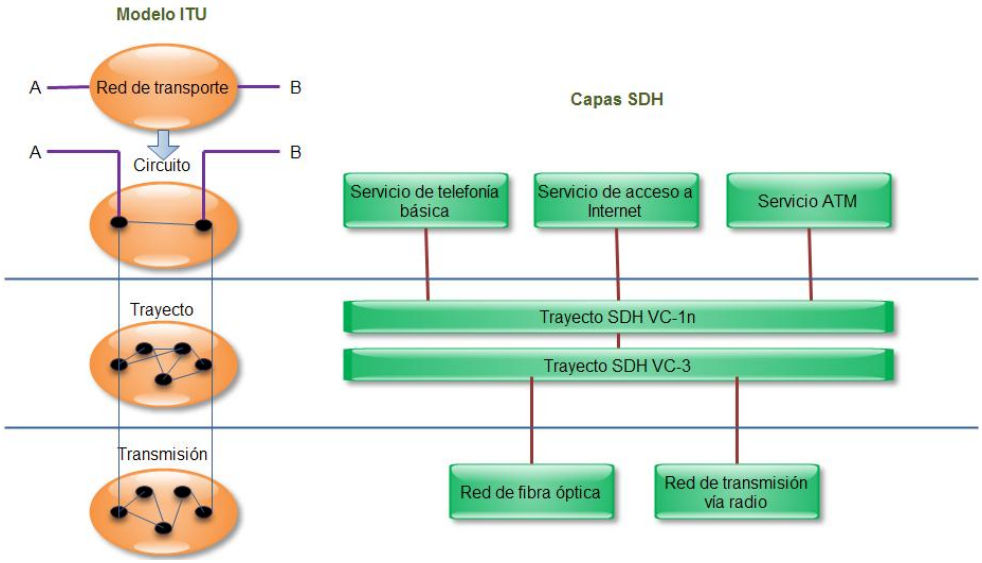


Figura No.2.9-Correspondencia entre las capas SDH y el modelo ITU.

En la capa de circuito se tienen los servicios que se pueden proporcionar actualmente a través de SDH como conexiones punto a punto. Por ejemplo la telefonía básica, acceso a internet, y el servicio ATM. [61]

La capa de trayecto de SDH se divide en dos subcapas. Esta subdivisión está relacionada con la operación de agregación o multiplexación de flujos de información que se van a transportar. Finalmente, la capa de transmisión hace referencia a los medios de trasmisión los cuales pueden ser alámbricos o inalámbricos. [61]

El sistema SDH tiene cinco niveles jerárquicos, estos parten de una velocidad básica de 155,520 Mbps para un valor de N=1, y permiten distintas velocidades según vaya variando el valor de N, tal como se muestra en la Tabla No. 2.3. [10]

Tabla No.2.3-Niveles jerárquicos SDH.

Denominación	Velocidad exacta	Valor de N	No. De canales	Velocidad simplificada
STM-1	155,520 Mbps	1	1890	155 Mbps
STM-4	622,060 Mbps	4	7560	620 Mbps
STM-16	2,488,320 Mbps	16	30240	2.5 Gbps
STM-64	9,953,280 Mbps	64	120960	10 Gbps
STM-256	39,813,120 Mbps	256	483840	40 Gbps

2.4.3.1.3. DWDM (Dense Wavelength Division Multiplexing, Multiplexación por División de Longitudes de Onda Densas)

La multiplexación por división de longitudes de onda densas es una técnica de transmisión de señales a través de fibra óptica. DWDM es muy similar a la Multiplexación por división de frecuencia, consiste en transmitir varias señales portadoras por una única fibra óptica utilizando distintas longitudes de onda (Ver Figura No.2.10). Cada portadora óptica forma un canal óptico que podrá ser tratado independientemente del resto de canales que comparten el medio, además de contener diferente tipo de tráfico. De esta manera se puede multiplicar el ancho de banda efectivo de la fibra óptica. [31]

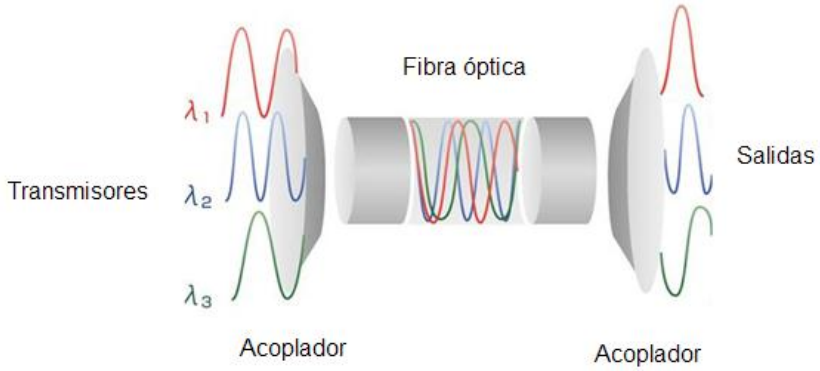


Figura No.2.10-Multiplexación por división de longitud de onda

La tecnología WDM se considera densa o DWDM a partir de 16 portadoras (canales). Para poder transmitir mediante DWDM son necesarios dos dispositivos complementarios: un multiplexor en el lado del transmisor y un demultiplexor en el lado del receptor. Actualmente se pueden conseguir 40, 80 o 160 canales ópticos de 0.8 nm y 1.6 nm, separados entre sí 100 GHz, 50 GHz o 25 GHZ respectivamente. [56]

2.4.3.2. Tecnologías de telefonía

Anteriormente se presentaron las tecnologías de telecomunicaciones más conocidas, ahora es el turno de exponer, describir y presentar las tecnologías de telefonía.

2.4.3.2.1 SS7 (Signalling System No. 7, Sistema de señalización Número 7).

SS7 es un sistema de señalización avanzado que incluye protocolos para el establecimiento de la llamada, encaminamiento y control, destinado a convertirse en estándar para las redes públicas de conmutación de circuitos y contiene los protocolos siguientes: Message Transfer Part (MTP) encargado de realizar la mayoría de las funciones de los primeros tres niveles de OSI, Signaling Connection Control Part (SCCP) que añade las funciones de direccionamiento OSI a MTP, Telephone User Part (TUP) diseñado para la telefonía vocal, Transaction Capabilities Applications Part (TCAP) que brinda servicios de red inteligente y finalmente el ISDN User Pard (ISUP) para redes de servicios integrados. [50]

SS7 consta de cuatro niveles (Ver Figura No.2.11), semejante al modelo OSI.

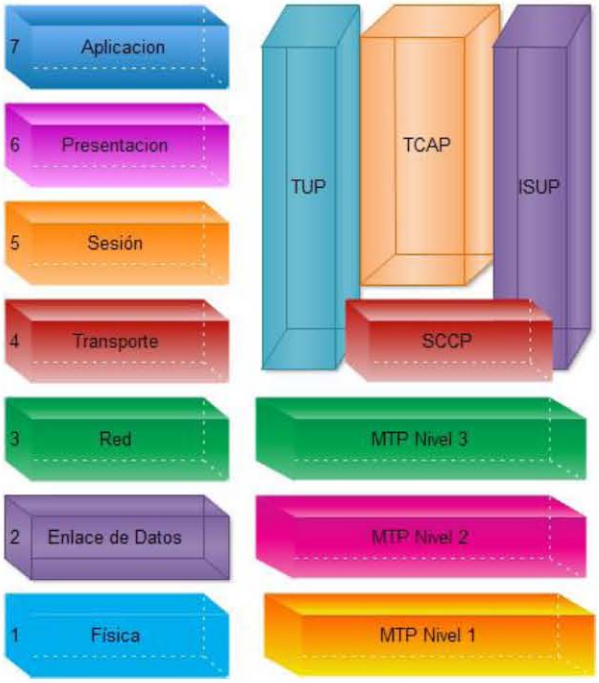


Figura No.2.11- Protocolos de SS7 con relación al modelo OSI

El sistema de señalización número 7 cuenta con una topología típica, cuyos elementos fundamentales son (Ver Figura No. 2.12): [62]

- **SCP** (Service Control Points. Puntos de Control de Servicio). Punto donde se encuentran el software y las bases de datos destinados a la administración de llamadas.
- **STP** (Signaling Transfer Points. Puntos de Transferencia de Señalización). Destinados a la traducción de los mensajes SS7 y al enrutamiento de los mensajes entre los nodos de la red y las bases de datos. Además son puntos de conmutación de mensajes entre los SCP, STP y SSP.
- **SSP** (Service Switching Points. Puntos de comunicación de servicios). Sirven de origen y destino de los mensajes SS7.

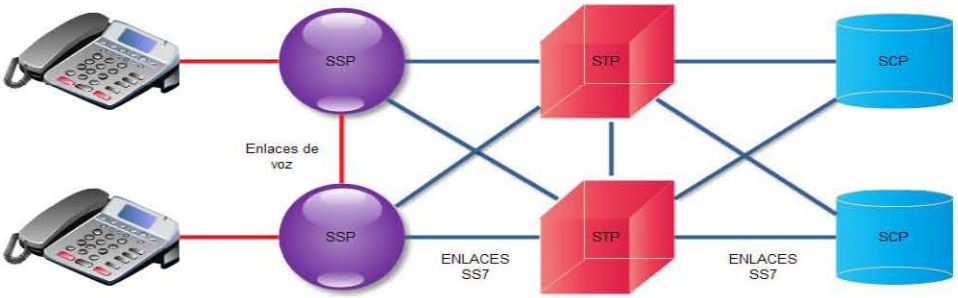


Figura No.2.12-Topología SS7

Las aplicaciones más comunes de SS7 son: el establecimiento básico, administración y finalización de las llamadas, la portabilidad de números locales (LNP, Local Number

Portability), el reenvío de llamadas, identificación de llamadas y conferencias entre varios participantes. [56]

Entre las principales ventajas de la señalización SS7 se encuentran la mejoría de la flexibilidad y velocidad en el establecimiento de la llamada, la reducción del tiempo de uso del costo de voz, señalización bidireccional, además de permitir cambios de información de señalización en tiempo real entre redes de conmutación. [56]

2.4.3.2.2. VoIP (Voice Over IP)

Voz sobre IP es una tecnología de comunicación telefónica que brinda conexiones a Internet de banda ancha, permitiendo la transmisión de la voz a través de paquetes IP. Además integra todos los servicios de datos, voz y video en un solo canal. [56]

Para comprender el funcionamiento de VoIP es necesario conocer las fases de una llamada telefónica sobre una red de paquetes, estas son: Establecimiento de la llamada y la propia conversación. En cualquiera de estas fases es necesaria la presencia de estándares que regulen y permitan la interconexión de equipos provenientes de diferentes fabricantes, tales como los protocolos de señalización y los protocolos de transporte (ver Figura No. 2.13). [56]

Figura No.2.13-Protocolos de señalización y transporte

Como se mencionó en el párrafo anterior, el proceso de una llamada requiere de protocolos de señalización, los cuales tienen como objetivo el establecimiento de las llamadas y son básicamente el núcleo de la voz sobre paquetes, diferenciándola de otros tipos de servicios. Algunas de las funciones que realizan los protocolos de señalización son: [56]

- Localización de usuarios.
- Establecimiento de sesión.
- Negociación de la sesión.
- Administración de los participantes en la llamada

Para cumplir con las funciones anteriores existen tres protocolos fundamentales: SIP (Session Initiation Protocol, Protocolo de Inicio de Sesión) H.323 y MGCP (Media Gateway Control Protocol, Protocolo de control de puerta de enlace al medio). Enseguida se describirán las características principales de cada uno de estos protocolos.

H.323 en realidad es una suite de protocolos de audio y video preparada para compartir aplicaciones con el objetivo de soportar comunicaciones multimedia sobre redes de paquetes sin conexión, ni garantía de calidad de servicio. H.323 fue desarrollado en 1996, bajo la protección de ITU, para soportar comunicaciones multimedia sobre LAN llamadas Intranets, aunque posteriormente se aplicó a la voz sobre paquetes. [70]

H.323 también tiene un control de dirección de llamadas, manejo de multimedia y ancho de banda con interfaces que permiten conectar LAN con redes de otro tipo [70]. Se considera que es un protocolo relativamente seguro debido a que emplea el protocolo RTP (Real-time Transport Protocol, Protocolo de Transporte en Tiempo Real). Una desventaja de este protocolo es que su especificación es compleja, además tiene problemas con NAT. [56]

SIP (Session Initiation Protocol, Protocolo para Inicio de Sesión) fue creado por la IETF como alternativa a H.323 en marzo de 1999. SIP es un protocolo de control de la capa de aplicación del modelo de referencia OSI, que define como establecer, modificar o finalizar una sesión entre dos o más extremos, no importando el tipo de sesión del que se trate. [70]

El SIP toma control de la señalización básica de las llamadas, activa la localización de servicios, la localización de usuario y controla los registros básicos de dicho usuario. Así mismo SIP utiliza protocolos ligeros, con poca complejidad. [70]

La arquitectura del SIP es muy similar a HTTP o SMTP, lo que significa que las solicitudes del cliente se envían a un servidor, éste las procesa y envía una respuesta al cliente. Otra característica de SIP es que está basado en la arquitectura Cliente/servidor y reutiliza la infraestructura de DNS o de SMPT. [70]

SIP considera a cada conexión como un par y se encarga de negociar las capacidades entre ellos, tiene métodos para minimizar los efectos de Negación de Servicio y utiliza un mecanismo seguro de transporte mediante TLS (Transport Layer Security, Seguridad de la capa de transporte). [56]

MGCP (Media Gateway Control Protocol, Protocolo de control de puerta de enlace al medio). Es un protocolo de dispositivos donde un Gateway esclavo es controlado por un maestro. MGCP simplifica en lo posible la comunicación con terminales como los teléfonos, utiliza una arquitectura cliente-servidor y está compuesto por: [37]

- Un MGC (Media Gateway Controller, Maestro)
- Uno o más MG (Media Gateway, Esclavo)
- Uno o más SG (Signaling Gateway, Señalización)

Con esto se concluye con los protocolos de señalización utilizados en VoIP. Junto con los protocolos de señalización funcionan los protocolos de transporte los cuales son indispensables para realizar el proceso de una llamada.

Los protocolos de transporte tienen como objetivo asegurar la comunicación de voz. Dentro de dichos protocolos se pueden encontrar al menos tres dificultades: mayor

requerimiento de ancho de banda, tráfico en tiempo real y la secuencia de carácter crítico en la generación de los datos multimedia. [56]

El RTP (Real-time Transport Protocol, Protocolo de Tiempo Real) contrarresta las dificultades mencionadas anteriormente, suministra servicios de entrega de datos en los extremos de la red en tiempo real, semejante al audio y video interactivo. Los servicios incluyen un tipo de identificación, número de secuencia, tiempo de reconocimiento y verificación de entrega, las aplicaciones corren en RTP o en UDP para hacer el uso de multiplexado y otros servicios. RTP soporta transferencia de datos hacia múltiples destinos utilizando un control distribuido definido por la red. [7]

El protocolo de control RTP (RTCP, Real-time Transport Control Protocol) se basa en la transmisión periódica de paquetes de control a todos los participantes que intervienen en una sesión, utilizando el mismo mecanismo de distribución de RTP. RTCP realiza cuatro funciones básicas: [7]

1. Brinda información sobre la calidad de los datos distribuidos.
2. Mantiene un identificador persistente en el transporte de una fuente RTP denominada nombre canónico.
3. Controla la tasa de envío en caso de que exista un número elevado de participantes.
4. Comunica un mínimo de información de control de la sesión, esta función es opcional.

2.4.3.2.3. ISD (Integrated Services Digital Network, Red Digital de Servicios Integrados)

La Red Digital de Servicios Integrados según la definición del CCITT (Comité Consultivo Internacional de Telegrafía y Telefonía), es una red emanada de la red telefónica digital integrada que suministra conectividad digital de extremo a extremo en apoyo de una gama amplia de servicios a los cuales los usuarios tienen acceso mediante un conjunto limitado de interfaces estándar. [17]

ISDN proporciona una única conexión física en las instalaciones del suscriptor, con la cual se puede disponer de varios servicios. Existen dos tipos de estructuras que se pueden emplear: [56]

- Acceso básico. Este recurso es utilizado por pequeñas y medianas empresas, debido a que permite la conexión de varios equipos terminales.
- Acceso primario. Permite utilizar hasta 30 canales y generalmente es utilizado por medianas o grandes empresas con grandes servidores para acceso remoto.

La red ISDN proporciona una mayor velocidad de acceso a Internet (64 kbps a 128 kbps), mayor calidad de voz entre usuarios que disponen de ISDN, así como una seguridad, robustez y disponibilidad superior en las líneas superiores. [56]

Los servicios de videoconferencia nacional, internacional, de voz, transmisión de datos, backups de IPL (Initial Program Load, Carga de Programa Inicial) y de internet de banda ancha son aplicaciones que proporciona la Red Digital de Servicios Integrados. [56]

2.4.3.2.4. xDSL (x Digital Subscriber Lines, x Línea de Abonado Digital).

xDSL es una familia de tecnologías de acceso a Internet de banda ancha. Todos los miembros de esta familia tienen en común dos características: [14]

1. Son técnicas de transmisión en la red de acceso. Para realizar la transmisión se requiere situar un modem en la central local y otro en el edificio del suscriptor.
2. Estas técnicas poseen una limitación respecto a la longitud del cable, dependiente del grosor y tipo del mismo.

Las principales características de las tecnologías xDSL son:

DSL (Digital Subscriber Line, Línea de Abonado Digital) fue el primer sistema xDSL normalizado, alcanza una tasa de transmisión de 160 Kbits/s sobre un único par de abonado.[47] DSL utiliza los cables de telefonía estándar para transmitir datos desde el domicilio de usuario al punto de presencia (PoP, Point of Presence) de la compañía telefónica por medio de una conexión privada punto a punto. A partir de ese punto, las señales viajan por el equipo de conmutación estándar de la compañía telefónica hasta otra conexión DSL en el destino. La Tabla No.2.4 muestra las velocidades y distancias máximas de DSL y de otras tecnologías de la familia xDSL. [56]

Tabla No.2.4-Características de la familia xDSL

Nombre de la Tecnología	Concepto	Velocidad de bajada	Velocidad de subida	Distancia máxima
IDSL	ISDN DSL	144 kbps	144 kbps	5.5 km
HDSL	High Data Rate DSL	1,544 Mbps	1,544 Mbps	3.6-4.6 km
SDSL	Symetric DSL	1,544 Mbps	1,544 Mbps	3 km
ADSL	Asymetric DSL	1,544-8,444 Mbps	640 Kbps-1,544 Mbps	3-5.5 km
RADSL	Rate Adaptive DSL	1,544-8,448 Mbps	641 Kbps-1,544 Mbps	3-5.5 km
VDSL	Very-High DSL	12.96-51.84 Mbps	1.6-2.3 Mbps	300-1400 m

2.4.3.3. Estándar IEEE 802.11

Estándar que define las características de una red de área local inalámbrica (WLAN, Wireless Local Area Network). Wi-Fi que significa Fidelidad inalámbrica es el nombre de la certificación otorgada por la Wi-Fi Alliance, grupo que garantiza la compatibilidad entre dispositivos que utilizan el estándar 802.11.

En la Tabla No. 2.5 se mencionan algunos de los estándares inalámbricos de las redes PAN, LAN, MAN y WAN, así como la velocidad, su intervalo de cobertura y las aplicaciones.[56]

Tabla No.2.5-Estándares inalámbricos

	PAN	LAN	MAN	WAN
Estándares	Bluetooth	802.11	802.11 802.16 802.20	GSM, CDMA, Satélite
Velocidad	< 1 Mbps	11 - 54 Mbps	10-100 Mbps	10Kbps-2Mbps
Intervalo de cobertura	Cortocircuito	Medio	Medio-Largo	Largo
Aplicaciones	Punto a Punto	Redes de empresas	Acceso de última milla	Dispositivos móviles

Una red local bajo el estándar 802.11 se basa en una arquitectura celular donde el sistema está dividido en células denominadas Conjunto de Servicios Básicos (BSS), a su vez cada una de las células está controlada por una estación base denominada Punto de Acceso (AP). [3]

Existen dos modos diferentes de operación para los dispositivos 802.11 denominadas topologías, las cuales son: Ad Hoc (Juego de Servicios Independientes Básicos, IBSS) e Infraestructura (Juegos de Servicios Extendidos, ESS). [25]

La topología Ad Hoc es aquella donde los dispositivos inalámbricos crean la LAN, por lo tanto no existen controladores centrales, ni de puntos de acceso. Cada dispositivo crea una conexión punto a punto, en lugar de pasar por un controlador central. Por su parte la topología de infraestructura conecta una red LAN alámbrica con una LAN inalámbrica a través de un punto de acceso (AP, Access Point). El Access Point sirve de controlador central de la red LAN inalámbrica, coordina la transmisión y recepción de los dispositivos inalámbricos en una extensión específica. En la modalidad de infraestructura puede existir más de un punto de acceso con el fin de brindar una mayor cobertura geográfica. [25]

Además de las topologías, el estándar 802.11 define tres medios de nivel físico y tres tipos básicos de trama de nivel MAC: [56]

- Medios de nivel físico

- **FHSS**, Frecuency Hopping Spread Spectrum (Espectro Extendido de Salto de Frecuencia) cuenta con 79 canales, cada uno de los cuales tiene un ancho de banda de 1 MHz. FHSS tiene una banda de frecuencia de 2.4 GHz y usa un algoritmo predeterminado para imponer cambios de frecuencia pseudoaleatorios. [69]
- **DSSS**, Direct Sequence Spread Spectrum (Espectro Extendido de Secuencia Directa). Al igual que FHSS está restringido a 1 o 2 Mbps. Cada bit se transmite como 11 chips utilizando la secuencia de Barke. Su banda de frecuencia es de 2.4 GHz y su ancho de banda de 83 MHz entre 2400 y 2483 GHz. DSSS ocupa un código por chip que tiene una velocidad de bits más alta que las señal de datos. [69]

- **Infrarrojos**, usan frecuencias en el intervalo de 850-950 nanómetros, soportando una velocidad de transmisión de 1 Mbps y una velocidad operacional de 2 Mbps, con una cobertura geográfica de 10 a 20 m. [69]

- Trama del nivel MAC [56]

- **Tramas de datos**, empleadas para transmitir datos de los niveles superiores entre estaciones.
- **Tramas de control**, encargadas de reclutar el acceso al medio de la red y de reconocer las tramas de datos transmitidas.
- **Tramas de administración,** usadas para intercambiar información de administración de la red.

2.4.3.4. Estándar IEEE 802.16

Estándar denominado WiMAX debido a sus siglas en Ingles Worldwide Interoperability for Microwave Access (Interoperabilidad mundial para acceso por microondas). Las características principales de este estándar son: radio de acción de hasta 50 km, cuenta con un gran ancho de banda, es independiente de protocolos, es capaz de transmitir otros servicios agregados como VoIP, tiene compatibilidad con antenas inteligentes. [56]

El estándar IEEE 802.16 cuenta con varias versiones: [2]

- 802.16d, empleada para los accesos de dispositivos fijos. La velocidad máxima teórica es de 70 Mbps, pero en la práctica sólo se ha alcanzado 20 Mbps en distancias de 6 km.
- 802.16e, permite la movilidad del usuario e implementa facilidades para dispositivos móviles.
- 802.16, alcanza velocidades de hasta 135 Mbps en las bandas de 10-66 GHz, acepta celdas de cobertura de 2 a 8 km, aunque es recomendable no sobrepasar los 6 km.
- 802.16a. Amplia el estándar a las bandas de frecuencia 2-66 GHz.
- 802.16m. Aún no es aprobada pero teóricamente se espera que llegue a 1 Gbps en condiciones meteorológicas perfectas.

Una vez integrada la red, las tecnologías que se usarán y lo medios que se emplearán, se procede a la dirección o ejecución del proyecto con el fin de poner la red a funcionar. Ésta etapa del ciclo administrativo se conoce como Dirección.

2.4.4. Dirección

También conocida como ejecución, comando o liderazgo, es una función de gran importancia ya que en ella se lleva a cabo la ejecución de los planes de acuerdo con la planeación, organización e integración. [64]

El administrador de red funge como el líder del equipo y será encargado de la ejecución de los planes, de motivar, guiar y conducir a su equipo de trabajo para alcanzar los objetivos y metas definidas en la planeación, así como supervisar el correcto funcionamiento de la red.

Dentro de la dirección existen principios básicos para un correcto liderazgo los cuales son: [63]

- ❖ Principio de la armonía del objetivo. La dirección será eficiente si se enfoca en el logro de los objetivos generales de la red.
- ❖ Principio de impersonalidad de mando. La presencia de un líder o una autoridad es una necesidad, ya que se requiere alguien que coordine y dirija el equipo hacia el objetivo.
- ❖ Principio de la supervisión directa. El líder debe mantener una comunicación clara con su equipo durante la ejecución de los planes con el fin de que las tareas asignadas se realicen con mayor facilidad.
- ❖ Principio de la Resolución del conflicto. El administrador debe tener la virtud de resolver los problemas que surjan durante el proyecto, a partir del momento en que aparezcan.
- ❖ Aprovechamiento del conflicto. Si se da el caso de enfrentarse a un conflicto el administrador debe usar la experiencia para experimentar, investigar y aplicar la decisión que se haya tomado para resolver el conflicto.

La etapa de dirección es de vital importancia porque pone en marcha todos los lineamientos establecidos durante la planeación y organización. A través de la dirección se logran las formas de conducta más deseables en el equipo. Una correcta dirección es determinante en la productividad y provee la comunicación necesaria para que el equipo funcione.

Un administrador de red en la etapa de dirección debe ser capaz de: [63]

- Tomar decisiones. Previamente a tomar cualquier decisión, el administrador de red debe evaluar las alternativas, definir y analizar el problema, para posteriormente aplicar la mejor decisión.
- Integrar. El líder debe reclutar a los candidatos que aspiran a un puesto determinado, posteriormente se les ambientará para finalmente capacitarlos en el desarrollo de las funciones que habrán de realizar.
- Motivar. Es la función más importante de la dirección, a través de ella se logra la ejecución del trabajo de acuerdo a normas o patrones de conducta esperados.
- Comunicarse. Es vital que el administrador sepa comunicarse con todo su equipo de trabajo de una manera respetuosa, amable y cálida
- Supervisar. Debe vigilar y guiar al equipo de tal forma que las actividades se realicen adecuadamente.

Con la red en funcionamiento, probablemente existan contratiempos que no se analizaron en las primeras etapas del ciclo administrativo. Para solucionar éste problema y mantener una red con un constante mantenimiento y mejoras, es necesario emplear el último elemento del ciclo de la administración de redes denominado control.

2.4.5. Control

El control es una etapa básica en la administración de redes, pues aunque durante el proceso se hayan creado magníficos planes, una estructura organizacional adecuada y una dirección eficiente, el administrador de red no podrá verificar cual es la situación real de la red, y no sabrá si los objetivos han sido alcanzados, hasta que realice un correcto monitoreo de red y auditorías informáticas. [56]

Otra cuestión importante en el control de la administración de redes son los privilegios que se tengan, es primordial tener un control de acceso a la información con ayuda de los adecuados métodos de seguridad informática tales como listas de control de acceso, mecanismos y herramientas de seguridad.

Para controlar el acceso a la información de la red es necesario implementar seguridad informática, no sin antes identificar qué es lo que se quiere proteger, de qué se quiere proteger y cómo se va a proteger. [55]

Generalmente el proceso de identificar lo que se quiere proteger es sencillo, la parte compleja es cuando se tiene que definir de qué se quiere proteger. A continuación se describirán las principales amenazas y ataques que existen, con el fin de conocer los diferentes tipos de atentados que una red puede sufrir.

Una amenaza es toda persona, circunstancia o evento que atente contra aquello que se desee proteger. Las amenazas de la seguridad provienen de diferentes fuentes, estas se pueden clasificar en: [55]

- **De Humanos**. Ingeniería social, fraude, robo, sabotaje, todos estos pueden ser realizados por personal interno, ex –empleados, curiosos, terroristas o intrusos remunerados.
- **De Hardware**. Bajo voltaje, ruido electromagnético, distorsión, alto voltaje, variación de frecuencia, entre otros.
- **De Software**. Caballos de troya, virus, gusanos.
- **De red**. Negación de servicio, desconexión del canal, escaneos, amenazas de monitoreo.
- **Desastres Naturales**. Incendios, temblores, terremotos, inundaciones.

Por su parte los ataques se clasifican en pasivos y activos. Los ataques pasivos son aquellos en donde el perpetrador no altera la información, sin embargo, en los ataques activos la información es modificada.

Una vez identificadas las amenazas, vulnerabilidades y ataques que se tienen en una red, es aconsejable instalar las herramientas de seguridad que se consideren necesarias, las más conocidas son: SSH (Secure Shell), Open SSH, SSL (Secure Socket Layer), Tcp wrappers, Parches, Portentry, Sniffers, Tripwire, Nmap, PEM (Privacy Enhaced Mail), IDS (Intrusion Detection System), PGP (Pretty Good Privacy), Kerberos, Firewall HoneyPots, entre muchas otras. [55]

Además de las herramientas de seguridad es importante controlar el acceso a la información y/o a la red, esto puede lograrse mediante la implementación de listas de control de acceso (ACL´s), las cuales permiten el acceso a los usuarios a determinadas aplicaciones, bases de datos u otras áreas de información, agrupándolos según el criterio de privilegios de acceso. También controlan el tráfico en routers y switches encargándose de filtrar el tráfico que pasa por ellos, permitiendo o denegando el acceso. [4]

Con el uso de herramientas de seguridad y la implementación de listas de control de acceso, se termina de implementar la seguridad, ahora se abre paso al monitoreo y control de la red mediante las auditorías informáticas.

Una auditoría informática es un examen metódico de un sistema informático, realizado de una forma puntual y de modo discontinuo, con el fin de ayudar a mejorar la seguridad, eficacia, rentabilidad de la red que se está auditando. El examen de una auditoría informática abarca una serie de controles, verificaciones, entre otros para concluir en un conjunto de recomendaciones y lo más importante un plan de acción, éste último es lo que diferencia una auditoría informática de una auditoría de gestión. [1]

El último paso en el proceso de control de una red es la elaboración de un plan de contingencia, que consiste en los pasos que se deben seguir luego de un desastre, el cual debe tener como objetivo restaurar la red y los servicios que ésta brinde en forma rápida, eficiente y con el menor costo y pérdidas. [1]

CAPÍTULO 3.

Monitoreo

3. MONITOREO

El monitoreo se ha convertido en un elemento indispensable en la administración de redes, esto se debe a que proporciona un panorama general del estado de la red mediante la recolección de paquetes que brindan información sobre el estado y los elementos de la red. Además se tiene la opción de generar alarmas que se envíen al administrador sobre los errores que se presenten.

3.1. Definición de sistema de monitoreo

Un sistema de monitoreo de red puede detectar fallas o problemas de red tales como: abuso de ancho de banda, caída de una interfaz, tipo de tráfico, entre otros. Por ejemplo, para conocer el estado de un servidor web, el software de monitoreo puede enviar peticiones HTTP. Regularmente los datos que se monitorean son el tiempo de respuesta y la disponibilidad de la red. [27]

Un sistema de monitoreo es capaz de vigilar el comportamiento de routers, switches, hubs, firewalls, servidores, computadoras, utilizando diferentes tipos de métricas, algunos ejemplos son: tráfico de entrada, de tráfico de salida, uso de CPU, uso de memoria, temperatura, entre otras.

3.2. Historia y definición de SNMP (Simple Network Management Protocol. Protocolo Simple de Administración de Red)

Un sistema de monitoreo emplea protocolos de administración de redes, los cuales fueron diseñados con el fin de permitir a los administradores un mejor manejo de los dispositivos y dar seguimiento a los eventos críticos de la red.

IETF diseñó una plataforma de trabajo que constituyó la fundación de protocolos de manejo SNMP. El primer protocolo SNMP se utilizó en el año 1988 como un protocolo provisional. Posteriormente SNMP evolucionó y dio lugar a SNMPv2 en 1993; SNMPv2c en 1995; y SNMPv3 en 1997. [59]

SNMP en cualquiera de sus versiones es un protocolo que se encuentra en la capa de aplicación del modelo OSI, desarrollado para administrar servidores, estaciones de trabajo, routers, hubs, entre otros, en una red IP. SNMP permite a los administradores de red gestionar el rendimiento de la red, localizar y resolver problemas de red y planear el crecimiento de ésta. El sistema de administración de redes se entera de los problemas en la red mediante la recepción de traps o notificaciones de cambios enviados por los dispositivos de red que tengan SNMP configurado. [70]

3.3. Componentes de SNMP

Para el protocolo SNMP una red consta de tres componentes claves: Dispositivos administrados, Administradores o Gestores (Network Management Stations, NMS) y Agentes (Ver Figura No.3.1). Un dispositivo administrado es un nodo de la red que contiene un agente SNMP, reside en una

red administrada, recolecta y guarda información de administración para enviarla a los NMS a través de SNMP, también son conocidos como elementos de red. Continuando con la descripción de los componentes claves, llegó el turno del el agente, el cual es un software de administración de red que reside en los dispositivos administrados. Un agente tiene conoce la información local de administración de red del dispositivo administrado y traduce esta información en una forma compatible con SNMP. El último componente es el NMS, encargado de ejecutar aplicaciones de monitoreo y control en los dispositivos administrados. NMS provee la mayor parte de los recursos de procesamiento y memoria requeridos para la red. [53]

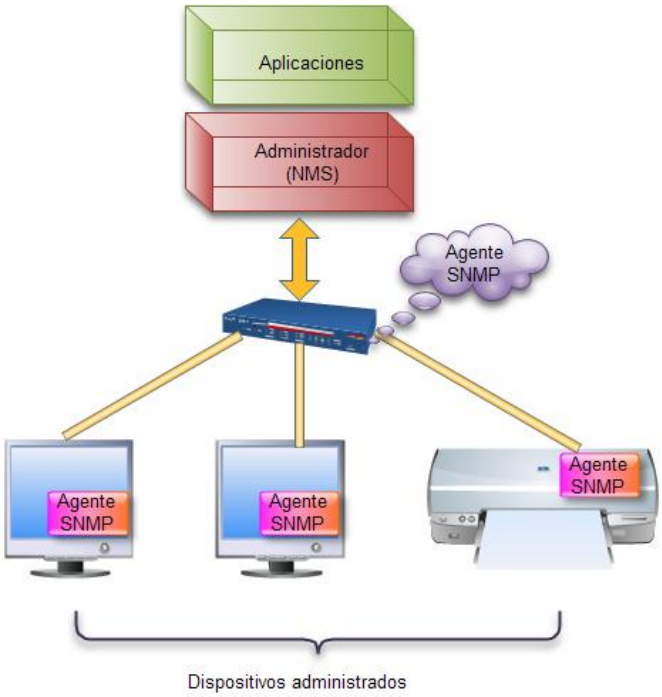


Figura No.3.1-Componentes claves de una red según SNMP

3.3.1. Estructura del protocolo SNMP

SNMP es un protocolo de aplicación que utiliza el protocolo de transporte UDP. El formato general de mensajes SNMP incluye la versión, comunidad y Unidad de Datos de Protocolo o PDU (Ver Figura No.3.2). El primer campo indica la versión de SNMP que se utiliza, el administrador y el agente deben contener el mismo número de versión, de lo contrario los paquetes se descartan. El campo de nombre de la comunidad es usado por el administrador para permitir o denegar el acceso al agente. El último campo indica el tipo y formato de las PDU para cada versión de SNMP, las cuales se explicaran en su correspondiente especificación. [53]

Figura No.3.2-Formato de los mensajes SNMP.

La arquitectura SNMP opera con un reducido grupo de objetos que se encuentran definidos en la Base de Información para la Gestión (MIB, Management Information Base), la cual es una base de datos completa, bien definida, organizada jerárquicamente y adecuada para manejar diversos grupos de objetos. [13]

Un objeto administrado, también conocido como objeto MIB, es una característica específica de un dispositivo administrado. Existen dos tipos de objetos administrados: escalares y tabulares. Los objetos escalares definen una instancia de objeto mientras que los tabulares definen múltiples instancias de objeto. Los objetos administrados se identifican mediante un OID (Object ID, Identificador de Objeto). [13]

Generalmente los objetos administrados se obtienen de la MIB-II, la cual es una base de datos común para la administración de equipos en internet, que originalmente se encontraba definida en el RFC1213. Con el nacimiento de SNMPv2 y SNMPv3 la MIB II se amplió y dividió en varios RFC´s: RFC 4293, RFC4022, RFC 4113, RFC 2863 y RFC 3418. La MIB II se compone de los siguientes nodos estructurales: [13]

- System: De este nodo dependen los objetos que proporcionan información del sistema administrado.
- Interfaces: Contiene información de las interfaces de red presentes en el sistema.
- At (Address translation, traducción de direcciones). Es un nodo obsoleto pero se mantiene para preservar la compatibilidad con la MIB-I. Almacena las direcciones del nivel de enlace correspondientes a una dirección IP.
- IP. Se almacena información relativa a la capa de red.
- ICMP. Almacena contadores de los paquetes ICMP entrantes y salientes.
- TCP. Información de la configuración, estadísticas y estado actual del protocolo TCP.
- UDP. Información relativa a la configuración, estadísticas y estado actual del protocolo UDP.
- EGP. Se encuentra la información con respecto a la configuración y operación del protocolo EGP (Exterior Gateway Protocol, Protocolo de puerta de enlace exterior).
- Transmission. Tipos de tecnologías del nivel de enlace implementadas en las interfaces de red del sistema administrado.

Estas fueron las características generales de SNMP, su estructura y su MIB, es tiempo de definir los protocolos según su versión.

3.3.2. Protocolo SNMPv1

SNMP es un protocolo desarrollado para administrar nodos en una red IP. Permite a los administradores de red gestionar el rendimiento de la red, así como encontrar, resolver problemas en la red y planear el crecimiento de la red. Un sistema de administración de red conoce los problemas de la red mediante la recepción de traps o avisos de cambio de los dispositivos de red que tienen SNMP. [53]

Como se mencionó anteriormente, existen tres versiones definidas de SNMP. A continuación se da una detallada descripción del protocolo SNMPv1, posteriormente serán descritos los protocolos SNMPv2 y SNMPv3.

SNMPv1 es un protocolo simple de petición/respuesta. El sistema de administración de red envía solicitudes y recibe las respuestas de los dispositivos administrados. Este comportamiento se implementa mediante una de cuatro posibles operaciones del protocolo: [13]

- GET usada por el administrador para recuperar el valor de uno o más objetos de un agente. Si el agente responde a la operación GET, éste no puede proporcionar valores para todas las instancias de objetos en una lista.
- GETNEXT utilizada por el NMS para recuperar el valor de la siguiente instancia objeto en una tabla o lista dentro de un agente.
- SET empleada por el administrador para establecer los valores de las instancias objeto.
- TRAP es la operación que sirve para realizar reportes o alarmas de eventos críticos.

3.3.2.1. Estructura del protocolo SNMPv1

Adopta el formato general, el cual consta de la versión, comunidad y PDU. La PDU para el protocolo SNMPv1 puede ser de tipo: GETREQUEST, GETNEXTREQUEST, GETRESPONSE, SETREQUEST o TRAP. [53]

El formato para las PDU del tipo GETREQUEST, GETNEXTREQUEST, GETRESPONSE y SETREQUEST es (Ver Figura No.3.3):

Tipo PDU	ID Solicitud	Estado Error	Index error	Objeto 1 Valor 1	Objeto 2 Valor 2	…

Figura No.3.3 Formato de las PDU SNMPv1

Dónde: [53]

- Tipo PDU especifica el tipo de PDU transmitida: 0=GETREQUEST, 1=GETNEXTREQUEST, 2=GETRESPONSE y 3=SETREQUEST.
- ID Solicitud asocia las solicitudes SNMP con las respuestas.
- Estado error indica el número y tipo de error. Este campo es utilizado por la operación GETRESPONSE, las otras operaciones deberán poner 0 en este campo
- Index error asocia un error con un objeto en particular. Sólo la operación GETRESPONSE lo utiliza, las demás operaciones deben llenar este campo con 0.
- Variables enlace, sirven como el campo de datos de la PDU de SNMPv1. Cada enlace asocia una variable de una instancia objeto con su valor actual, con la excepción de peticiones GET y GETNEXT.

Como se puede notar, el formato anterior no incluye el formato de la operación TRAP, el cual es el siguiente (Ver Figura No.3.4):

Tipo PDU	Empresa	Dirección Agente	Trap Genérico	Trap Específico	Fecha y Hora	Objeto 1 Valor 1	Objeto 2 Valor 2	…

Figura No.3.4-Formato PDU TRAP de SNMPv1

Dónde: [53]

- Tipo PDU. Especifica el tipo de PDU, en este caso 4, ya que es el identificador de la PDU Trap.

- El campo empresa identifica la administración empresarial, bajo cuya autoridad de registro se definió el trap.
- Dirección agente indica la dirección IP del agente.
- Trap genérico es el campo que describe el evento que se informa.
- Trap específico identifica un trap no genérico cuando el trap es específico de una empresa.
- Fecha y hora, calor del objeto sysUpTime, el cual representa la cantidad de tiempo transcurrido entre la última reinicialización y la generación de ese trap.

3.3.3. Protocolo SNMPv2

El protocolo SNMPv2 es una evolución del protocolo SNMPv1. Las operaciones GET, GETNEXT y SET utilizadas en SNMPv1 son exactamente las mismas que se usan en SNMPv2. SNMPv2 añadió y mejoró algunas operaciones de protocolo. Por ejemplo la operación TRAP, sirve para lo mismo que en el protocolo SNMPv1 con la diferencia de que utiliza un formato de mensaje diferente y está diseñado para reemplazar el Trap SNMPv1. [53]

SNMPv2 define dos nuevas operaciones: GETBULK utilizada para recuperar de manera eficiente grandes bloques de datos, tales como varias filas en una tabla. Además GETBULK llena mensajes de respuesta con la mayor cantidad de datos que se solicitan. La otra operación que se añadió es INFORM la cual permite a un NMS enviar un información de un trap a otro NMS y después recibir una respuesta. En SNMPv2 si el agente responde a operaciones GETBULK no provee los valores de todas las variables de la lista, provee resultados parciales. [53]

3.3.3.1. Estructura del protocolo SNMPv2

El formato del mensaje de SNMPv2 contiene versión, comunidad y PDU. Los tipos y formatos de PDU son diferentes para SNMPv1, v2, y v3. Para SNMPv2, las operaciones GETNEXT, INFORM, RESPONSE, SET y TRAP tienen el siguiente formato (Ver Figura No.3.5): [53]

Tipo	ID	Estado	Index	Objeto 1	Objeto 2	…
PDU	Solicitud	Error	error	Valor 1	Valor 2	

Figura No.3.5-Formato de las operaciones SNMPv2

Dónde: [53]

- Tipo PDU especifica el tipo de PDU transmitida: GET, GETNEXT, RESPONSE, SET o TRAP.
- ID Solicitud asocia las solicitudes SNMP con las respuestas.
- Estado error indica el número y tipo de error. Este campo es utilizado por la operación SET, las otras operaciones deberán poner 0 en este campo
- Index error asocia un error con un objeto en particular. Sólo la operación RESPONSE lo utiliza, las demás operaciones deben llenar este campo con 0.
- Variables enlace, sirven como el campo de datos de la PDU de SNMPv2. Cada enlace asocia una variable de una instancia objeto con su valor actual, con la excepción de peticiones GET y GETNEXT.

El formato de la operación GETBULK de SNMPv2 es (Ver Figura No.3.6):

Tipo PDU	ID Solicitud	No Repetidores	Repeticiones Máximas	Objeto 1 Valor 1	Objeto 2 Valor 2	…

Figura No.3.6-Formato de la operación GETBULK en SNMPv2

Dónde: [53]

- Tipo PDU especifica el tipo de PDU transmitida: GET, GETNEXT, RESPONSE, SET o TRAP.
- ID Solicitud asocia las solicitudes SNMP con las respuestas.
- No repetidores especifica el número de instancias objetos en el campo de asignaciones de variables que se deben de recuperar sólo una vez desde el inicio de la solicitud. Este campo se utiliza cuando alguno de los casos son objetos escalares con una sola variable.
- Repeticiones máximas, define el número máximo de veces que otras variables más allá de los especificados en el campo de no repeticiones, deben ser recuperadas.
- Variables enlace, sirven como el campo de datos de la PDU de SNMPv2. Cada enlace asocia una variable de una instancia objeto con su valor actual, con la excepción de peticiones GET y GETNEXT.

3.3.4. Protocolo SNMPv3

SNMPv3 agregó seguridad y capacidades de configuración remota, en comparación de las versiones anteriores. La arquitectura SNMPv3 introdujo una el modelo de seguridad basado en usuarios (USM, User-base Security Model) para la seguridad de los mensajes y el modelo de control de acceso basado en vistas (View-base Access Control) para otorgar permisos y privilegios. La arquitectura soporta el uso simultáneo de diferentes tipos de seguridad, tales como el control de acceso y los modelos de procesamiento de mensajes. Específicamente: [53]

- Seguridad.
- Autenticación y privacidad.
- Control de acceso y Autorización.
- Marco administrativo.
- Nombre de las entidades.
- Personas y políticas.
- Nombres de usuarios y administración de contraseñas.
- Destinos de notificación.
- Relaciones del proxy.
- Remotamente configurable a través de operaciones SNMP

Además SNMPv3 introdujo la habilidad de configurar dinámicamente al agente SNMP, mediante comandos SET SNMP hacia los objetos MIB que representan la configuración del agente. Esta configuración dinámica soporta la inserción, eliminación y modificación de entradas de configuración, ya sea de forma local o remotamente. [53]

3.3.4.1. Estructura del protocolo SNMPv3

La arquitectura de administración de red que maneja SNMPv3 se basa en la colección de entidades SNMP que interactúan entre sí, a su vez cada entidad está compuesta por un

motor SNMP el cual se encarga de enviar y recibir mensajes, además autentica y cifra/descifra mensajes, y controla el acceso a los objetos administrados. [53]

El formato del mensaje SNMPv3 es el siguiente (Ver Figura No.3.7):

<table>
<tr><td colspan="6">Msg Processed by MPM (Msg Processing Model)</td></tr>
<tr><td>Versión</td><td>ID</td><td>Tamaño de mensaje</td><td>Bandera de mensaje</td><td colspan="2">Modelo de seguridad</td></tr>
<tr><td colspan="6">Msg Processed by USM (User Security Module)</td></tr>
<tr><td>ID del motor autorizado</td><td>Arranque del motor autorizado</td><td>Tiempo de motor autorizado</td><td>Nombre de usuario</td><td>Parámetros de autenticación</td><td>Parámetros de privacidad</td></tr>
<tr><td colspan="6">Ámbito PDU</td></tr>
<tr><td>ID contexto del motor</td><td>Nombre del contexto</td><td colspan="4">PDU</td></tr>
</table>

Figura No.3.7-Formato mensaje SNMPv3

Dónde: [53]

- Versión indica la versión de SNMP que para SNMPv3 es 3.
- ID es un identificador único usado entre dos entidades SNMP para coordinar los mensajes de solicitud y respuesta.
- El tamaño de mensaje se refiere al tamaño máximo de un mensaje en octetos soportado por el remitente.
- Bandera de mensaje. Una cadena de octeto contiene tres banderas en los tres bits menos significativos: reportableFlag, privFlag, y authFlag.
- Modelo de seguridad. Consiste en un identificador para indicar que modelo de seguridad fue utilizado por el emisor y por lo tanto, que modelo de seguridad debe ser usado por el receptor para procesar el mensaje.
- ID del motor autorizado. Este valor se refiere al origen de un trap, response o report, y al destino de un get, getNext, GetBulk, Set o Inform.
- Arranque del motor autorizado. Se refiere al valor de snmpEngineBoots del motor SNMP autorizado para el intercambio de mensajes.
- Nombre de usuario. El usuario principal que se utiliza en el mensaje intercambiado.
- Parámetros de autenticación. Si la autenticación no es utilizada para el intercambio, el valor de este campo debe ser NULL. De lo contrario este campo se convierte en un parámetro de autenticación
- Parámetros de privacidad. Al igual que el parámetro de autenticación, si no se requiere de parámetro de privacidad se deberá colocar NULL en el campo, de lo contrario este campo se vuelve un parámetro de privacidad.
- PDU. Las PDU de SNMPv3 son las mismas que las de SNMPv2.

3.4. Historia y definición de MRTG (Multi Router Traffic Grapher)

MRTG es una herramienta que generalmente se utiliza para supervisar la carga de tráfico en los enlaces de red, las temperaturas, el uso de memoria RAM, carga del CPU, entre otros. MRTG es capaz de generar páginas de HTML que contienen imágenes gráficas que proporcionan una representación visual de lo que se desee visualizar. [13]

La historia de MRTG comienza en 1994, cuando Tobias Oetiker se encontraba trabajando en un sitio donde se tenía una línea de 64 kbps hacia el mundo exterior, este enlace provocó el interés de las personas en conocer la forma en que el enlace se llevaba a cabo, fue entonces cuando Oetiker decidió crear un código corto que creara un gráfica que se actualizara constantemente en la web, la cual mostrara la carga de tráfico en el enlace a Internet. Con el paso del tiempo el código se convirtió en un script configurable escrito en Perl llamado MRTG-1.0, lanzado en la primavera de 1995. [28]

Después de algunas actualizaciones, Oetiker decidió dejar su trabajo en la DMU para empezar a trabajar en el Instituto Federal Suizo de Tecnología. Debido a sus grandes ocupaciones, tuvo que abandonar por un tiempo el proyecto MRTG. Fue en enero de 1996 cuando recibió un correo de Dave Rand, el cual le cuestionaba sobre la deficiente velocidad de MRTG. Oetiker envió un correo explicándole a Dave que la programación de MRTG no era lo suficientemente eficiente y que ésta había sido escrita completamente en Perl. Después de una semana o más, Dave le envió un correo a Tobias diciéndole que había tomado la justificación del correo para intentar mejorar la velocidad de MRTG, pero los cambios no fueron suficientes, así que además de esta breve explicación, Dave escribió y adjuntó el código de las secciones de tiempo crítico de MRTG en C. Este código mejoró la velocidad de MRTG en un factor de 40! , razón por la cual Tobias decidió desarrollar MRTG-2. [28]

Poco después del comienzo del desarrollo de MRTG-2, Tobias empezó a dar copias betas a las personas interesadas. A cambio estas personas contribuyeron para lo que actualmente se conoce como MRTG. [28]

3.4.1. Características de MRTG [28]

MRTG consiste en un script de Perl que utiliza SNMP para leer las variables que se deseen monitorear y un programa en C que registra todos los datos con los cuales se crean las gráficas que son colocadas en páginas web que pueden ser vistas desde cualquier navegador web moderno.

Además de una vista diaria detallada, MRTG crea representaciones visuales semanales, mensuales y anuales. Esto es posible gracias al registro de todos los datos que mantiene MRTG. Este registro está configurado para que no se expanda con el tiempo, no obstante contiene todos los datos relevantes de las variables en los últimos dos años. [54]

Otras características de MRTG son:

- Portabilidad. MRTG trabaja en plataformas UNIX y en Windows NT.
- Utiliza una implementación SNMP altamente portátil escrita en Perl, por lo que no es necesario instalar ningún paquete SNMP externo.

- MRTG puede leer los contadores de 64 bits de SNMPv2.
- Los archivos de registro no crecen gracias a la utilización de un algoritmo de consolidación de datos único.
- La instalación de MRTG es muy sencilla gracias a un conjunto de herramientas de configuración.
- El aspecto de las páginas web producidas por MRTG son muy fáciles de configurar.
- MRTG se ejecuta como un demonio. Por defecto, cada cinco minutos recolecta la información de los dispositivos y ejecuta los scripts que se le indican en la configuración.
- En primera instancia, MRTG consultaba la información, la procesaba y generaba el informe y las gráficas. En las últimas versiones, la información se almacena en una base de datos a partir de la cual, y de forma separada se generan los informes y las gráficas, tal como lo hace el que se encuentra instalado en el servidor Sun Blade 6000.

CAPÍTULO 4.

Análisis del servidor

4. ANÁLISIS DEL SERVIDOR

En esta sección se dan a conocer todas las características técnicas del servidor ORACLE-SUN Blade, algunas de ellas son:

- Elementos del servidor
- Capacidad de almacenamiento
- Capacidad de memoria RAM
- Tipo de procesadores
- Conexiones del servidor
- Sistemas operativos que albergan en él

4.1. Características técnicas del ORACLE-SUN Blade 6000

El sistema modular Sun Blade 6000, es un sistema optimizado de servidores blade para aplicaciones de alto rendimiento, las cuales exigen una gran demanda de rendimiento de CPU, capacidad de memoria y ancho de banda de entrada y salida. El sistema soporta hasta 10 módulos de servidor (también conocidas como cuchillas) por chassis. El diseño del sistema provee una infraestructura de energía y refrigeración, capaz de soportar CPU's actuales y futuros, así como configuraciones de memoria, de tal forma que aseguran que el ciclo de vida del chassis tenga una duración de varias generaciones de módulo de servidor. El sistema brinda una arquitectura unificada y flexible que le permite consolidar múltiples entornos operativos y aplicaciones. [45]

4.1.1. Componentes del sistema modular Sun blade 6000

El sistema modular SUN BLADE 6000 cuenta con 10 módulos de servidor, dos fuentes de alimentación y dos módulos de ventilador en la parte frontal del chassis, tal como lo muestra la Figura No.4.1. En la parte trasera se encuentran los Módulos Express PCI, dos módulos express de red (NEMs, Network Express Modules), un módulo de administración de chassis (CMM) y seis módulos de ventilador (Ver Figura No.4.2). Todos los componentes del chassis que son fundamentales y críticos para la operación del sistema, son configurados de una manera redundante. [68]

El sistema Sun Blade 6000 está diseñado para brindar facilidad de servicio tanto al cliente como para el personal autorizado. [68]

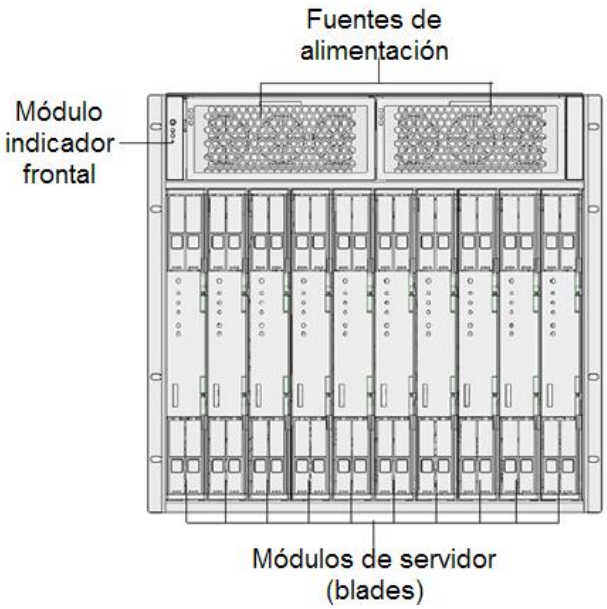


Figura No.4.1- Vista Frontal del Sun Blade

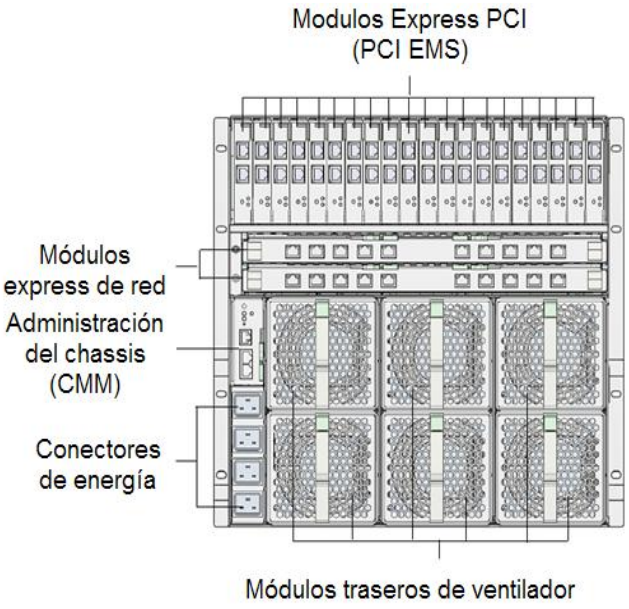


Figura No.4.2-Vista trasera del Sun Blade

La conectividad de entrada y salida está basada en Módulos Express PCI (PCI EMs) y en Módulos Express de red (NEMs). Los PCI EMs proveen funciones dedicadas de entrada y salida para cada módulo. Hay dos PCI EMs por cada módulo servidor, existe un máximo de 20 PCI EMS por chassis. Los PCI EMs disponibles incluyen: [68]

- Dual-port Gigabit Ethernet PCI EM. (Empleado en el Sun Blade del CENAPRED)
- Dual-port Fibre Channel PCI EM.
- Dual-port 4X InfiniBand PCI EM

Como se mencionó anteriormente, el sistema modular SUN BLADE 6000 cuenta con un módulo de gestión que generalmente se conoce como CMM.

CMM proporciona una interfaz serial RJ-45 y dos conectores Ethernet RJ-45. Los usos principales de la CMM son proporcionar: [68]

- Control automático de la velocidad del ventilador del chassis.
- Una interfaz de línea de comandos (CLI) que permita utilizar comandos para controlar y conocer el estado de los componentes presentes en el chassis. La CLI utiliza comandos para:
  - ✓ Mostrar componentes presentes.
  - ✓ Visualizar componentes de datos FRU SEEPROM.
  - ✓ Revisar el estado de los componentes.
  - ✓ Configurar los parámetros de red CMM.
  - ✓ Configurar los parámetros de red del módulo de servidor SP (Service Processor, Procesador de servicios).
  - ✓ Conectar al módulo de servidor SP CLI a través de ssh

Además de CMM Oracle brinda un complemento llamado ILOM debido a su nombre en inglés Integrated Lights Out Manager (Ver Figura No.4.3), el cual es un firmware de administración del sistema que permite administrar el servidor aunque el sistema host esté apagado. Esto es

posible gracias a que ILOM se ejecuta en otro procesador de servicio, uno para cada nodo del módulo servidor, que se enciende con la energía en espera del chassis. [68]

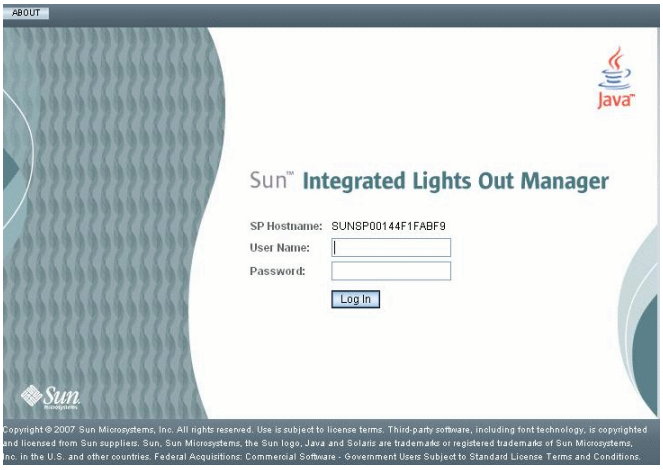


Figura No.4.3-Página de inicio ILOM

ILOM permite administrar y supervisar activamente el servidor independientemente del estado del sistema operativo. Algunas de las funciones de ILOM son: [21]

- Obtener información sobre errores de hardware conforme éstos se presenten.
- Controlar de forma remota el estado de energía del servidor.
- Ver las consolas gráficamente y no gráficamente correspondientes al host.
- Supervisar las medidas de consumo del módulo de servidor de energía.
- Ver el estado actual de los sensores y de los indicadores del sistema.
- Determinar la configuración del hardware del sistema.
- Recibir alertas generadas relativas a eventos del sistema, utilizando capturas SNMP, PET de IPMP o alertas por correo electrónico.
- Acceder a diagnósticos admitidos a través de ILOM para el sistema.

Además de todas las características mencionadas, el sistema modular SUN BLADE 6000 cuenta con las características RAS (Reliability, Availability y Serviceability-Confiabilidad, Disponibilidad y Mantenimiento). Estas características son aspectos del diseño de un sistema que afectan su capacidad de operar constantemente y de minimizar el tiempo necesario para el servicio del sistema. La confiabilidad se refiere a la capacidad del sistema de funcionar de manera continua y sin errores, manteniendo íntegros los datos. La disponibilidad se refiere a la capacidad del sistema para volver a funcionar con normalidad tras un fallo con un impacto mínimo. Mantenimiento hace referencia al tiempo que se tarda en restaurar el sistema después del fallo de un componente. En conjunto, las características del sistema modular SUN BLADE 6000 brindan un sistema capaz de operar continuamente. [68]

Para cumplir con las características RAS, el SUN BLADE cuenta con componentes redundantes que permiten al sistema continuar operaciones en caso de que uno de los componentes asociados falle. Esta separación de funciones reduce al mínimo el impacto de los componentes y el mantenimiento. [68]

Los componentes redundantes incluyen: [68]

- ✓ Fuentes de alimentación.
- ✓ Sistema de ventiladores (frontal y trasero)

Los siguientes módulos podrían ser redundantes, dependiendo la configuración de sistema. [68]

- ✓ Módulos de servidor.
- ✓ Módulos Express PCI.
- ✓ Módulos Express de red.

El sistema modular SUN BLADE 6000 cuenta con un sistema de monitoreo de entorno, el cual está diseñado para proteger los componentes de: [68]

- Temperaturas extremas.
- Falta de flujo de aire adecuado a través del sistema.
- Problemas de administración de energía.
- Problemas de hardware.

Los sensores de temperatura monitorean la temperatura ambiente del chassis y de los componentes internos. El software y el hardware hacen que la temperatura dentro del chassis no exceda determinados valores de temperatura. Si la temperatura registrada sale del rango de temperaturas especificados, el subsistema de software de monitoreo enciende en color ámbar los leds que se encuentran en la parte frontal y trasera del sistema. Si la temperatura persiste, el sistema puede iniciar un apagado. [68]

4.2. Hardware del ORACLE-SUN Blade 6000

El sistema Modular Sun Blade 6000 brinda una mayor flexibilidad respecto a otras plataformas. Además utiliza los microprocesadores de más alto desempeño de la industria Sun, Intel, AMD y proporciona soporte para los sistemas operativos Solaris, Windows y Linux. El aumento en la capacidad de memoria y mayor ancho de banda (E/S) convierte a Sun Blade 6000 en la plataforma de virtualización óptima. [36]

El sistema Modular Sun Blade 6000 que se encuentra dentro de las instalaciones del CENAPRED incluye los siguientes componentes:

- Chassis Sun Blade 6000, usado para el procesamiento.
- 4 Sun Blade X6250, utilizados para procesamiento.
- Sun StorageTek 2530, ocupado para el almacenamiento

4.2.1. Chassis SUN BLADE 6000

El Chassis Sun Blade 6000 soporta hasta 10 servidores con características de alto rendimiento. Con 6.4 Terabits por segundo máximos de rendimiento de E/S y hasta 10 módulos de servidor por chassis que ofrece hasta 960 núcleos por rack y hasta 10.24 TB de memoria por rack. [45]

La arquitectura modular y los componentes intercambiables del chassis Sun Blade 6000 (Ver Figura No.4.4), permiten consolidar una amplia gama de aplicaciones de centro de datos comparada con la que es posible con la computación tradicional Blade. Esto reduce notablemente los costos de la virtualización y aplicaciones empresariales, al mismo tiempo que facilita el desarrollo acelerado de los sistemas de producción y alta disponibilidad. [45]

Figura No.4.4-Chassis Sun Blade 6000, componente intercambiable.

A diferencia de los blades que compiten con el chassis Sun Blade, éste último tiene un diseño que simplifica la administración, el mantenimiento, y facilita la integración con infraestructura existente para reducir aún más los costos. El chassis Sun Blade 6000 puede ser rápidamente integrado dentro de su infraestructura de administración usada con varias herramientas para terceros, gracias a su consola remota Javabased. Esto elimina la complejidad innecesaria y permite una infraestructura TI heterogénea sin ningún entrenamiento o herramientas especiales. [45]

Algunas características técnicas del Chassis son: [45]

- Para las interfaces de entrada y salida es capaz de soportar los siguientes protocolos: PCIe 2.0, SAS 2.0, SATA 3.0, y Gigabit Ethernet (GbE); cada módulo de servidor tiene una conexión directa con 2 PCIe EMs y dos NEMs.
- Las temperaturas que tolera el chassis mientras está en funcionamiento son de 5°C a 32°C, el ambiente óptimo es de 22°C, si no está operando puede soportar temperaturas de entre -40°C a 65°C.
- La altitud que soporta cuando está funcionando es de hasta 3,048 m.
- Administración de energía: AC 1+1 PSU, 6,272 W, o 6,400 VA en cada fuente de alimentación.
- Voltaje: 200-240 V AC.
- Frecuencia: 50Hz-60Hz.

4.2.2. Módulo de servidor SUN BLADE X6250

Desarrollado por los procesadores Intel Xeon, el módulo de servidor Sun Blade X6250 de Oracle, es ideal para las demandas de la Web y niveles de aplicación, así como la computación técnica de alto rendimiento. El módulo de servidor está diseñado para ofrecer mayor rapidez al procesador Intel Xeon. El Sun Blade X6250 ofrece un rendimiento superior y excelentes características en un tamaño compacto, ayudando a mejorar el tiempo de comercialización (Ver Figura No. 4.5). [44]

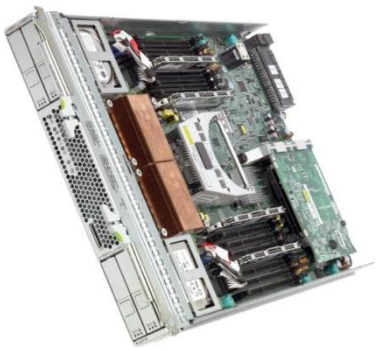


Figura No.4.5- Módulo de servidor SUN BLADE X6250

El Sun Blade X6250 es el único servidor basado en procesadores Intel Xeon de dos núcleos que ofrece una capacidad ilimitada de E/S y 64 GB de memoria, totalmente accesible en una configuración de un solo CPU. Las características del X6250 son la escalabilidad, debido a que ofrece una densidad de memoria alta de hasta 64GB de RAM por cada blade, además brinda la oportunidad de consolidar la infraestructura del centro de datos en menos espacio y más potencia y uso eficiente del espacio que provoca una disminución considerable de costos. [44]

La capacidad de almacenamiento de Sun Blade X6250 ayuda a eliminar los cuellos de botella, mientras que la memoria permite sacar el máximo provecho de los CPUs. [44]

4.2.3. Sun StorageTek 2530

El Sun StorageTek 2530, combina la nueva generación de tecnología serial-attached SCSI (SAS), a prueba de tiempo de los diseños de almacenamiento externo, y la administración de software para crear un sistema de almacenamiento idealmente equipado para los requerimientos de SMB. Su diseño modular crea un punto de entrada asequible sin sacrificar la escalabilidad futura que permite a los clientes empezar poco a poco e ir creciendo cuando estén listos (Ver Figura No.4.6). [38]

Figura No.4.6- Sun StorageTek 2530.

Entre las características más importantes del Sun StorageTek 2530 se encuentran: [38]

- Tecnología de interfaz SAS que proporciona un alto rendimiento en cada puerto SAS de 3 Gb/seg.
- Soporte para el alto rendimiento de SAS y/o alta capacidad de unidades SATA.
- Aprovechamiento de las generaciones de desarrollo de almacenamiento Sun para una mejor tecnología.
- "Comenzar con algo pequeño, hacerlo crecer", significa que cuenta con escalabilidad que permite la expansión de hasta un total de 48 unidades.
- Software Sun StorageTek Common Array Manager (CAM), simple de manejar y administrar.
- La solución a la elección de topologías clúster de dos nodos, proporcionando alta disponibilidad y redundancia.

Lo anterior describió las capacidades de almacenamiento, características generales de los componentes del sistema modular Sun Blade 6000, a continuación se mencionan las características específicas del Sun Blade 6000 que se encuentra en el Centro Nacional de Prevención de Desastres.

CHASSIS SUN BLADE 6000. Tiene la capacidad de ser multiplataforma, mejor rendimiento y es de bajo costo.

MÓDULO DE SERVIDOR SUN BLADE X6250. Se cuentan con 4 de estos módulos de servidor, cada uno tiene 2 procesadores Intel Xeon Quad Core 3Ghz, arreglo entre discos RAID1 de 146 GB y 32 GB de memoria RAM expandible a 64 GB.

SUN STORAGE TEK 2530. Arreglos entre discos RAID5, Serial SCSI, 3 Gb/s, 12 discos SATA de 1 TB y disco SPARE.

4.3. Software del ORACLE-SUN Blade 6000

Como se mencionó en la parte del hardware, el sistema modular Sun Blade 6000, tiene la capacidad de soportar 10 módulos de servidor, actualmente en el CENAPRED se cuentan con 4 módulos de servidor (Ver Figura No.4.7).

Figura No.4.7-Foto del Sun Blade 6000

Dentro de los módulos de servidor se tienen sistemas operativos, estos pueden ser Solaris, Windows o Linux. En el caso del Sun Blade del CENAPRED se tienen tres módulos de servidor con Windows Server 2008 y uno con Red Hat Enterprise Linux 5.

Según Microsoft, Windows Server 2008 está diseñado para ofrecer a las organizaciones la plataforma más productiva para la virtualización de cargas de trabajo, creación de aplicaciones eficaces y protección de redes. Además ofrece una plataforma segura y de fácil administración para el desarrollo y alojamiento confiable de aplicaciones y servicios web. [43]

Windows Server proporciona a los profesionales de Tecnologías de la Información un mayor control sobre los servidores e infraestructura de red, y les permite centrarse en las necesidades críticas del negocio o proyecto. La instalación y administración basadas en funciones con Administrador del servidor facilita la tarea de administrar y proteger las múltiples funciones de servidor en una empresa. [43]

Otra de los beneficios que Windows Server 2008 aporta es la seguridad mejorada, la cual aumenta la protección del sistema operativo mediante una base sólida para dirigir y construir un negocio o proyecto según sea el caso. Incluye innovaciones de seguridad que reducen la exposición de ataques del núcleo, lo que produce un entorno de servidor más seguro y estable. [43]

Por su parte el sistema operativo Red Hat Enterprise Linux 5 es una plataforma empresarial apropiada para una amplia gama de aplicaciones de la infraestructura de las Tecnologías de Información. Según la encuesta sobre el calor de los proveedores realizada por la revista CIO Insight, los gerentes de tecnologías de información colocaron a la calidad de la tecnología de Red Hat Enterprise Linux en el primer nivel de la lista de proveedores de software durante los últimos años. [48]

Red Hat Enterprise Linux ofrece un mayor tiempo productivo, reduce el tiempo de inactividad, lo que permite invertir el tiempo en tareas de TI más estratégicas. Las infraestructuras de TI actuales son compatibles con múltiples plataformas y proveedores. [48]

Los sistemas operativos de Sun Blade 6000 tienen una función específica, cada uno de ellos tiene asociado un nombre y un numero de Blade, tal como lo muestra la Tabla No.4.1.

Tabla No.4.1-Asociación de SO con nombres

No. Blade	Nombre	Sistema Operativo
B0	SER1	Windows Server 2008
B1	SER2	Red Hat Enterprise Linux 5
B2	SER3	Windows Server 2008
B3	SER4	Windows Server 2008

Los nombres asignados a cada Blade tienen relación con su función y la información que resguardan. A continuación se menciona la información principal que resguarda cada sistema.

SER1: Es el servidor encargado de almacenar y proveer las imágenes correspondientes al Área del Atlas Nacional de Riesgos.

SER2: En este servidor se encuentra alojado el portal web del Área de Sistemas de Información Sobre Riesgo.

SER3: La importancia de este servidor radica en que dentro de éste se encuentra la base de datos de ArcSDE. ArcSDE es un servidor de software producido y comercializado por ESRI, el cual tiene por objeto permitir el uso de Sistemas de Administración de Bases de Datos Relacionales para datos espaciales. Los datos espaciales se pueden utilizar como parte de una base de datos geográfica.

SER4: Dentro de este servidor se encuentra el ArcGIS, la cual es una herramienta que agrupa varias aplicaciones para la captura, edición, análisis, tratamiento, diseño, publicación e impresión de información geográfica.

La Figura No.4.8 es un ejemplo ilustrativo sobre los sistemas operativos del Sun Blade y sus operaciones, como se puede observar, SER1, SER3 y SER4 se mantienen en comunicación debido a la necesidad de intercambiar información.

Figura No.4.8-Funciones de los módulos de servidor.

4.4. Conexiones del ORACLE-SUN Blade

El Oracle Sun Blade 6000 cuenta con la característica de alta disponibilidad gracias a que tiene dos interfaces configuradas de tal modo que si una llega a fallar, la otra inmediatamente toma el lugar de la interfaz caída. Dentro de este sistema cada blade cuenta con una dirección IP primaria, por la que se puede conectar vía escritorio remoto o por medio de SSH, el modo de acceso depende del sistema operativo que se use.

Además de la dirección primaria, existen direcciones web que son utilizadas por el ILOM, para tener acceso mediante una aplicación de internet a cada sistema operativo.

En la Tabla No.4.2 se muestran las direcciones IP para acceder a cada Blade vía Web, así como el sistema operativo asociado, el nombre y la interface.

Tabla No.4.2-Relación de nombres, IP´s y sistemas operativos del Sun Blade.

Interface	Dirección IP	Uso	Tipo de acceso	Nombre	Sistema Operativo
NetMgt	192.168.1.5	CMM Management Port	Web	Chassis	-
NetMgt : BL0	192.168.1.1	Blade 0 ILOM	Web	SER1	Windows Server 2008
NetMgt : BL1	192.168.1.2	Blade 1 ILOM	Web	SER2	Red Hat Enterprise Linux
NetMgt : BL2	192.168.1.3	Blade 2 ILOM	Web	SER3	Windows Server 2008
NetMgt : BL3	192.168.1.4	Blade 3 ILOM	Web	SER4	Windows Server 2008

Como se mencionó anteriormente, los módulos de servidor también cuentan con IP´s primarias y de pruebas, en las siguientes tablas se muestra la relación de éstas direcciones con cada Blade en específico: SER1 (Ver Tabla No.4.3), SER2 (Ver Tabla No.4.4), SER3 (Ver Tabla No.4.5), SER4 (Ver Tabla No.4.6).

SB6250 SER1 (Windows Server 2008)

Tabla No.4.3-IP´s de SER1.

Interface	Dirección IP	Uso	Tipo de acceso
Network Bridge	192.168.1.10	Dirección primaria	Escritorio remoto
Local Area Connection	-	Interfaz	-
Local Area Connection 2	-	Interfaz	-

SB6250 SER2 (Red Hat Enterprise Linux)

Tabla No.4.4-IP´s de SER2

Interface	Dirección IP	Uso	Tipo de acceso
bond0	192.168.1.11	Dirección primaria	SSH
eth0	-	Interfaz	-
eth1	-	Interfaz	-

SB6250 SER3 (Windows Server 2008)

Tabla No.4.5-IP´s de SER3

Interface	Dirección IP	Uso	Tipo de acceso
Network Bridge	192.168.1.12	Dirección primaria	Escritorio remoto
Local Area Connection	-	Interfaz	-
Local Area Connection 2	-	Interfaz	-

SB6250 SER4 (Windows Server 2008)

Tabla No.4.6-IP´s de SER4

Interface	Dirección IP	Uso	Tipo de acceso
Network Bridge	192.168.1.13	Dirección primaria	Escritorio remoto
Local Area Connection	-	Interfaz	-
Local Area Connection 2	-	Interfaz	-

CAPÍTULO 5.

Planeación

5. PLANEACIÓN

En ese capítulo se justifican los motivos por los cuales se elegirá el sistema operativo sobre el cuál se implementa el sistema de monitoreo, los requerimientos de software y hardware que éste debe tener.

Por otra parte se planea y argumenta las elecciones de las variables a monitorear, dependiendo la importancia que tienen en el sistema, el daño que puedan causar y el impacto que tengan dentro del Centro Nacional de Prevención de Desastres.

Una vez elegidas las variables a monitorear, se explica la forma en que se envían las alertas cuando éstas variables tomen un valor determinado, estas alertas se conocen como traps.

5.1. Sistema operativo

En este subtema se fundamenta la elección del sistema operativo, pero se comienza contestando preguntas básicas como ¿Qué es un sistema operativo?, ¿Cuáles son su funciones principales? ¿Cuáles son sus elementos claves? ¿En qué se debe de basar para elegir al mejor?

La definición técnica de sistema operativo es: Conjunto de programas que, ordenadamente relacionados entre sí, contribuyen a que la computadora lleve a efecto correctamente el trabajo asignado. [58]

Por otro lado, desde el punto de vista del usuario, éste definiría el sistema operativo como un conjunto de programas que facilitan el acceso al hardware, ofreciendo una forma sencilla y flexible de acceso al mismo.[69] Dentro de los sistemas operativos se pueden clasificar cuatro grandes grupos, cada uno de ellos responsable de la administración de los distintos tipos de recursos de la computadora. Estos grupos son (Ver Figura No.5.1): [60]

Figura No.5.1-Estructura en capas de un SO

- Administrador del procesador. Encargado de administrar los programas que se han de ejecutar en la computadora y cómo han de hacerlo.

- Administrador de entrada/salida. Conjunto de rutinas y datos necesarios para administrar los dispositivos hardware de E/S.
- Administrador de la memoria. Se encarga de administrar el uso de la memoria de forma segura y eficiente.
- Administrador de información o de ficheros. Permite organizar la información que se va generando y almacenando en el sistema.

Estos cuatro administradores junto con el sistema operativo tienen dos objetivos fundamentales: Seguridad y Abstracción. [60]

Con lo que respecta a la seguridad, el sistema operativo debe actuar contra cualquier manipulación extraña, ya sea accidental o premeditada que pudiera dañar la información, perjudicar a otros usuarios o provocar un funcionamiento indeseado del sistema. Por otra parte la abstracción se refiere a la tendencia actual del software y de los lenguajes de programación por ocultar lo más que se pueda los detalles de más bajo nivel, intentando dar a los niveles superiores una visión más abstracta. Los datos u objetos sólo serán accesibles a través de las funciones que operan con ellos. Gracias a la abstracción, los sistemas operativos enmascaran los recursos físicos, permitiendo su manejo con funciones más generales que ocultan las básicas, constituyendo verdaderos recursos ficticios o virtuales, que se mejoran y son más potentes que los físicos. [60]

Además de los principales objetivos de los sistemas operativos, éstos también ofrecen servicios tales como: [60]

- Administración de la información, de tal modo que facilita el almacenamiento de los datos en medios magnéticos, y proporciona funciones de recuperación de dichos datos.
- Administración del hardware. Control directo del CPU, la memoria, los discos, las pantallas, el teclado, y todos aquellos dispositivos que permitan realizar las tareas dirigidas al usuario y a los programas que se ejecutan en la computadora.
- Interfaz de usuario, la cual permite al usuario trabajar con el sistema operativo, controlando el hardware, los programas, administrando los usuarios, el espacio en disco, permitiendo la facturación del uso. En realidad, la interfaz de usuario no forma parte del núcleo del sistema operativo, pero es un componente inseparable del mismo, y es el que ofrece su aspecto o parte visible al usuario.

Una vez definidos los conceptos generales de sistema operativo, es tiempo de decidir sobre qué sistema operativo se implementará el sistema de monitoreo, para el cual se tienen dos opciones: Windows Server 2008 y Red Hat Enterprise Linux 5, donde Windows es una distribución de Microsoft Windows y Red Hat de Linux.

Actualmente las empresas Microsoft y Linux compiten por el usuario básico en el mercado de las computadoras personales, así como el mercado de los servidores, y se utilizan en agencias del gobierno, escuelas, oficinas, hogares, servidores de intranet y de internet, supercomputadoras y sistemas integrados.

Windows tiene un éxito rotundo en las computadoras personales y de escritorio, logrando acaparar el 90% de dichas computadoras, mientras que Linux toma la delantera en las supercomputadoras más poderosa, abarcando el 85% de ellas. [23]

Linux y Windows varían en facilidad de instalación, facilidad de uso, apariencia, estabilidad, seguridad, entre otros (Ver Tabla No.5.1). Ambas distribuciones buscan fortalecer sus debilidades, el área débil de Windows es la estabilidad, por su parte Linux maneja un pobre escritorio para el mercado popular. [23]

Característica	Windows	Linux
Facilidad de Instalación	En Windows Server 2003 y anteriores, la instalación se realiza en dos etapas; la primera en modo texto y la segunda en modo gráfico. Para la versión Vista, Seven y Server 2008 la instalación solo se realiza en modo gráfico	Varía mucho según la distribución. Las distribuciones de propósito general ofrecen un live CD o un instalador con GUI (Graphical User Interface, Interfaz Gráfica de Usuario) como es el caso de Red Hat. Dependiendo el fin del sistema, éste también puede ser instalado por archivos fuentes que deben ser copiados y compilados.
Tiempo de instalación	Depende de la versión a instalar, la configuración de hardware, si es una actualización o restauración. Generalmente se lleva a cabo entre 20 y 60 minutos, el tiempo adicional puede ser requerido para instalar los drivers	Las gamas son de 6 a 60 minutos, dependiendo la distribución. Para Red Hat el tiempo es de 5 a 30 minutos. Regularmente las distribuciones tipo Red Hat, cuentan con software básico ya instalado.
Drivers	Con frecuencia deben ser instalados por separado, la mayoría de los drivers comunes se encuentran disponibles en Windows Update.	La mayoría de los drivers disponibles son incluidos en la mayoría de las distribuciones o pueden ser encontrados en línea.
Software pre-instalado	Windows Media Player, Wordpad, Bloc de Notas, Paint, Calculadora, Internet Explorer, Windows Live Messenger, Windows Media Center (Vista), por mencionar algunos.	Programas multimedia, gráficos, internet, paquetes de oficina, juegos, utilidades del sistema, ambientes alternativos de escritorio, entre otros.
Apariencia	La interacción con el usuario es coherente, amigable y fácil de usar	La calidad del diseño varía entre ambientes de escritorio y distribuciones, sin embargo, Linux no es dinámico e incluso puede reflejar complejidad en su manejo.
Estabilidad general	En sus versiones iniciales, Windows era muy inestable, provocando constantes reinicios y la aparición de varias pantallas azules. Actualmente se han hecho mejoras en las nuevas versiones, sin embargo Windows aún sigue teniendo problemas de inestabilidad.	Eficientemente estable, la probabilidad de que ocurra un error que provoque pérdida de datos o el reinicio del sistema.
Seguridad	Windows cuenta con un Firewall que protege al equipo de intrusos como hackers y software malintencionado. El problema de la seguridad de Windows es que debido a su gran acaparamiento del mercado, existen una gran cantidad de software malintencionados (virus, gusanos, troyanos, entre otros) creados para atacar a Windows.	Linux proporciona un sistema completo de seguridad que va desde el control de firewall hasta contenedores seguros para el aislamiento de aplicaciones. Linux es una plataforma segura ya que la mayor cantidad de virus están dirigidos a Windows.
Software	Tiene una gran cantidad de Software de descarga y generalmente la descarga e instalación es un poco más complicada que en Linux pero en un ambiente muy gráfico.	Linux tiene una menor cantidad de software en comparación con Windows, esto no implica que no se encuentre el software deseado para Linux. La ventaja con Linux es que la búsqueda e instalación de software es fácil.
Comunicación con otros sistemas operativos	Windows solo es capaz de leer y escribir sus propios sistemas de archivos, presenta incompatibilidades entre algunas de sus versiones.	Linux lee y escribe en sistemas de archivos de Windows, Macintosh, entre otros. Por red, se comunica con cualquier otro sistema.

Tabla No.5.1-Cuadro comparativo entre Windows y Linux.

Una vez examinadas las características de los sistemas operativos, lo más importante al momento de la implementación del sistema de monitoreo es la seguridad, estabilidad y la comunicación con otros sistemas operativos, características en las cuales Linux tiene ventaja sobre Windows.

Se requiere que el sistema operativo sea seguro ya que la información que maneja SNMP es muy valiosa y a la vez reveladora debido a que contiene toda la información del sistema, además las gráficas sólo deben ser vistas por las personas autorizadas.

Así mismo se necesita que el lugar donde el sistema de monitoreo residirá sea estable, se dice que un sistema es estable cuando su nivel de fallos disminuye por debajo de un determinado umbral. El sistema operativo debe ser estable porque SNMP y MRTG recolectan información de las variables cada cinco minutos, por lo que los reinicios o retrasos causarían pérdida de datos y resultados erróneos.

Simultáneamente a las características de estabilidad y seguridad se requiere la compatibilidad de sistemas operativos debido a que se monitorearán sistemas operativos Windows y Linux, además en caso de que en un futuro se introdujeran sistemas operativos diferentes a los que se tienen, Linux muestra una gran adaptabilidad y compatibilidad con otros sistemas.

Debido a estas tres características importantes, el sistema sobre el cual se implementará el sistema de monitoreo del Sun Blade 6000 es Linux. Ahora es momento de definir el software que se requiere sobre Linux y Windows para la instalación de SNMP y MRTG

5.2. Requerimientos de software

Previo a comenzar con la instalación, es necesario saber que elementos de software se requieren para poder instalar el protocolo SNMP y la herramienta MRTG de tal modo que éstos funcionen correctamente sin atentar contra los recursos del sistema.

Los requerimientos de hardware no son tan relevantes debido al poco uso de recursos que requiere SNMP tanto en Windows Server 2008 como en Red Hat Linux Enterprise 5. Además como se describió anteriormente, el servidor Sun Blade tiene unas capacidades de hardware sorprendentes las cuales no se verán afectadas por las paqueterías que se instalarán. Sin embargo el software es importante ya que sin este las herramientas no podrían ser instaladas.

WINDOWS SERVER 2008

En el sistema operativo Windows Server 2008 y en los sistemas Windows actuales, el servicio SNMP viene instalado por defecto, esto no implica que el proceso se esté ejecutando por defecto ni que éste ya esté correctamente configurado.

Windows muestra una interfaz gráfica muy dinámica y fácil de usar en la que la configuración e inicialización del servicio SNMP es muy sencilla. El servicio SNMP se encuentra dentro de las herramientas de sistema donde es posible, iniciarlo, detenerlo, reiniciarlo y configurarlo.

Sólo basta con asegurarse que el servicio esté visible para Windows, en caso de que no esté visible, es necesario ir a "*Activar o desactivar características de Windows"* y buscar el Protocolo

Simple de Administración de Redes o SNMP para activar todas las casillas, tal como lo muestra la Figura No.5.2.

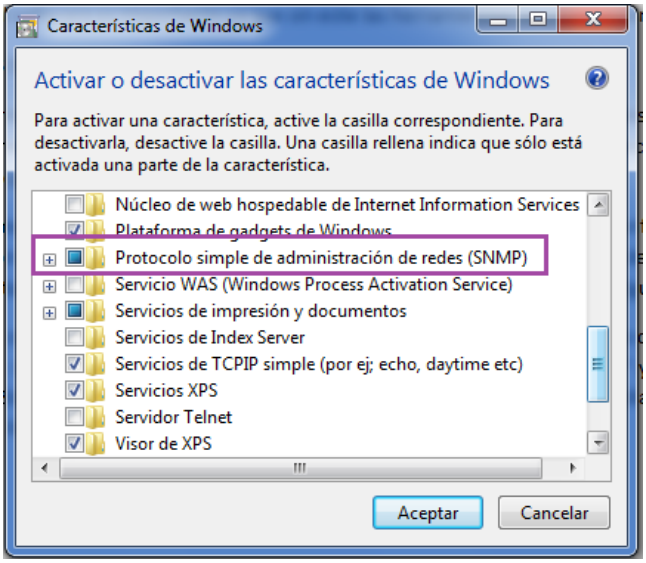


Figura No.5.2-SNMP visible en Windows

De esta manera se asegura que SNMP esté visible y listo para ser configurado en cuanto se desee. Con esta configuración se terminan los requerimientos de software para Windows Server 2008. A continuación se mencionan los requerimientos necesarios para Red Hat.

RED HAT ENTERPRISE LINUX 5

Los requisitos de software para que Linux pueda trabajar con SNMP y MRTG son pocos debido a la gran flexibilidad y compatibilidad que tienen. A diferencia de Windows, en Linux es importante analizar los requerimientos de MRTG porque es en donde se mostrarán las gráficas de las variables seleccionadas.

Los únicos requisitos para la instalación son: contar con una versión de perl posterior a la v5.6.0., para el caso de SNMPv3 que contiene seguridad, el sistema debe tener los módulos de cifrados DES, MD5, SHA1 y HMAC.

Simultáneamente a las características anteriores, Linux debe tener un servidor http con el fin de que MRTG pueda generar páginas de HTML que contengan las gráficas de las variables deseadas. Regularmente este servidor ya viene preinstalado en algunas distribuciones en Linux, esto no significa que ya esté correctamente configurado, por lo que es necesario corroborar el correcto funcionamiento del servicio.

Por otro lado la instalación de SNMP y MRTG requiere de paqueterías que pueden ser descargadas desde sus sitios oficiales en internet, o pueden ser instaladas desde la terminal del sistema mediante el comando yum install. Las paqueterías que se necesitan para SNMP son: “net-snmp” y “net-snmp utils”, por su parte MRTG sólo requiere de la paquetería “mrtg”.

Una vez que se cuenta con el software necesario, es momento de definir las variables a monitorear.

5.3. Variables a monitorear

El sistema de monitoreo del SUN BLADE 6000 se encarga de monitorear variables de hardware y de software de cada sistema operativo que reside en él.

Como se mencionó anteriormente el fin del sistema de monitoreo es prevenir fallas en el sistema, razón por la cual se decidió que las variables a monitorear gráficamente son:

- Temperatura de los procesadores.
- Tráfico web.
- Tráfico en la tarjeta de red.
- Carga activa del CPU.
- Memoria RAM total.
- Memoria RAM en uso

Por otro lado existen variables que causarán alertas y envío de e-mails pero no serán graficadas debido a que no es necesario analizar su comportamiento a través del tiempo, estas variables son:

- Reinicio del sistema.
- Apagado del sistema.
- Inicio del sistema.
- Error de autenticación de usuario.
- Disco duro lleno

El tema de las variables es muy complejo debido a que existen dos medios de los cuales se tomarán los datos. Existen las variables tomadas directamente del sistema operativo y otras tomadas desde la ILOM de cada blade.

5.3.1. Variables extraídas del sistema operativo

Las variables extraídas directamente de los sistemas operativos son: tráfico web, tráfico en la tarjeta de red, carga activa del CPU, memoria RAM total, memoria RAM en uso y disco duro lleno, para obtener estas variables se necesita conocer el OID (Object Identifier, Identificador de Objeto) de cada variable, el cual es una secuencia de números que se asignan jerárquicamente y que permite identificar objetos en la red.

Los OID se obtienen mediante los distintos comandos de SNMP: snmpwalk, snmpget, snmptranslate, snmpgetnext, snmptable y snmpset. A continuación se describirá brevemente la utilidad de cada uno.

SNMPGET. Este comando puede ser utilizado para obtener datos de un host remoto dado su nombre de host, la información y un OID. Como ejemplo véase la Figura No.5.3 en donde se hace una consulta del valor de la temperatura del procesador.

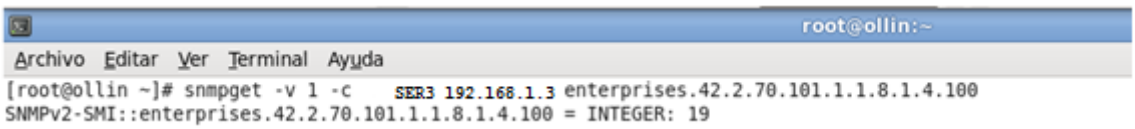


Figura No.5.3-Comando snmpget.

La sintaxis de la Figura No.47 es: snmpget –v 1 [versión de SNMP (1, 2c, 3)] –c SER3 [comunidad] 192.168.1.3 [IP host] enterprises.42.2.70.101.1.1.8.1.4.100 [OID deseado]. Por cuestiones de seguridad en la Figura No.47 no se muestra el nombre de la comunidad.

SNMPTRANSLATE. Es un comando muy poderoso que permite explorar el la MIB de diversas maneras desde la línea de comandos. Su forma más básica permite pasar de un OID a la variable que representa por ejemplo:

```
#snmptranslate .1.3.6.1.2.1.1.3.0
SNMPv2-MIB::sysUpTime.0
```

Además snmptranslate permite pasar del nombre de la variable al OID que representa, entre otras funciones que se pueden consultar en el manual de snmptranslate.

SNMPGETNEXT. Similar al comando snmpget debido a que se utiliza para obtener el siguiente OID de la MIB, es decir, en lugar de obtener los datos que se solicitan directamente, se obtiene el valor posterior al OID pedido. Por ejemplo:

```
#snmpgetnext –v 2c –c public localhost system.sysUpTime.0
SNMPv2-MIB::sysContact.0 = STRING: Root
```

SNMPWALK. Esta orden realiza una serie completa de getnexts automáticamente y se detiene cuando devuelve resultados que no están en el rango del OID especificado originalmente. Un ejemplo real de este comando es la Figura No.5.4:

```
[root@ollin ~]# snmpwalk -v 1 -c [illegible]SER4 192.168.1.13
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: Intel64 Family 6 Model 23 Stepping 10 AT/AT
Free)
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.2
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (519332633) 60 days, 2:35:26.33
SNMPv2-MIB::sysContact.0 = STRING:
```

Figura No.5.4- Comando SNMPWALK.

SNMPTABLE. Muestra una tabla SNMP en un formado de filas y columnas de manera que su presentación visual y su comprensión son más sencillas que si se utilizara snmpwalk.

SNMPSET. Esta orden se utiliza para modificar información en un host. Por cada una de las variables que se quiere establecer, es necesario el OID a actualizar, el tipo de datos de la variable y el valor al que se quiera poner la variable. La Figura No.5.5 es un ejemplo de cómo se puede utilizar el comando snmpset en conjunto con el comando snmpget.

```
#snmpget -v 2c -c public localhost sysContact.0
SNMPv2-MIB::sysContact.0 = STRING: Root <root@localhost>
#snmpset -v 2c -c public localhost sysContact.0 s "Admin"
SNMPv2-MIB::sysContact.0 = STRING: Admin
#snmpget -v 2c -c public localhost sysContact.0
SNMPv2-MIB::sysContact.0 = STRING: Admin
```

Figura No.5.5-Comando SNMPSET

Una vez descritos los comandos que se pueden utilizar gracias a SNMP, con ayuda de snmpwalk, snmpget o snmptable se empezaron a analizar las variables que existían dentro de la MIB y dentro de cada sistema operativo. Después de grandes horas invertidas en la búsqueda de los OID de las variables deseadas, se obtuvieron los siguientes resultados:

- **Tráfico web**. El tráfico web sólo será graficado para el servidor SER4 de acuerdo con los requisitos del administrador. SER4 recibe mucha carga web y su disponibilidad para los usuarios es de gran importancia. Los OID´s encargados de brindar los datos del tráfico web son :

  ```
  1.3.6.1.4.1.311.1.7.3.1.2.0 o enterprises.311.1.7.3.1.2.0
  Y
  1.3.6.1.4.1.311.1.7.3.1.4.0 o enterprises.311.1.7.3.1.4.0
  ```

  El primero corresponde al tráfico web de entrada y el segundo al tráfico web de salida.

- **Tráfico en la tarjeta de red**. La conexión física de cada Blade utiliza dos interfaces conectadas con el fin de brindar una alta disponibilidad. Mientras una interfaz de red esté funcionando correctamente la otra estará a la espera de que ocurra algún error en dicha tarjeta para ocupar su lugar y evitar que se pierda la conexión. En ambas tarjetas no se tiene configurada una IP o datos de red, esto se debe a que lógicamente las tarjetas de red se encuentran conectadas mediante un puente.
  La explicación anterior implica que sólo se monitorean 3 interfaces de red, la tarjeta en uso, la tarjeta en espera y el puente.
  Estas variables son obtenidas automáticamente mediante la herramienta cfgmaker que forma parte del paquete MRTG y que su uso se explicará en el capítulo de implementación, por esta razón, las variables no se encuentran con el formato de OID. A continuación, en la Tabla No.5.2 se muestra una tabla de los nombres de las interfaces, sus identificadores de red y su descripción correspondientes a cada sistema operativo.

Tabla No.5.2-identificadores de interfaces de red.

	Nombre-ID interfaz	Descripción
SER1	ethernet 6 -(ID 10)	Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S
	ethernet 8 -(ID 11)	Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S #2
	ethernet 10 -(ID 12)	Puente MAC
SER2	eth1 -(ID 3)	ethernet 1
	bond0 -(ID 5)	bond0
	eth0 -(ID 8)	ethernet 0
SER3	ethernet 6 -(ID 10)	Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S
	ethernet 8 -(ID 11)	Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S #2
	ethernet 10 -(ID 12)	Puente MAC
SER4	ethernet 6 -(ID 11)	Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S
	ethernet 8 -(ID 12)	Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S #2
	ethernet 10 (ID 13)	Puente MAC

- **Carga activa del CPU.** El OID asignado a la carga del procesador es `hrProcessorLoad.*` o `.1.3.6.1.2.1.25.3.3.1.2.*`, en cada sistema operativo se cuentan con 8 variables de este tipo como consecuencia de que cada sistema operativo cuenta con dos procesadores de cuatro núcleos cada uno entre los cuales se divide la carga del CPU.
  Estas variables cambian según el sistema operativo del que se obtengan, por lo tanto las variables hrProcessorLoad de los Windows serán iguales y las de Red Hat Enterpises Linux diferirán en el último dígito de la variable.

  En la Tabla No. 5.3 se mencionan todas las variables de carga activa de CPU pertenecientes a cada sistema operativo.

Tabla No.5.3-OID de la carga del CPU.

Variable	SER1	SER2	SER3	SER4
1	hrProcesorLoad.2	hrProcesorLoad.768	hrProcesorLoad.2	hrProcesorLoad.2
2	hrProcesorLoad.3	hrProcesorLoad.769	hrProcesorLoad.3	hrProcesorLoad.3
3	hrProcesorLoad.4	hrProcesorLoad.770	hrProcesorLoad.4	hrProcesorLoad.4
4	hrProcesorLoad.5	hrProcesorLoad.771	hrProcesorLoad.5	hrProcesorLoad.5
5	hrProcesorLoad.6	hrProcesorLoad.772	hrProcesorLoad.6	hrProcesorLoad.6
6	hrProcesorLoad.7	hrProcesorLoad.773	hrProcesorLoad.7	hrProcesorLoad.7
7	hrProcesorLoad.8	hrProcesorLoad.774	hrProcesorLoad.8	hrProcesorLoad.8
8	hrProcesorLoad.9	hrProcesorLoad.775	hrProcesorLoad.9	hrProcesorLoad.9

Es importante mencionar que la parte del OID `hrProcessorLoad` puede ser sustituida por el OID numérico `.1.3.6.1.2.1.25.3.3.1.2.`, un ejemplo, el OID `hrProcessorLoad.2` puede ser sustituido por el OID numérico `.1.3.6.1.2.1.25.3.3.1.2.2`, se puede usar uno u otro dependiendo las necesidades de cada administrador. En el caso del sistema operativo se utilizaran los OID con palabras ya que contribuyen a una mejor comprensión.

- **Memoria RAM total**. En todos los sistemas operativos que residen en el Sun Blade 6000, existe la variable de memoria RAM en uso, la cual es identificada con el OID `hrStorageSize.*` o el OID numérico `.1.3.6.1.2.1.25.2.3.1.5.*`, en donde el asterisco tomará el valor según el blade del que provenga, así como lo muestra la Tabla No.5.4.

Tabla No.5.4-OID de la Memoria RAM total

Blade	Variable de memoria RAM total
SER1	`hrStorageSize.5`
SER2	`hrStorageSize.2`
SER3	`hrStorageSize.7`
SER4	`hrStorageSize.5`

- **Memoria RAM en uso.** Para la memoria RAM se cuenta con el OID `hrStorageUsed.*` o el OID en su forma numérica `.1.3.6.1.2.1.25.2.3.1.6.*`, igual que en el caso de la Memoria RAM total, el asterisco debe de ser remplazado según las variables del Blade que se esté supervisando. La Tabla No.5.5 indica las variables de memoria en uso que corresponden a cada Blade.

Tabla No.5.5-OID de la Memoria RAM en uso

Blade	Variable de Memoria RAM en uso
SER1	`hrStorageUsed.5`
SER2	`hrStorageUsed.2`
SER3	`hrStorageUsed.7`
SER4	`hrStorageUsed.5`

5.3.2. Variables extraídas del ILOM

La variable de la temperatura se extrae directamente de la dirección IP del ILOM según el blade que se desee utilizar, lo que implica que no se utilizará la dirección IP primaria. Existen dos temperaturas de procesador por cada sistema operativo debido a que cada uno de los sistemas contiene dos procesadores Intel Xeon Quad Core. Los OID´s correspondientes a dichas temperaturas son:

- Para SER1
  `1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.124`
  `1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.125`

- Para SER2
  `1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.124`
  `1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.125`

- Para SER3
  `1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.100`
  `1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.101`

- Para SER4
  `1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.136`
  `1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.137`

Además de estas variables, dentro de la ILOM es posible configurar 15 alertas por cada Blade y una por el CMM, lo que da un total de 75 alertas posibles. Estas alertas están predefinidas para informar acerca de:

- Inicio de sistema, siempre y cuando éste sea hecho desde la ILOM.
- Apagado de sistema, si es que se realizó desde la ILOM.
- Inicio del servicio SNMP.

Más adelante se explica cómo activar y configurar dichas alertas. En caso de que el encendido o alguna de estas modificaciones no se realicen desde el ILOM y sea por medio de conexión a escritorio remoto, el servicio SNMP para Windows ofrece las opciones que se mencionan a continuación.

5.3.3. Variables predefinidas de Windows

El servicio SNMP en Windows brinda la facilidad de crear alertas según lo que se desee. La desventaja de este tipo de alertas es que sólo pueden ser activadas o desactivadas pero no modificadas. Las variables que se eligieron activar para alertar en caso de que las condiciones que éstas definen se cumplan son: reinicio del sistema, apagado del sistema, inicio del sistema, error de autenticación de usuario, disco duro lleno. En el capítulo de Implementación se dan más detalles acerca de la configuración de estas alertas.

Hasta ahora se han tratado temas de OID´s, tipos de variables SNMP, alertas, pero ¿cuál es el fin de generar alertas y de monitorear las variables?, la respuesta son las notificaciones.

5.4. Notificaciones trap [13]

SNMP proporciona la capacidad de enviar notificaciones, para informar al administrador cuando una o más condiciones de una variable se cumplen. Las notificaciones son paquetes de red que contienen datos relativos a un componente del sistema.

Estas notificaciones no requieren que el administrador SNMP haga una petición previa. Además estas notificaciones no solicitadas o asíncronas se pueden generar de dos formas: como traps o como peticiones de informe. Ejemplos típicos de su uso son fallo en la autenticación de usuario y el reinicio del sistema.

Los traps son mensajes que sirven para alertar al administrador SNMP de alguna condición de la red. La desventaja delos traps respecto a las peticiones de informe es que son menos fiables debido a que no existe una confirmación de recibido. Por lo tanto el agente que la ha enviado no sabrá si el trap fue recibido o no.

Las peticiones de informe son similares a los traps, pero implican una solicitud de acuse de recibo por parte del administrador SNMP y son implementadas con los mensajes de tipo inform-request de SNMPv2, pensados para el intercambio de información entre administradores.

Cuando un administrador SNMP recibe una petición de informe, reconoce el mensaje mediante un mensaje de respuesta SNMP. Si el agente no recibe una respuesta tras el envío del informe, éste puede reenviarse, por esta razón, la petición de informe es más confiable que un trap.

Sin embargo, los traps generalmente son el método preferido tal como es el caso del sistema de monitoreo del SUN BLADE 6000, ya que las peticiones de informes consumen más recursos en el dispositivo y en la red. Al contrario de los traps que se descartan cuando son enviados, una petición de informe se debe almacenar en memoria hasta que llegue el acuse de recibo o hasta que expire. Además los traps se envían sólo una vez, mientras que una petición de informe puede reenviarse varias veces. Estos reintentos aumentan el tráfico y la carga de la red. Tomando en cuenta los argumentos anteriores, se deben acomodar las prioridades de confiabilidad y uso de recursos, para el caso del Sun Blade 6000 es más importante el uso de recursos.

Los traps pueden ser clasificados en: traps genéricos y traps específicos. Existen 6 traps genéricos o estandarizados, los cuales ya se encuentran previamente definidos: [56]

- Cold Start (0): Indica que el agente ha sido inicializado o reinicializado.
- Warm Start (1): Indica que la configuración del agente ha cambiado.
- Link Down (2): Una interfaz de comunicación se encuentra inactiva
- Link Up (3): Alguna interfaz de comunicación se encuentra activa.
- Authentication failure (4): El agente recibió un requerimiento de un NMS no autorizado
- EGP neighbor Loss (5): En alguno de los routers que se esté utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio.
- Enterprise (6): En esta categoría se encuentran todos los traps incluidos por los fabricantes.

Por su parte, los traps específicos son usados por empresas privadas para definir sus traps específicos de servicios.

Los traps serán configurados en los sistemas operativos y en la ILOM. Los del sistema operativo serán definidos en el capítulo de implementación, sin embargo, los traps de la ILOM sólo pueden activar debido a que se encuentran previamente definidos, esto es porque existen sensores que generan los traps. Los traps SNMP predefinidos se encuentran en las Tabla No. 5.6, 5.7, 5.8 y 5.9. [20]

Tabla No.5.6-Traps SNMP de eventos en la memoria

Mensaje de trap SNMP	Mensaje de evento de ILOM	Descripción	Nombre del sensor
sunHwTrapMemoryFault	Fault.memory.channel.misconfigured	Importante; se sospecha que un componente de memoria está ocasionando error.	/SYS/MB/P/D
sunHWTrapMemoryFault Cleared	Fault.memory.channel.misconfigured	Informativo; se ha solucionado un error de un componente de memoria	/SYS/MB/P/D
sunHwTrapComponentFault	fault.memory.intel.dimm.none fault.memory.conroller.inputinvalid fault.memory.controller. initfailed fault.memory.intel.dimm. population-invalid	Importante; se sospecha que un component de memoria está ocasionando un error	/SYS/MB
sunHwTrapComponentFault Cleared	fault.memory.intel.dimm.none fault.memory.conroller.inputinvalid fault.memory.controller. initfailed fault.memory.intel.dimm. population-invalid	Informativo; se ha solucionado un error de un componente de memoria	/SYS/MB
sunHWTrapMemoryFault	fault.memory.intel.dimm. incompatible fault.memory.intel.dimm. incompatible-maxranks fault.memory.intel.dimm. incompatible-quadrank	Importante; se sospecha que un componente de memoria está ocasionando un error	/SYS/MB/P/D
sunHWTrapMemoryFault Cleared	fault.memory.intel.dimm. incompatible fault.memory.intel.dimm. incompatible-maxranks fault.memory.intel.dimm. incompatible-quadrank	Informativo; se ha solucionado un error de un componente de memoria	/SYS/MB/P/D

Tabla No.5.7-Traps SNMP del entorno

Mensaje de captura SNMP	Mensaje de evento de ILOM	Descripción	Nombre del sensor
sunHwTrapPowerSupply Fault	fault.chassis.env.-power.loss	Importante; se sospecha que un componente de fuente de energía está ocasionando un error	/SYS/MB/PS
sunHwTrapPowerSupply Fault Cleared	fault.chassis.env.-power.loss	Informativo: se ha solucionado un error de un componente de fuente de energía	/SYS/MB/PS
sunHwTrapComponentF ault	fault.chassis.env.-temp.over-fail	Importante; se sospecha que un componente está ocasionando un error	/SYS/
sunHwTrapComponentF ault Cleared	fault.chassis.env.-temp.over-fail	Informativo; se ha solucionado un error de un componente	/SYS/
sunHwTrapTempCrit-Threshold Exceeded	Se ha excedido un umbral crítico inferior	Importante;un sensor de temperatura ha notificado que su valor es superior a una configuración de umbral crítico superior o inferior a una configuración de umbral crítico.	/SYS/MB/T_AMB_FRONT /SYS/MB/T_AMB_REAR
sunHwTrapTempCrit-Threshold Deasserted	Ya no se supera el umbral crítico inferior	Informativo; un sensor de temperatura ha notificado que su valor se encuentra dentro del rango normal de funcionamiento	/SYS/MB/T_AMB_FRONT /SYS/MB/T_AMB_REAR
sunHwTrapTempNonCrit ThresholdExceeded	Se ha superado el umbral no crítico superior	Menor; un sensor de temperatura ha notificado que su valor es superior a una configuración de umbral crítico superior o inferior a una configuración de umbral crítico inferior	/SYS/MB/T_AMB_FRONT /SYS/MB/T_AMB_REAR
sunHwTrapTempOk	Ya no se supera el umbral no crítico superior	Informativo; un sensor de temperatura ha notificado que su valor se encuentra dentro del rango normal de funcionamiento	/SYS/MB/T_AMB_FRONT /SYS/MB/T_AMB_REAR
sunHwTrapTempFatal ThresholdExceeded	Se ha excedido un umbral grave inferior	Grave; un sensor de temperatura ha notificado que su valor es superior a una configuración de umbral grave superior o inferior a una configuración de umbral grave inferior	/SYS/MB/T_AMB_FRONT /SYS/MB/T_AMB_REAR
sunHwTrapTempFatal ThresholdDeasserted	Ya no se supera el umbral grave inferior	Informativo; un sensor de temperatura ha notificado que su valor es inferior a una configuración de umbral grave superior o inferior a una configuración de umbral grave inferior.	/SYS/MB/T_AMB_FRONT /SYS/MB/T_AMB_REAR
sunHwTrapTempFatal ThresholdExceeded	Se ha superado el umbral grave superior	Grave; un sensor de temperatura ha notificado que su valor es superior a una configuración de umbral grave superior o inferior a una configuración de umbral grave inferior	/SYS/T_AMB
sunHwTrapTempCrit-Threshold Exceeded	Se ha superado el umbral crítico superior	Importante; un sensor de temperatura ha notificado que su valor es superior a una configuración de umbral crítico superior o inferior a una configuración de umbral crítico inferior	/SYS/T_AMB
sunHwTrapTempCrit-Threshold Deasserted	Ya no se supera el umbral crítico superior	Informativo; un sensor de temperatura ha notificado que su valor se encuentra dentro del rango normal de funcionamiento	/SYS/T_AMB
sunHwTrapTempFatal ThresholdDeasserted	Ya no se supera el umbral grave superior	Informativo; un sensor de temperatura ha notificado que su valor es inferior a una configuración de umbral grave superior o	/SYS/T_AMB

		inferior a una configuración de umbral grave inferior.	
sunHwTrapComponentError	Aceptar	Importante; un sensor de fuente de energía ha detectado un error	/SYS/HOT /SYS/PS*n*/S*n*/V_OUT_OK
sunHwTrapComponentOk	Denegar	Informativo; un sensor de fuente de energía ha vuelto a su estado normal	/SYS/HOT /SYS/PS*n*/S*n*/V_OUT_OK

Tabla No.5.8- Traps SNMP de eventos del dispositivo

Mensaje de captura SNMP	Mensaje de evento de ILOM	Descripción	Nombre del sensor
sunHwTrapComponentFault	fault.chassis.device.missing	Importante; se sospecha que un componente principal está ocasionando un error	/SYS/
sunHwTrapComponentFault Cleared	fault.chassis.device.missing	Informativo; se ha solucionado un error de un componente	/SYS/
sunHwTrapComponentFault	fault.chassis.device.fail	Importante; se sospecha que un componente está ocasionando un error	/SYS/CMM
sunHwTrapComponentFault Cleared	fault.chassis.device.fail	Informativo; se ha solucionado un error de un componente	/SYS/CMM
sunHwTrapIOFault	fault.chassis.device.fails	Importante; se sospecha que un componente del subsistema de E/S está ocasionando un error	/SYS/NEM
sunHwTrapIOFault Cleared	fault.chassis.device.fails	Informativo; se ha solucionado un error del componente del subsistema de E/S	/SYS/NEM

Tabla No.5.9- Traps SNMP de eventos de la fuente de energía.

Mensaje de captura SNMP	Mensaje de evento de ILOM	Descripción	Nombre del sensor
sunHwTrapPowerSupplyError	Aceptar	Importante; un sensor de fuente de energía ha detectado un error	/SYS/PWRBS
SunHwTrapPowerSupplyOk	Denegar	Informativo; un sensor de fuente de energía ha vuelto a su estado normal	/SYS/PWRBS
sunHwTrapPowerSupplyFault	fault.chassis.env.power.loss	Importante; se sospecha que un componente de fuente de energía está ocasionando un error	/SYS/PS
sunHwTrapPowerSupplyFault Cleared	fault.chassis.env.power.loss	Informativo: se ha solucionado un error de un componente de fuente de energía	/SYS/PS

Ya se han definido los traps, tipos de traps, los traps que pueden ser configurados dentro de la ILOM, pero no se ha mencionado como se van a utilizar. Con respecto a los traps el sistema de monitoreo Sun Blade 6000, funciona de la siguiente manera:

El sistema operativo Red Hat Linux fungirá como el servidor trap, el cuál será el encargado de recibir todos los traps de todos los sistemas operativos, incluyéndose él mismo. Una vez que el

trap sea recibido, este será enviado a uno o más correos electrónicos, notificando que existe un suceso dentro de algún sistema operativo. Al igual que las configuraciones de los traps, la configuración para enviar el email se verá en el capítulo de implementación.

CAPÍTULO 6.

Implementación

6. IMPLEMENTACIÓN

En este capítulo se explica paso a paso toda la instalación del sistema de monitoreo Sun Blade 6000, abarca desde la instalación de la paquetería snmp, mrtg, así como las configuraciones de las mismas para mostrar el resultado gráficamente. Por otro lado se muestran las gráficas obtenidas y el modo de configurar los traps para que éstos sean enviados a un correo electrónico.

6.1. Instalación del software

Previo a comenzar con la instalación de las paqueterías snmp y mrtg, se debió revisar si se tenía instalado un servidor http, generalmente el más conocido es apache. Apache es un servidor web HTTP de código abierto el cual permitirá a MRTG mostrar las gráficas obtenidas en la página web local de la máquina.

Para instalar, actualizar o remover apache y cualquier paquetería que sea necesaria, se ocupó la herramienta yum. Para el caso de la instalación de apache, la sintaxis del comando es `yum install apache2`. Con la ejecución de este comando quedó instalado el servidor http que se requiere y se comienza con la instalación de las paqueterías snmp y mrtg.

Del mismo modo en que se instaló el servidor http, se instaló snmp. A diferencia de apache, la instalación de snmp constó de dos pasos debido a que existen dos paqueterías que trabajan en conjunto las cuales son:

- "net-snmp", proporciona herramientas y librerías relacionadas con SNMP incluyendo un agente extensible, una librería SNMP, herramientas para solicitar información u obtener información de agentes SNMP y herramientas para generar y manejar los traps SNMP.
- "net-snmp-utils", contiene varias utilidades para usarlas con el proyecto de administración de redes NET-SNMP.

Para la instalación de la paquetería net-snmp se ejecutó el comando `yum install net-snmp`, tal como lo muestra la Figura No.6.1.

```
[root@eli ~]# yum install net-snmp
Loaded plugins: presto, refresh-packagekit
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package net-snmp.i686 1:5.5-17      set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package           Arch          Version                 Repository        Size
================================================================================
Installing:
 net-snmp          i686          1:5.5-17                updates          301 k

Transaction Summary
================================================================================
Install       1 Package(s)
Upgrade       0 Package(s)

Total download size: 301 k
Installed size: 824 k
Is this ok [y/N]:
```

Figura No.6.1-Instalación de la paquetería net-snmp

Sólo bastó con aceptar la instalación mediante una “y” o un “yes” para completar la instalación de la paquetería net-snmp. Con la instalación de la paquetería net-snmp no fue suficiente ya que aún no se podían ejecutar los comandos de snmp: snmpwalk, snmpget, snmpgetnext, entre otros (Ver FiguraNo.6.2), los cuales se utilizan para obtener el valor de las variables a monitorear. Este es el motivo por el cual se instaló la paquetería net-snmp-utils.

```
[root@eli ~]# snmpwalk
-bash: /usr/bin/snmpwalk: No such file or directory
[root@eli ~]#
```

Figura No.6.2-Ejecución del comando snmpwalk sin la paquetería net-snmp-utils

Al igual que net-snmp, net-snmp-utils fue instalada mediante el comando `yum install net-snmp-utils` tal como se muestra en la Figura No.6.3.

```
[root@eli ~]# yum install net-snmp-utils
Loaded plugins: presto, refresh-packagekit
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package net-snmp-utils.i686 1:5.5-17.     set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                Arch            Version                Repository      Size
================================================================================
Installing:
 net-snmp-utils         i686            1:5.5-17.              updates         163 k

Transaction Summary
================================================================================
Install       1 Package(s)
Upgrade       0 Package(s)

Total download size: 163 k
Installed size: 287 k
Is this ok [y/N]: y
```

Figura No.6.3-Instalación de la paquetería net-snmp-utils

Para corroborar que los paquetes snmp hayan sido instalados correctamente, es necesario ejecutar el comando snmpwalk, el cual debe arrojar un resultado igual o similar al de la Figura No.6.4.

```
[root@eli ~]# snmpwalk
No hostname specified.
USAGE: snmpwalk [OPTIONS] AGENT [OID]

  Version:  5.5
  Web:      http://www.net-snmp.org/
  Email:    net-snmp-coders@lists.sourceforge.net

OPTIONS:
  -h, --help            display this help message
  -H                    display configuration file directives understood
  -v 1|2c|3             specifies SNMP version to use
  -V, --version         display package version number
SNMP Version 1 or 2c specific
  -c COMMUNITY          set the community string
```

Figura No.6.4-Comprobación de la correcta instalación de las paqueterías net-snmp.

Con la ejecución del comando snmpwalk se finalizó la instalación de snmp. El siguiente paso fue instalar la herramienta mrtg, mediante el comando `yum install mrtg`. (Ver Figura No.6.5).

```
[root@eli ~]# yum install mrtg
Loaded plugins: presto, refresh-packagekit
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package mrtg.i686 0:2.16.2-4      set to be updated
--> Processing Dependency: perl-IO-Socket-INET6 for package: mrtg-2.16.2-4      i686
--> Processing Dependency: perl-Socket6 for package: mrtg-2.16.2-4      i686
--> Processing Dependency: perl(SNMP_Session) for package: mrtg-2.16.2-4      i686
--> Processing Dependency: perl(BER) for package: mrtg-2.16.2-4      i686
--> Running transaction check
---> Package perl-IO-Socket-INET6.noarch 0:2.66-1      set to be updated
---> Package perl-SNMP_Session.noarch 0:1.12-4      set to be updated
---> Package perl-Socket6.i686 0:0.23-3      set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                Arch            Version                Repository      Size
================================================================================
Installing:
 mrtg                   i686            2.16.2-4                                707 k
Installing for dependencies:
 perl-IO-Socket-INET6   noarch          2.66-1                 updates          19 k
 perl-SNMP_Session      noarch          1.12-4                                  67 k
 perl-Socket6           i686            0.23-3                                  23 k
```

Figura No.6.5-Instalación de MRTG.

Con este último comando se terminó de instalar el software necesario para poner a trabajar el sistema de monitoreo, la siguiente etapa consistió en realizar las configuraciones correspondientes a SNMP, MRTG y los traps.

6.2. Configuración de SNMP

La configuración de SNMP dependerá del sistema operativo con el que se esté trabajando, además se debe tener en cuenta que Linux tendrá el papel de administrador SNMP y tendrá instalado un agente SNMP que responda al administrador SNMP, sin embargo, los blades que tengan Windows como sistema operativo sólo contarán con el agente SNMP que responderá a las peticiones del administrador SNMP.

6.2.1. Configuración de SNMP en Windows Server 2008.

Como se mencionó en el tema 5.2, Windows tiene la ventaja de tener instalado el servicio SNMP el cuál es muy fácil de configurar mediante una interfaz gráfica. Para comenzar con la configuración de SNMP en Windows se debe acceder a los servicios de Windows, lo cual se puede realizar de dos maneras:

1. Start (Inicio) > Control Panel (Panel de Control) > Administrative Tools (Herramientas Administrativas) > Services (Servicios).
2. Start (Inicio) > Run (Ejecutar) > escribir “services.msc” > OK.

Al momento de ejecutar el proceso 1 o 2, se debe mostrar una ventana con todos los servicios de Windows que se pueden iniciar, detener o pausar, dentro de esta ventana, se debe buscar el SNMP Service (Servicio SNMP) (Ver Figura No.6.6) y dar doble click sobre él.

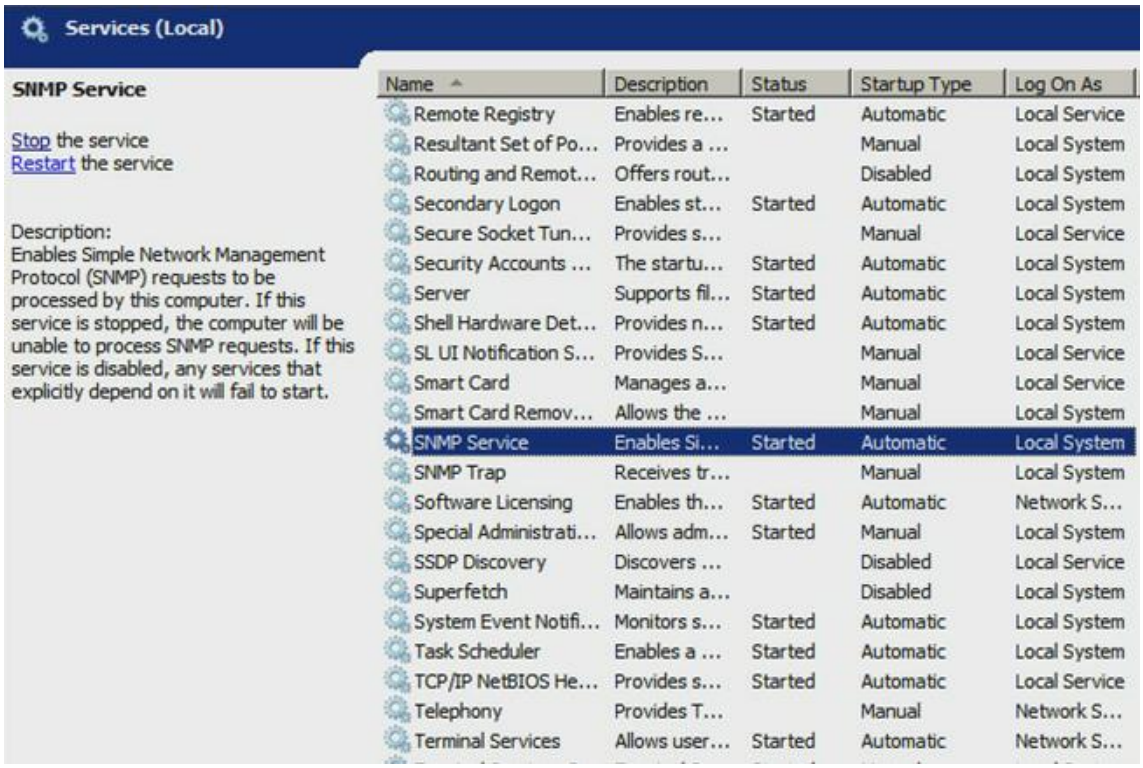


Figura No.6.6-Acceso al servicio SNMP.

Al dar doble click sobre SNMP Service, se muestra una ventana con las pestañas “General (General), Log On (Iniciar sesión), Recovery (Recuperación), Agent (Agente), Traps (Capturas), Security (Seguridad) y Denpendencies (Dependencias)”, se debe seleccionar la pestaña de Security (Seguridad), y es aquí donde comienza la configuración.

En la pestaña Security (Seguridad), debajo de “Accepted community names (Nombres de comunidad aceptados)” se encuentra el botón “Add (Agregar)”, se debe dar click sobre éste y configurar el nombre de la comunidad y sus derechos. Los derechos de la comunidad pueden ser: None (Ninguno), Notify (Notificar), Read Only (Sólo Lectura), Read Write (Lectura y Escritura) y Read Create (Lectura y Creación). La decisión sobre los permisos o derechos de la comunidad dependen del fin y la necesidad del administrador. Con los permisos y el nombre de la comunidad configurados, sólo queda dar click sobre el botón “Add (Agregar) para que las configuraciones se guarden y sean aplicadas.

Para el caso del sistema de monitoreo, para cada blade se creó una comunidad con el nombre de éste, de tal modo que las comunidades son SER1, SER2, SER3 y SER4, todas con permisos de sólo lectura.

Enseguida de definir las comunidades, se indica si se quiere aceptar paquetes SNMP de cualquier host de red o de uno o varios host en específico.

En el sistema de monitoreo se desea limitar la aceptación de paquetes SNMP, con el fin de que el sistema sea más seguro, es por esta razón que se selecciona la casilla “Accept SNMP packets from these hosts (Aceptar paquetes SNMP de estos hosts)” y se escribirá el nombre o dirección IP deseados. Por último se da click sobre el botón “Add (Agregar)” y “OK”. En el sistema de

monitoreo, se pondrá la dirección IP 192.168.1.11, la cual le corresponde al administrador SNMP, quien será el único que podrá recibir respuesta de los hosts (Ver Figura No.6.7).

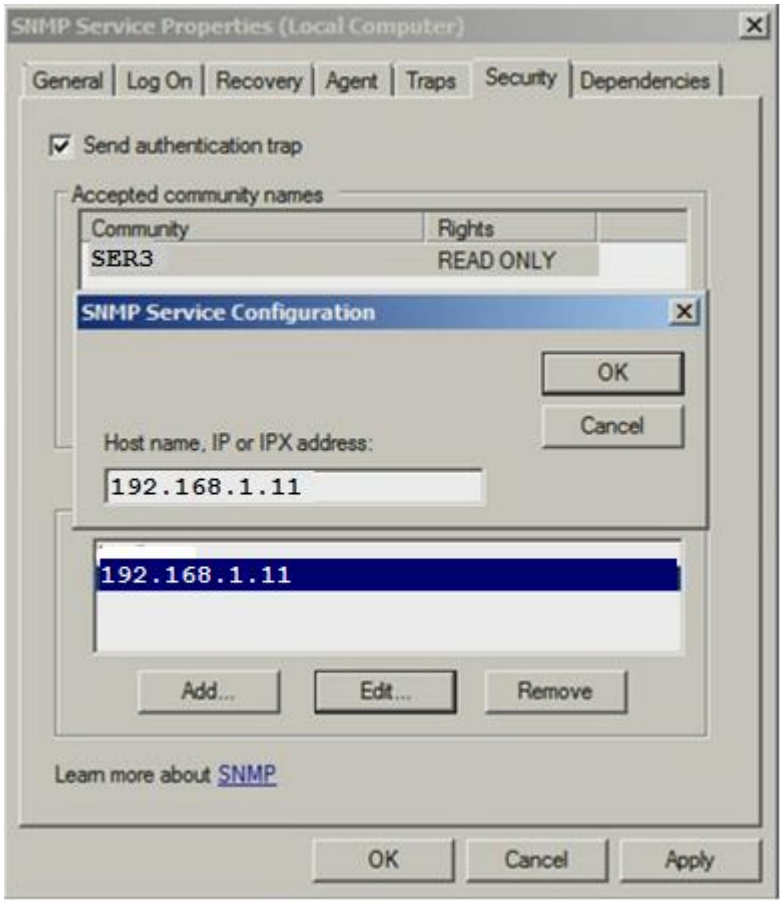


Figura No.6.7-Configuración de comunidades SNMP

Al momento de dar click sobre el botón “OK” con el fin de que todas las configuraciones sean aplicadas, acutomáticamente estará en la pantalla la ventana de los servicios, y será SNMP el que esté seleccionado. En la parte superior izquierda aparece la opción de iniciar el servicio, sobre la cual se debe dar click y con esto ya se tiene completamente configurado e inicializado el servicio SNMP en Windows Server 2008.

Todo este proceso debe relizarse en los tres blades que tienen como sistema operativo Windows. Ahora es el turno de configurar el administrador SNMP, que además también tendrá instalado un agente SNMP de tal manera que se pueda monitorear a si mismo y se encontrará en el Red Hat Enterprise Linux.

6.2.2. Configuración de SNMP en Red Hat Enterprise Linux

La configuración de Red Hat Enterprise Linux es totalmente diferente a como se realizó en el Windows Server 2008, debido a que no se cuenta con una interfaz gráfica y todo se realizará desde la terminal.

Cuando se instalaron las paqueterías net-snmp, se creó automáticamente una carpeta con ruta `/etc/snmp` que contiene el archivo de configuración snmpd.conf. El archivo snmpd.conf es

en donde se configuran las comunidades que tienen acceso al sistema, entre otras características.

Generalmente el archivo snmpd.conf que se instala por defecto es muy complicado de entender. Lo más recomendable es renombrar el archivo snmpd.conf y crear un fichero nuevo y limpio de contenido mediante los siguientes pasos:

1. Abrir una Terminal
2. Ingresar el comando `cd /etc/snmp` para acceder a la carpeta que contiene el archivo snmpd.conf
3. Mover el archivo snmpd.conf al archivo snmpd.conf.old, a través del comando `mv snmpd.conf snmpd.conf.old`.
4. Crear un nuevo archivo llamado snmpd.conf, el cual no contendrá datos. Esta acción se realiza con el comando `touch snmpd.conf`

Con el archivo snmpd.conf completamente en blanco, éste debe ser abierto para empezar a configurar el servicio SNMP como sea requerido. Para abrir el archivo snmpd.conf basta con ejecutar el comando `vi snmpd.conf`.

Lo primero que se debe hacer cuando se abre el archivo snmpd.conf es crear las listas de control de acceso que sirven para definir quien tendrá acceso al servicio SNMP. A estas listas se les debe otorgar el permiso que se desee, los permisos pueden ser de sólo lectura o de lectura y escritura. Para el caso del sistema de monitoreo se asignarán permisos de sólo lectura.

Para agregar las listas de control de acceso se insertan las siguientes líneas dentro del archivo snmpd.conf:

```
#       nombre          origen          comunidad
com2sec  local       192.168.1.11          SER2

# Asignar el nombre de seguridad a cada grupo
#    Nombre de grupo Modelo de seguridad Nombre de seguridad
group   MyROGroup           v1                 local
group   MyROGroup           v2c                local
```

Con la sintaxis anterior, se definió que existe una lista de control de acceso denominada “local” y que corresponderá sólo a la dirección “192.168.1.11”, asignando “SER2” como clave de acceso. Además se creó el grupo “MyROGroup”, que será un grupo al que se le asignarán permisos de sólo lectura. La parte del modelo de seguridad hace referencia al tipo de acceso que se permitirá en un momento dado al grupo MyROGroup.

El siguiente paso consiste en especificar las ramas que se permitirán ver a través del servicio SNMP. La sintaxis más común para estas líneas es:

```
## nombre   incl/excl subárbol   máscara (opcional)
view    all  included  .1         80
```

Posteriormente se especifican los permisos que tendrá el grupo MyROGroup mediante las líneas:

```
##group context sec.model sec.level prefix read write  notif
access MyROGroup   any   noauth    exact  all    none  none
```

Como se puede notar, las últimas dos columnas asignan los permisos de lectura escritura y notificaciones, en este caso como no se requiere que la información sea modificada, sino leída, es necesario asignar el valor de none a las opciones de lectura y notificaciones.

Por último se definen dos parámetros de carácter informativo para que cuando se utilicen aplicaciones cliente como MRTG se incluya información del sistema al que se está accediendo. Esta comfiguración se realiza de la siguiente manera:

```
syslocation CENAPRED (edit /etc/snmp/snmpd.conf)
syscontact Root <root@localhost>
```

Ya con todas las configuraciones realizadas, el archive snmpd.conf debe quedar de la siguiente manera:

```
#Listas de control de acceso (ACL)
#       nombre          origen          comunidad
com2sec  local       192.168.1.11        SER2

# Asignar el nombre de seguridad a cada grupo
#    Nombre de grupo Modelo de seguridad Nombre de seguridad
group   MyROGroup           v1                 local
group   MyROGroup           v2c                local

#Ramas MIB que se permiten ver
## nombre   incl/excl subárbol   máscara (opcional)
view    all  included  .1        80

#Establece permisos de lectura y escritura
##group context sec.model sec.level prefix read write  notif
access MyROGroup   any   noauth    exact  all    none  none


#Información de contacto del sistema
syslocation CENAPRED (edit /etc/snmp/snmpd.conf)
syscontact Root <root@localhost>
```

Para poner a funcionar correctamente SNMP, se deben guardar los cambios en el archivo snmpd.conf, iniciar el servicio snmp y añadirlo a los servicios que arrancan cuando inicia el sistema. Esto se logra a través de la ejecución de los siguientes comandos.

```
service snmpd start #Inicio del servicio snmp
chkconfig snmpd on. #Arrancar snmp junto con el sistema
```

Con el fin de comprobar que las configuraciones se realizaron correctamente, es necesario ejecutar un comando snmp, en este caso se eligió el comando snmpwalk y el resultado se muestra en la Figura No.6.8.

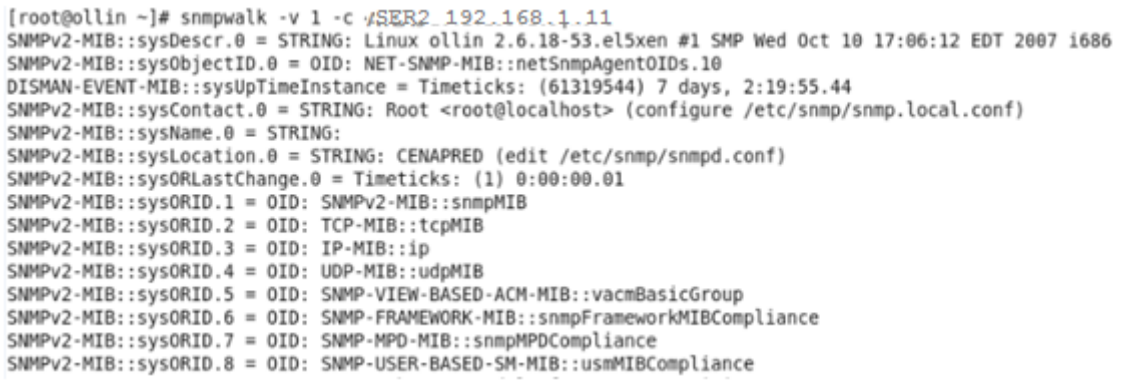


Figura No.6.8-Comprobación de la configuración de SNMP en RHEL.

Además de obtener respuesta del Blade Atlas con dirección IP 192.168.1.11, también se puede obtener respuesta de los blades SER1 (192.168.1.10), SER3 (192.168.1.12) y SER4 (192.168.1.13). La manera de comprobar si se está recibiendo respuesta a las peticiones snmp, es ejecutar los siguientes comandos:

- `snmpwalk –v 1 –c SER1 192.168.1.10`
- `snmpwalk –v 1 –c SER3 192.168.1.12`
- `snmpwalk –v 1 –c SER4 192.168.1.13`

El resultado de cada uno de estos comandos debe ser similar a la anterior Figura No.57, donde se despliega toda la información de la MIB.

Hasta este momento ya se pueden obtener algunas de las variables mencionadas en el tema 5.3, las cuales serán graficadas y son: tráfico web, tráfico en la tarjeta de red, carga activa de CPU, Memoria RAM total, Memoria RAM en uso. Por lo tanto aún faltan las temperaturas de los procesadores, variables que serán obtenidas de la dirección IP del ILOM de cada Blade, cuyo proceso de obtención se explicará en el tema siguiente.

6.2.3. Configuración de SNMP usando las direcciones IP de la ILOM

La configuración del agente SNMP dentro del CMM y de cada Blade se realizará de la misma manera. Se comienza con la apertura de la ILOM y su acceso a ella. Una vez que se ingresa a la ILOM, se mostrará una ventana, que en la parte izquierda superior contiene un árbol donde la rama principal es Chassis (Ver Figura No.6.9), en esta árbol se debe seleccionar el Blade con el que se desee trabajar, las opciones son CMM (global), Blade 0 (SER1), Blade 1 (SER2), Blade 2 (SER3) y Blade 3 (SER4).

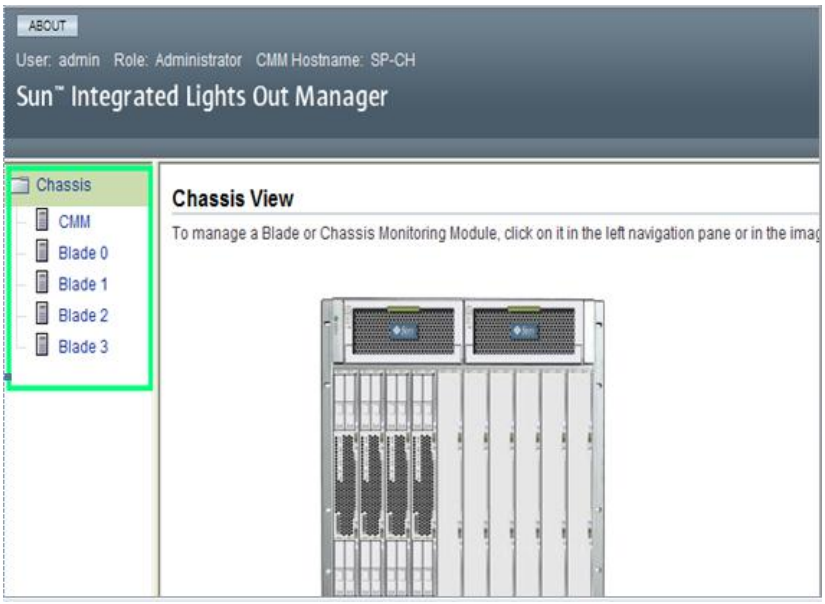


Figura No.6.9-Pantalla inicial del ILOM.

Se pondrá el ejemplo seleccionando la rama “CMM”, la cual engloba a todos los blades, en seguida de la pantalla derecha se selecciona la pestaña de nombre “Configuration”, la cual desplegará otra serie de pestañas de las que se debe elegir la que tenga el nombre de “System Management Access”, al momento de seleccionar esta pestaña, se puede observar una nueva pestaña llamada “SNMP” que se debe seleccionar.

La pestaña SNMP es la que permitirá configurar los documentos, comunidades y usuarios que se deseen para el Protocolo Simple de Administración de Redes.

Se comenzará marcando la casilla “Enabled (Activado)” para activar el servicio. También se elegirán las versiones que SNMP aceptará, las opciones que aparecen son: v1, v2c y v3. En este caso se decidió que se activarían todas las casillas y para guardarlos se da click sobre el botón “Save” (Ver Figura No.6.10).

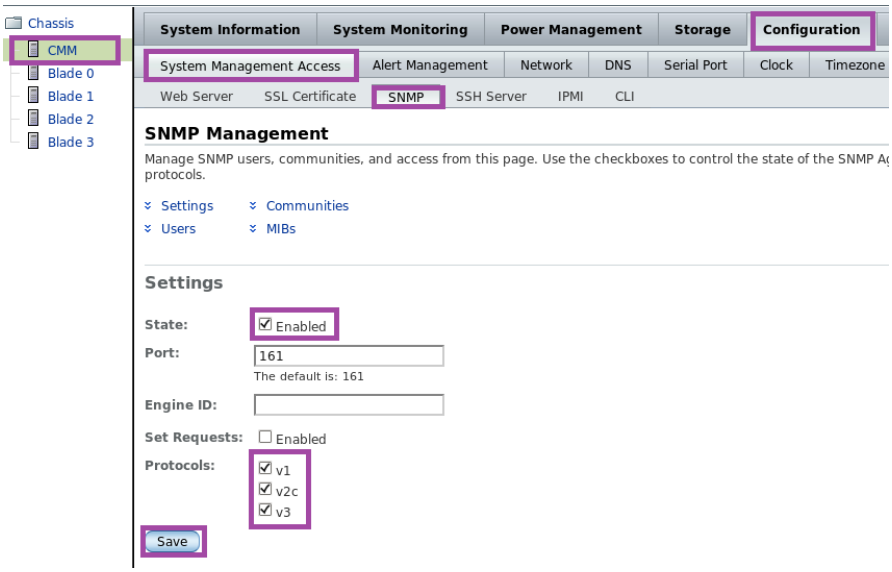


Figura No.6.10-Configuración de la versión de los protocolos aceptados.

Enseguida de las versiones aceptadas, se encuentran las comunidades snmp. Existen las opciones de agregar, editar o borrar una comunidad. Es en esta sección donde se declarará el nombre de la comunidad, si tendrá permisos de lectura y/o escritura. El nombre de la comunidad será Chassis y tendrá permisos de sólo lectura (Ver Figura No.6.11), por defecto están definidas dos comunidades de nombre “public” y “private”, las cuales deben eliminarse por cuestiones de seguridad.

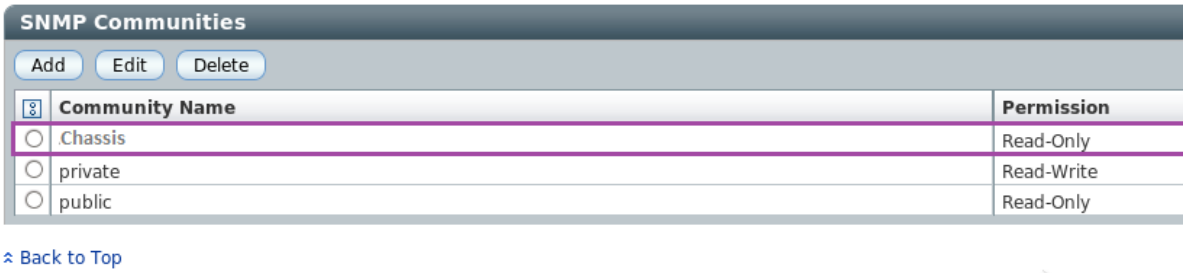


Figura No.6.11-Configuración de comunidades en el Chassis

Este procedimiento se debe repetir en cada Blade, de modo que sea posible realizar un snmpwalk hacia las direcciones ILOM de cada Blade (Ver Figura No.6.12).

```
[root@ollin ~]# snmpwalk -v 1 -c SER4 192.168.1.4 | more
SNMPv2-MIB::sysDescr.0 = STRING: Sun Blade X6250 Server Module, ILOM v3.0.6.13, r48614
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.42.2.200
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (413164012) 47 days, 19:40:40.12
SNMPv2-MIB::sysContact.0 = STRING: (none)
SNMPv2-MIB::sysName.0 = STRING: SP-BL3
SNMPv2-MIB::sysLocation.0 = STRING: (none)
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (3702612018) 428 days, 13:02:00.18
SNMPv2-MIB::sysORID.1 = OID: IF-MIB::ifMIB
SNMPv2-MIB::sysORID.2 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.3 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.4 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.5 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.6 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.7 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.8 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.9 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
```

Figura No.6.12-snmpwalk a SER4 usando su dirección IP ILOM.

Así es como concluye la configuración básica de SNMP para que pueda obtener las variables necesarias y crear gráficas a través la herramienta MRTG.

6.3. Configuración de MRTG

La configuración de MRTG inicia con la generación del directorio de trabajo, lugar donde se guardará la información de los blades que MRTG recolecte. El directorio se debe encontrar dentro de la carpeta /var/www/html, porque es en ella donde se localiza el archivo index.html que se muestra en la página web local del sistema.

La creación del directorio de trabajo se realiza mediante la ejecución de la línea: `mkdir /var/www/html/mrtg`. Con estas líneas se pretende que cuando se abra un navegador de internet y se ponga la dirección localhost/mrtg se logren visualizar las gráficas de MRTG.

Enseguida se crea la carpeta que contendrá los archivos de configuración de mrtg a través del comando:

`mkdir /etc/mrtg` #Crea una carpeta llamada mrtg.

Existirán cinco archivos de configuración dentro de la carpeta recién creada, el nombre de los archivos serán: mrtg.cfg, mrtg1.cfg, mrtg2.cfg, mrtg3.cfg, mrtg4.cfg. Los archivos mrtg1.cfg, mrtg2.cfg, mrtg3.cfg, mrtg4.cfg, incluirán la información de configuración de SER1, SER2, SER3 y SER4, respectivamente, mientras que mrtg.cfg tendrá toda la información de todos los blades, lo que implica que los archivos mrtg1.cfg, mrtg2.cfg, mrtg3.cfg, mrtg4.cfg formarán el archivo mrtg.cfg.

La razón por la que se crean estos cuatro archivos de configuración es porque contribuirán al diseño y presentación de la página web. En teoría sólo se debería crear un archivo de configuración, sin embargo si sólo se creara este archivo, la presentación de las gráficas sería sobre una sola página web, lo que le daría una apariencia desordenada y difícil de visualizar frente al administrador. En el tema 6.4 se explicará cómo es que los archivos mrtg1.cfg, mrtg2.cfg, mrtg3.cfg y mrtg4.cfg ayudan a la presentación de la página web de MRTG.

Sin embargo, el archivo de configuración mrtg.cfg es el más importante en la configuración porque será éste el único que mrtg será capaz de leer para almacenar los datos. Este archivo será creado hasta que los otros cuatro archivos mrtg sean creados. Los archivos mrtg.cfg son la base para crear las páginas html que mostrarán las gráficas.

Para generar los ficheros antes mencionados, a excepción del mrtg.cfg, se deben insertar las siguientes líneas:

```
1. cfgmaker      SER1@192.168.1.10      --global      "WorkDir:
   /var/www/html/mrtg --output /etc/mrtg/mrtg1.cfg
2. cfgmaker      SER2@192.168.1.11      --global      "WorkDir:
   /var/www/html/mrtg --output /etc/mrtg/mrtg2.cfg
3. cfgmaker      SER3@192.168.1.12      --global      "WorkDir:
   /var/www/html/mrtg --output /etc/mrtg/mrtg3.cfg
4. cfgmaker      SER4@192.168.1.13      --global      "WorkDir:
   /var/www/html/mrtg --output /etc/mrtg/mrtg4.cfg
```

Para explicar lo que significa la sintaxis de las líneas 1-4, se utilizará como ejemplo sólo la primera línea donde:

- **cfgmaker**, comando que permite crear un archivo de configuración con extensión .cfg
- **SER1@192.168.1.10**, SER1 es la clave de acceso definida previamente en la configuración SNMP y 192.168.1.10 es la dirección IP que se desea supervisar.

- **--global "WorkDir: /var/www/html/mrtg ,** indica que dentro del archivo se crea una variable local que se refiere al directorio de trabajo el cual será /var/www/html/mrtg.
- **–-output /etc/mrtg/mrtg.cfg,** implica que los resultados serán almacenados en el archivo mrtg.cfg.

En el momento que se ejecuta el comando, automáticamente se crea un archivo con el siguiente contenido inicial:

```
# created by
# /usr/bin/cfgmaker --global 'WorkDir: /var/www/html/mrtg' --output
/etc/mrtg/mrtg.cfg SER1@192.168.1.10
EnableIPv6: no
WorkDir: /var/www/html/mrtg

######################################################################
# System: SER1
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 #AT/AT
COMPATIBLE - Software: Windows Version 6.0 (Build 6002 #Multiprocessor
Free)
# Contact:
# Location:
######################################################################
```

Enseguida de estas líneas aparecen una serie de datos pertenecientes a las 18 interfaces de red, no obstante, como se indicó en el tema 5.3.1 sólo se graficarán tres de las interfaces presentes en el archivo las cuales se definieron en la Tabla No. 5.2, lo que implica que sólo se conservarán las interfaces cuya descripción coincida con las variables especificadas previamente y las otras 15 interfaces deben ser borradas del archivo. La Tabla No.6.1 mostrará la relación de cada Blade con sus respectivas interfaces e identificador de estas.

Tabla No.6.1-Relación de nombre de interfaces y sus identificadores

	Nombre de la interfaz	Identificador de Interfaz
SER1	ethernet 6	10
	ethernet 8	11
	ethernet 10	12
SER2	eth1	3
	bond0	5
	eth0	8
SER3	ethernet 6	10
	ethernet 8	11
	ethernet 10	12
SER4	ethernet 6	11
	ethernet 8	12
	ethernet 10	13

Con ayuda de la Tabla No.6.1 se puede definir que las interfaces que deben quedar son las que tienen el identificador 10,11 y 12 en SER1, esto sólo con el fin de ejemplificar. Además de borrar todas las interfaces a excepción de las ya mencionadas, se debe configurar los elementos que

indican el nombre del sistema y el administrador, si es el caso, traducir todos los datos que aparezcan en inglés al español. He aquí un ejemplo de cómo quedó la configuración de la interfaz 10.

```
###Interface 10 >> Descr: 'Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S  | Name: 'ethernet_6' | Ip: '' | Eth: '00-23-8b-17-a7-34' ###

Target[192.168.1.10_10]: 10:SER1@192.168.1.10:
SetEnv[192.168.1.10_10]: MRTG_INT_IP="" MRTG_INT_DESCR="Intel(R)-PRO/1000-EB-
Conexión de red con Aceleración E/S"
MaxBytes[192.168.1.10_10]: 125000000
Options[192.168.1.10_10]: growright,nopercent
Title[192.168.1.10_10]: Análisis de trafico eth6 (ID10) -- SER1
PageTop[192.168.1.10_10]: <h1>Análisis de trafico eth6 (ID10) -- SER1</h1>
        <div id="sysdetails">
              <table>
                   <tr>
                      <td>Sistema:</td>
                      <td>SER1</td>
                   </tr>
                    <tr>
                       <td>Administrador:</td>
                       <td>Elizabeth</td>
                    </tr>
                    <tr>
                       <td>Descripcion:</td>
                       <td> Intel(R)-PRO/1000-EB-Conexión de red  con Aceleración
E/S  </td>
                    </tr>
                    <tr>
                        <td>Tipo de interfaz:</td>
                        <td>ethernetCsmacd (6)</td>
                    </tr>
                    <tr>
                        <td>Nombre de interfaz:</td>
                        <td>ethernet_6</td>
                    </tr>
                    <tr>
                        <td>Velocidad Maxima:</td>
                        <td>125.0 MBytes/s</td>
                    </tr>
                 </table>
              </div>
```

Hasta este punto ya se encuentran definidas todas las variables de las interfaces de red, sin embargo aún quedan pendientes las variables del rendimiento del CPU, las temperaturas del procesador, tráfico web y el monitoreo de la memoria RAM. Estas configuraciones se realizarán de modo manual, es decir, no hay ningún comando que pueda ayudar a que automáticamente se generen como fue el caso de las interfaces de red.

Previo a comenzar a definir las variables que faltan, se deben definir otras variables globales en cada uno de los archivos de configuración, las cuales irán al inicio del archivo junto a la línea que comienza con “WorkDir”. Las variables que se agregarán son “Language (Idioma)” y “LoadMIBs (Cargar MIBs)”, la primera se refiere al idioma que será utilizado al momento de graficar, el cual será “spanish (español)”, mientras que LoadMIBs hace referencia al directorio en donde se encuentran las MIBs que serán utilizadas para la búsqueda de OID.

LoadMIBs se puede omitir siempre y cuando se utilicen los OID´s numéricos en todas las variables definidas. En el caso del sistema de monitoreo se emplearán los OID textuales para identificar

mejor a cada uno. Por lo tanto si se utilizará la variable local LoadMIBs y el inicio de los archivos mrtg1.cfg, mrtg2.cfg, mrtg3.cfg, mrtg4.cfg queda de la siguiente manera:

```
WorkDir: /var/www/html/mrtg
Language: spanish
LoadMIBS: /usr/share/snmp/mibs/UCD-SNMP-
MIB.txt,/usr/share/snmp/mibs/TCP_MIB.txt,/usr/share/snmp/HOST-RESOURCES-
MIB.txt
```

Ahora, es tiempo de comenzar a definir las variables que faltan, sólo se explicará el archivo de configuración mtrg1.cfg correspondiente a SER1 con el fin de dar un ejemplo, la redacción de los archivos mrtg2.cfg, mrtg3.cfg y mrtg4.cfg será similar y se presentarán al final del tema. Se iniciará con la configuración correspondiente al rendimiento del CPU para SER1, el cual queda de la siguiente manera:

```
#####Grafica del rendimiento del CPU#####
Target[192.168.1.10_cpu]:
(hrProcessorLoad.2&hrProcessorLoad.2:SER1@192.168.1.10 +
hrProcessorLoad.3&hrProcessorLoad.3:SER1@192.168.1.10 +
hrProcessorLoad.4&hrProcessorLoad.4:SER1@192.168.1.10 +
hrProcessorLoad.5&hrProcessorLoad.5:SER1@192.168.1.10 +
hrProcessorLoad.6&hrProcessorLoad.6:SER1@192.168.1.10 +
hrProcessorLoad.7&hrProcessorLoad.7:SER1@192.168.1.10 +
hrProcessorLoad.8&hrProcessorLoad.8:SER1@192.168.1.10 +
hrProcessorLoad.9&hrProcessorLoad.9:SER1@192.168.1.10) / (8)
MaxBytes[192.168.1.10_cpu]: 100
Title[192.168.1.10_cpu]: Carga CPU--SER1
PageTop[192.168.1.10_cpu]: <H1>Carga Activa CPU %--SER1</H1>
ShortLegend[192.168.1.10_cpu]: %
YLegend[192.168.1.10_cpu]: Utilizacion del CPU
Legend1[192.168.1.10_cpu]: CPU activa %
LegendI[192.168.1.10_cpu]: Active
LegendO[192.168.1.10_cpu]:
Options[192.168.1.10_cpu]: growright,nopercent,gauge
```

Donde:

- **Target,** es la palabra clave que se emplea para definir lo que se va a monitorear.
- **192.168.1.10_cpu,** es el nombre único que debe ser añadido a cada parámetro que pertenece a la misma Target. Este nombre también se utiliza como nombre de las páginas web, los archivos de registro y las imágenes de destino.
- Frente a Target se encuentra la suma de los 8 OIDs de carga de CPU definidos en el tema 5.3.1. La razón por la que estos OID se suman es porque cada uno indica su carga personal, sin embargo, lo que se desea saber es la carga total del CPU.
  Además de la suma, se puede contemplar una división, si no existiera la división entre 8, cada uno de los ocho OID **hrProcessorLoad** tomaría un valor de 0% a 100% de carga, lo que arrojaría un resultado máximo de 800% de carga, esto significa que se mostraría un resultado difícil de comprender y analizar, es por ello que se decidió dividir entre ocho, para obtener un resultado más comprensible.
- **MaxBytes,** indica el valor más alto que se puede alcanzar.
- **Title,** provee el título de la página HTML que se genera para la gráfica.
- **PageTop,** es el texto que se suma a la parte superior de la página HTML generada.
- **ShortLegend,** son las unidades que se utilizan para el valor máximo, mínimo y promedio.

- **Legend1**, leyenda que aparecerá en la gráfica que se genere.
- **LegendI,** Leyenda que aparecerá debajo de la gráfica y hará referencia a los datos obtenidos
- **LegendO,** Se conserva vacía ya que sólo interesa que sea un dato el que se muestre, en caso de tener dos variables por separado en la gráfica, ésta línea deberá llenarse.
- **Options,** permite configurar algunas características de la gráfica.
    - **`growright,`** Por defecto las gráficas de MRTG crecen hacia la izquierda, la opción growright cambia la dirección de crecimiento hacia la derecha.
    - **`nopercent,`** generalmente MRTG muestra el resultado deseado y un porcentaje, esta opción se utiliza para que este porcentaje no sea mostrado.
    - **`gauge,`** trata a los valores obtenidos de las mediciones de destino como 'estado actual', esto es útil para controlar cosas como el espacio en disco, carga del procesador, la temperatura, entre otros.
      En ausencia de 'gauge', MRTG trata las variables como contadores, calcula la diferencia entre el valor actual del contador y el valor anterior, lo divide entre el tiempo transcurrido entre las dos últimas lecturas para obtener el valor a representar.

Otra de las variables que se deben de incluir en el archivo de configuración para que se genere su gráfica, es el monitoreo de la memoria que está conformada por los OID´s de memoria RAM total y la memoria RAM en uso. La redacción dentro del archivo mrtg1.cfg queda de la siguiente manera:

```
######Monitoreo de memoria######
Target[192.168.1.10_mem]:
hrStorageUsed.5&hrStorageSize.5:SER1@192.168.1.10 *
hrStorageAllocationUnits.5&hrStorageAllocationUnits.5:SER1@192.168.1.10 *
1000 / 1048576
PageTop[192.168.1.10_mem]: <H1>Memoria libre--SER1</H1>
Options[192.168.1.10_mem]: nopercent,gauge,growright
Title[192.168.1.10_mem]: Memoria libre--SER1
MaxBytes[192.168.1.10_mem]: 100000000000000
YLegend[192.168.1.10_mem]: bytes
ShortLegend[192.168.1.10_mem]: bytes
LegendI[192.168.1.10_mem]: Memoria en uso
LegendO[192.168.1.10_mem]: Memoria total
```

Las opciones de PageTop, Options,Title, MaxBytes, YLegend, ShortLegend, LegendI y LegendO ya no serán explicadas debido a que fueron abordadas en el proceso de configuración de la carga activa del CPU. La única opción que se explicará es el contenido de Target.

Dentro de Target se encuentra una serie de variables multiplicadas y divididas, las cuales se explicarán por partes:

- **`hrStorageUsed.5&hrStorageSize.5`**, indica que se representarán dos datos sobre la gráfica, `hrStorageUsed.5` correspondiente a la memoria RAM en uso y `hrStorageSize.5` a la memoria RAM total. Ambos OID están dados en unidades de `hrStorageAllocationUnits`.

- **hrStorageAllocationUnits** representa el tamaño, en bytes, de los objetos de datos asignados al grupo `hrStorageEntry` que involucra a `hrStorageIndex`, `hrStorageType`, `hrStorageDescr`, `hrStorageSize y hrStorageUsed`. Si esta entrada está monitoreando sectores, bloques, buffers o paquetes, este número generalmente será mayor que uno.
  Con esta información se argumenta el motivo por el cual los OID´s `hrStorageSize y hrStorageUsed` son multiplicados por el OID `hrStorageAllocationUnits`, lo que nos da el resultado en bytes.
  MRTG por sí solo no es capaz de convertir dichas cantidades a Gigabytes, por esta razón es que la conversión se realizará manualmente. He aquí la demostración con datos obtenidos del blade SER1.
  Datos:
  - hrStorageSize.5 = 524243
  - hrStorageAllocationUnits.5 = 65536
  El resultado de la multiplicación de ambas cantidades es:
  524243 x 65536 = 34356789248 bytes.
  Si sólo se graficaran estos datos en crudo, MRTG no los podría graficar correctamente, malinterpretaría los resultados, es por eso que se debe hacer la conversión manual a Gigabytes:

$$34356789248 \text{ bytes}\left(\frac{1\ KByte}{1024\ Bytes}\right)\left(\frac{1\ MByte}{1024\ KBytes}\right) = \ 32765 \text{ Mbytes}$$

  Este resultado es el que se requiere en pantalla, sin embargo, si éste número se pone tal como está, MRTG lo malinterpreta y creería que son Kbytes, para crear una correcta interpretación y tomando en cuenta que MRTG utiliza el sistema binario para las conversiones, dicho resultado se multiplica por 1000.

$$32765 * 1000 = \ 32765000$$

  Este resultado que se mostrará en la gráfica es un 32.8 GBytes, el cual coincide con el Sistema de monitoreo del rendimiento de Windows, ubicado en el Administrador de tareas.

Simultáneamente con la definición de las variables de carga activa de CPU y con la memoria RAM, se deben definir las temperaturas de los procesadores, que serán representadas en una misma gráfica. La configuración dentro del archivo mrtg queda de la siguiente manera:

```
###Temperatura procesadores#######
Target[192.168.1.1_tem-proc-im]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.100&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.1
01:SER1@192.168.1.1
PageTop[192.168.1.1_tem-proc-im]: <H1>Temperatura de los procesadores--
SER1</H1>
Options[192.168.1.1_tem-proc-im]: gauge,nopercent,growright
Title[192.168.1.1_tem-proc-im]: Temperaturas de procesadores--SER1
MaxBytes[192.168.1.1_tem-proc-im]: 50
LegendI[192.168.1.1_tem-proc-im]: Temperatura del procesador 1
LegendO[192.168.1.1_tem-proc-im]:Temperatura del procesador 2
ShortLegend[192.168.1.1_tem-proc-im]: °
```

La definición de Target para las temperaturas es muy sencilla, sólo basta con declarar los dos OID correspondientes a las temperaturas del procesador, el OID 1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.124 representará la temperatura del primer procesador, mientras 1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.125, además se puede observar que este dato se obtiene de la dirección 192.168.1.1 que es la dirección de SER1 a través de ILOM.

La última configuración del archivo mrtg1.cfg es la perteneciente al tráfico web. La sintaxis dentro del archivo queda de la siguiente manera:

```
#####Trafico web de SER4###########
Target[192.168.1.10_web]:
1.3.6.1.4.1.311.1.7.3.1.2.0&1.3.6.1.4.1.311.1.7.3.1.4.0:SER1@192.168.1.10
PageTop[192.168.1.10_web]: <H1>Trafico web—SER4</H1>
Options[192.168.1.10_web]: growright,nopercent
Title[192.168.1.10_web]: Trafico web—SER4
MaxBytes[192.168.1.10_web]: 125000000
```

Con la adición de estas últimas líneas, se termina el proceso de creación del archivo de configuración de MRTG. Si se desea ver la configuración individual de los archivos mrtg1.cfg, mrtg2.cfg, mrtg3.cfg y mrtg4.cfg, debe observar el Anexo 1, Anexo 2, Anexo 3 y Anexo 4 respectivamente.

Además de generar los archivos de configuración individuales, se requiere crear el archivo de configuración global, que llevará por nombre mrtg.cfg, el cual es muy importante para la generación de las gráficas, ya que MRTG solamente se basará en este archivo para la consulta de datos, la creación de las gráficas y el almacenamiento de los datos, de tal manera que si no existiera mrtg.cfg, MRTG no sería capaz de generar las gráficas, ni de crear los archivos log, donde se guardan los datos obtenidos de la consulta.

El contenido del archivo mrtg.cfg, será la suma de los archivos mrtg1.cfg, mrtg2.cfg, mrtg3.cfg y mrtg4.cfg, creados anteriormente, de tal forma que su estructura queda como se muestra en el Anexo 5.

Si sólo existiera el archivo mrtg.cfg, todas las gráficas se mostrarían sobre una sola página web, situación que causaría una saturación de gráficas en la pantalla y se vería de un modo desordenado. La función de los archivos mrtg1.cfg, mrtg2.cfg, mrtg3.cfg y mrtg4.cfg es contribuir con el diseño de la página web.

El beneficio que proporcionan los archivos mrtg1.cfg, mrtg2.cfg, mrtg3.cfg y mrtg4.cfg es que cada Blade tendrá su propia página web, de tal manera que las gráficas se mostrarán de manera ordenada y separada.

El siguiente paso es generar las gráficas, proceso que se realizará mediante el ingreso de un comando, a pesar de que los archivos html se generarán automáticamente, existe la necesidad de modificar el archivo html de la página local para brindarle una mejor presentación. Todo este proceso se describirá en el siguiente tema.

6.4. Creación de gráficas

Para crear las gráficas se requiere la ayuda del script indexmaker perteneciente a la paquetería mrtg. Indexmaker genera automáticamente una página web a partir de los archivos de configuración de mrtg. Sin embargo, la creación de las páginas webs puede realizarse manualmente.

Se generarán cinco páginas webs, de las cuales cuatro serán creadas con ayuda del script indexmaker, lo que implica que se hará uso de los archivos de configuración de mrtg. La Tabla No.6.2 muestra los nombres de las páginas web y su archivo de configuración base.

Tabla No.6.2-Relación de archivos html con archivos mrtg

Nombre página web	Archivo de configuración MRTG
SER1.html	mrtg1.cfg
SER2.html	mrtg2.cfg
SER3.html	mrtg3.cfg
SER3.html	mrtg4.cfg

Con base en la Tabla No.6.2 la creación de las gráficas se realizará de la siguiente manera:

- Para la página web de SER1 (Ver Anexo 6) :
  ```
  indexmaker /etc/mrtg/mrtg1.cfg >> /var/www/html/mrtg/SER1.html
  ```

- Para la página web de SER2 (Ver Anexo 7):
  ```
  indexmaker /etc/mrtg/mrtg2.cfg >> /var/www/html/mrtg/SER2.html
  ```

- Para la página web de SER3 (Ver Anexo 8):
  ```
  indexmaker /etc/mrtg/mrtg3.cfg >> /var/www/html/mrtg/SER3.html
  ```

- Para la página web de SER4 (Ver Anexo 9):
  ```
  indexmaker /etc/mrtg/mrtg1.cfg >> /var/www/html/mrtg/SER4.html
  ```

Cada uno de los comandos anteriores, generó un archivo html, a los cuales se les asignó el nombre de: SER1.html, SER2.html, SER3.html y SER4.html. Para concluir con la etapa de las gráficas, sólo resta configurar la página que será mostrada al inicio, y la cuál funcionará como un índice al administrador.

La página principal mostrará cuatro imágenes, una de cada Blade, las cuales al momento de ser seleccionadas enviarán a la página específica del blade correspondiente. Las imágenes seleccionadas para mostrarse en la página principal corresponden a las páginas del tráfico de tarjeta de red.

El archivo index.html será el encargado de darle el formato a la página principal, cuya estructura es la siguiente:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
    <TITLE>MRTG Index Page</TITLE>
    <!-- Command line is easier to read using "View Page Properties" of your
browser -->
    <!-- But not all browsers show that information. :-(
-->
    <META NAME="Command-Line" CONTENT="/usr/bin/indexmaker /etc/mrtg/mrtg.cfg">
    <META HTTP-EQUIV="Refresh" CONTENT="300">
    <META HTTP-EQUIV="Cache-Control" content="no-cache">
    <META HTTP-EQUIV="Pragma" CONTENT="no-cache">
    <META HTTP-EQUIV="Expires" CONTENT="Mon, 08 Aug 2011 17:37:03 GMT">
    <LINK HREF="favicon.ico" rel="shortcut icon" />

<style type="text/css">
<!--
/* commandline was: /usr/bin/indexmaker /etc/mrtg/mrtg.cfg */
/* sorry, no style, just abusing this to place the commandline and pass
validation */
-->
</style>
</HEAD>

<BODY bgcolor="#ffffff" text="#000000" link="#000000" vlink="#000000"
alink="#000000">


<H1>Sistema de monitoreo</H1>

<TABLE BORDER=0 CELLPADDING=0 CELLSPACING=10>
<tr>
<td><DIV><B>SER1</B></DIV>
<DIV><A HREF="SER1.html"><IMG BORDER=1 ALT="192.168.1.10_10 Traffic Graph"
SRC="192.168.1.10_10-day.png"></A><BR>
<SMALL><!--#flastmod file="SER1.html" --></SMALL></DIV>
</td><td><DIV><B>SER2</B></DIV>
<DIV><A HREF="SER2.html"><IMG BORDER=1 ALT="192.168.1.11_3 Traffic Graph"
SRC="192.168.1.11_3-day.png"></A><BR>
<SMALL><!--#flastmod file="SER2.html" --></SMALL></DIV>
</td></tr>
<tr>
<td><DIV><B>SER3</B></DIV>
<DIV><A HREF="SER3.html"><IMG BORDER=1 ALT="192.168.1.12_10 Traffic Graph"
SRC="192.168.1.12_10-day.png"></A><BR>
<SMALL><!--#flastmod file="SER3.html" --></SMALL></DIV>
</td><td><DIV><B>SER4</B></DIV>
<DIV><A HREF="SER4.html"><IMG BORDER=1 ALT="192.168.1.13_11 Traffic Graph"
SRC="192.168.1.13_11-day.png"></A><BR>
<SMALL><!--#flastmod file="SER4.html" --></SMALL></DIV>
</td></tr>
<tr>
</tr>
</TABLE>

<BR>
<TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0>
  <TR>
```

```
    <TD WIDTH=63><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-l.png" WIDTH=63 HEIGHT=25 ALT="MRTG"></A></TD>
    <TD WIDTH=25><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-m.png" WIDTH=25 HEIGHT=25 ALT=""></A></TD>
    <TD WIDTH=388><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-r.png" WIDTH=388 HEIGHT=25
    ALT="Multi Router Traffic Grapher"></A></TD>
  </TR>
</TABLE>
<TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0>
  <TR VALIGN=top>
  <TD WIDTH=88 ALIGN=RIGHT><FONT FACE="Arial,Helvetica" SIZE=2>
  version 2.14.5</FONT></TD>
  <TD WIDTH=388 ALIGN=RIGHT><FONT FACE="Arial,Helvetica" SIZE=2>
  <A HREF="http://tobi.oetiker.ch/">Tobias Oetiker</A>
  <A HREF="mailto:tobi+mrtglink@oetiker.ch">&lt;tobi@oetiker.ch&gt;</A>
  and <A HREF="http://www.bungi.com/">Dave Rand</A> <A
HREF="mailto:dlr@bungi.com">&lt;dlr@bungi.com&gt;</A></FONT>
  </TD>
</TR>
</TABLE>
</BODY>
</HTML>
```

Con la configuración del archivo index.html, se tiene la página principal que se mostrará cuando se ingrese en un navegador de internet la dirección: “localhost/mrtg”, la cual arrojará el siguiente resultado (Ver Figura No.6.13):

Figura No.6.13-Página principal del sistema de monitoreo.

Una vez creado el archivo index.html se termina con la generación de las gráficas, quedando pendiente la configuración de los traps, cuyo proceso se explicará siguiente tema.

6.5. Creación de traps

Este tema abarcará la configuración de los traps en los sistemas operativos Windows Server 2008 y en Red Hat Enterprise Linux. Como se mencionó en el tema 5.4, además de las configuraciones por cada sistema operativo, los traps también serán configurados a través de la ILOM.

Los traps serán los encargados de enviar alertas a uno o más correos electrónicos, en caso de que ocurra algún evento inesperado, dichos eventos serán configurados por el administrador.

Red Hat Linux será el encargado de recibir los traps provenientes de todos los blades, tanto de sus direcciones IP primarias como de sus direcciones IP del ILOM. Para que Red Hat pueda cumplir con dicha función, se debe configurar el archivo "snmptrapd.conf" que define cómo opera el demonio que recibe traps snmp, si es que se llega a dar el caso.

El contenido del archivo debe quedar de la siguiente manera:

```
authCommunity log,execute, SER2

traphandle default /usr/bin/perl /usr/bin/traptoemail -f root -s
192.168.1.141 elayrubme@hotmail.com
```

donde:

- **`authCommunity log, execute, SER2.`** Es la configuración más sencilla para un archivo snmptrapd.conf, y significa que snmptrap procesará las notificaciones cuya comunidad lleve el nombre de SER2.
- **`traphandle default /usr/bin/perl /usr/bin/traptoemail -f root -s 192.168.1.141 elayrubme@hotmail.com.`** Esta línea indica que cualquier trap que sea recibido será enviado al correo elayrubme@hotmail a través del servidor SMTP 192.168.1.141.
  Traphandle es una utilidad de snmptrap donde se definen qué programas serán ejecutados cuando se reciba un trap, en este caso los programas que se ejecutan son perl y traptoemail, éste último encargado de enviar vía mail el reporte.

Si se deseara enviar el correo a más de un e-mail, bastaría con agregar un espacio y la dirección del correo deseado, quedando una línea similar a la siguiente:

```
traphandle default /usr/bin/perl /usr/bin/traptoemail -f root –s
192.168.1.141 elayrubme@hotmail.com [e-mail deseado]
```

Después de tener el archivo snmptrapd.conf correctamente configurado, es tiempo de comenzar la configuración en cada sistema operativo y en la ILOM.

Se comenzará explicando la configuración de los traps en los sistemas Windows Server 2008, para fines de ejemplificación, el proceso se explicará sólo una vez, pero la configuración se deberá realizar en los blades SER1, SER3 y SER4.

6.5.1. Configuración de traps en Windows Server 2008

Para configurar los traps en los sistemas operativos Windows Server 2008, se realiza un proceso similar al del tema 8.2.1. Se comienza por acceder a los servicios de Windows, de alguna de las siguientes maneras:

1. Start (Inicio) > Control Panel (Panel de Control) > Administrative Tools (Herramientas Administrativas) > Services (Servicios).
2. Start (Inicio) > Run (Ejecutar) > escribir “services.msc” > Aceptar.

Se debe seleccionar el SNMP Service o servicio SNMP, para que se muestre una ventana con siete pestañas, de las cuales se debe elegir la que lleva el nombre de Traps (Capturas). Una vez estando en dicha pestaña, se debe agregar el nombre de la comunidad para enviar los traps y la dirección IP hacia donde se enviarán los traps.

Para agregar la comunidad basta con dar click sobre el botón “Add to list (Agregar a la lista)”, e ingresar el nombre de la comunidad deseada. Por otro lado, para especificar hacia donde se dirigirán los traps que se generen, se debe dar click sobre el botón “Add (Agregar)”, que se encuentra en el campo de “Trap Destinations (Destinos Trap)”, y definir la dirección IP del host que recibirá los traps.

En el caso del sistema de monitoreo, se establece que la dirección encargada de recibir los traps es la 192.168.1.11 perteneciente al blade SER2, razón por la cual el nombre de la comunidad es el mismo que el del nombre del Blade (Ver Figura No.6.14).

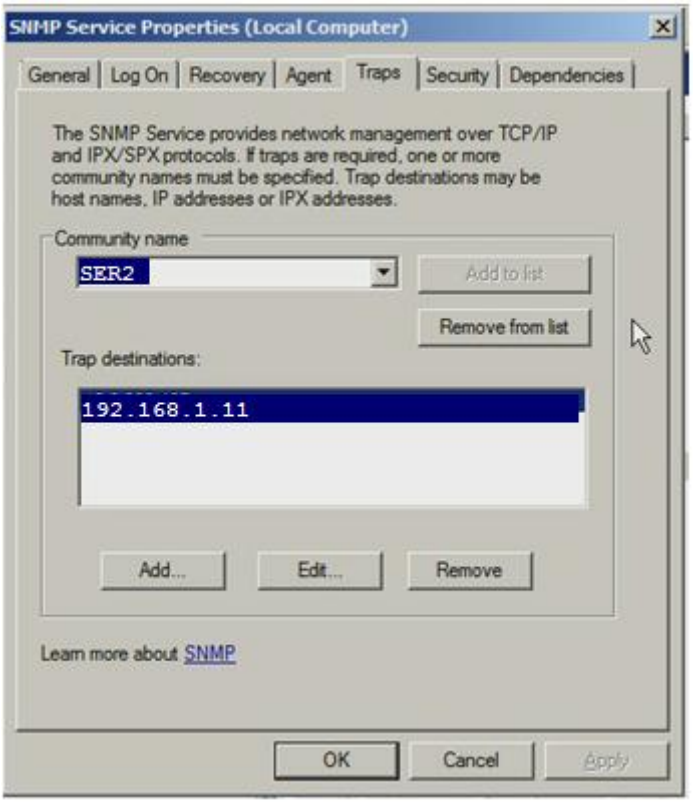


Figura No.6.14-Configuración de traps en Windows

Para guardar dicha configuración, se debe dar click sobre el botón OK y con ello Windows será capaz de enviar los traps que se generen hacia la dirección configurada.

Adicionalmente a la configuración anterior, se deben determinar los eventos que generarán traps. Ésta determinación se realiza con la ayuda del comando eventwin, el cual inicia un Event to Trap Translator (Traductor de evento a captura), el cual es un programa gráfico que permite configurar algunos tipos de traps previamente definidos dentro del sistema operativo Windows Server 2008.

Para ingresar al Event to Trap Translator (Traductor de evento a captura), se debe seguir la siguiente ruta:

Start (Inicio) > Run (Ejecutar) > escribir “evntwin” > OK (Ver Figura No.6.15).

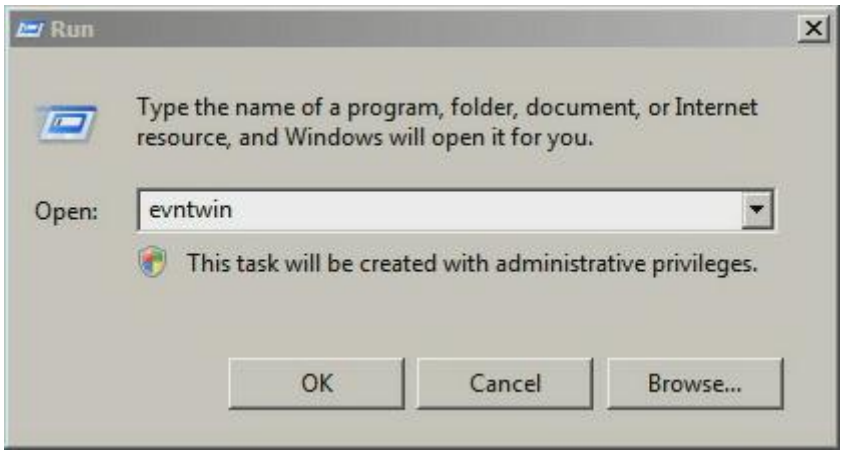


Figura No.6.15-Ejecución de evntwin

Al momento de realizar el procedimiento anterior, se muestra en pantalla la ventana perteneciente al Event to Trap Translator la cual brinda dos opciones de configuración: Custom (Personalizada) y Default (Predeterminada), se selecciona la opción de Custom (Personalizada), y posteriormente se da click sobre el botón Edit (Editar) para poder elegir que eventos generarán los traps.

Cuando se da click sobre el botón Edit, se despliega una lista de Event Sources (Orígenes de eventos) y los Events (Eventos), tal como lo muestra la Figura No.6.16.

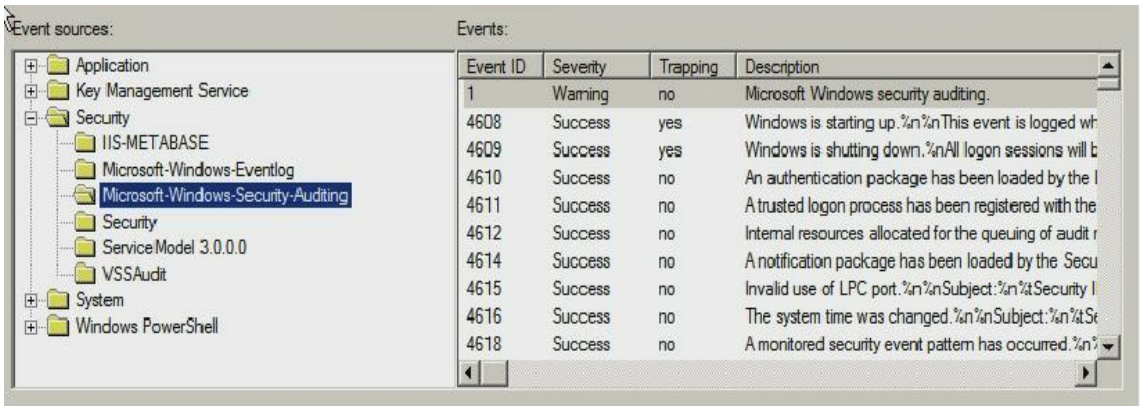


Figura No.6.16-Lista de orígenes de eventos y eventos.

De tales listas, se elegirán las variables que tienen que ver con: reinicio del sistema, apagado del sistema, inicio del sistema, error de autenticación de usuario, disco duro lleno y temperaturas fuera del umbral permitido.

Las variables de autenticación de usuario, reinicio, apagado e inicio de sistema se encuentran en la subcarpeta “Microsoft Windows Security Auditing” de la carpeta “Security”. Para lograr que dichos eventos generen traps, basta con seleccionar el evento deseado y dar click sobre el botón “Add (Agregar)”, ésta acción desplegará una ventana llamada “Properties (Propiedades)” donde sólo se debe seleccionar el botón “OK”.

Para generar el trap de espacio de disco duro insuficiente, se debe seleccionar la carpeta “Application (Aplicaciones)” para posteriormente elegir la subcarpeta “Chkdsk”, en ella se encuentra todo lo referente a los eventos que pueden ocurrir con las unidades de almacenamiento internas y externas, se debe seleccionar los eventos deseados y dar click sobre “Add (Agregar)” y posteriormente sobre “OK”.

En el caso de la variable de temperatura, se debe seleccionar la carpeta “ACPI” y en cada subcarpeta se buscarán y elegirán las variables relacionadas con las temperaturas. Los traps de la temperatura se activarán cuando ésta salga del rango de 5ºC a 32 ºC.

Para guardar y aplicar los cambios, se debe dar click sobre el botón “Aplicar”, posteriormente en “Aceptar” y reiniciar el servicio SNMP.

La Figura No.6.17 corresponde a los eventos que se eligieron para generar los traps en los Windows Server 2008.

Application	Chkdsk	1010	Success	1	0	%1 bytes available on disk.
Application	Chkdsk	1011	Success	1	0	%1 total bytes memory.
Application	Chkdsk	1012	Success	1	0	%1 bytes free.
Security	Microso...	4608	Success	1	0	Windows is starting up.%n%nThis event is logged when LSASS.E
Security	Microso...	4609	Success	1	0	Windows is shutting down.%nAll logon sessions will be terminated
Security	Microso...	4625	Success	1	0	An account failed to log on.%n%nSubject:%n%tSecurity ID:%t%t%
Security	Security	2	Success	1	0	Logon/Logoff
Security	Security	512	Success	1	0	Windows is starting up.
Security	Security	513	Success	1	0	Windows is shutting down. All logon sessions will be terminated b
System	acpi	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event
System	acpi	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event
System	adp94xx	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event
System	adp94xx	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event
System	adpahci	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event
System	adpahci	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event
System	adpu16...	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event
System	adpu16...	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event
System	adpu320	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event
System	adpu320	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event
System	aic78xx	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event
System	aic78xx	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event
System	AmdK8	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event
System	AmdK8	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event
System	adp94xx	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	adpahci	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	adpahci	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	adpu16...	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	adpu16...	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	adpu320	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	adpu320	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	aic78xx	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	aic78xx	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	AmdK8	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	AmdK8	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	eventlog	2013	Warning	1	0	The %2 disk is at or near capacity. You may need to delete some f
System	eventlog	4193	Error	1	0	Unable to read the configured IP addresses for network adapter %
System	eventlog	4194	Error	1	0	Unable to read the configured subnet masks for network adapter %
System	eventlog	4202	Informat...	1	0	The system detected that network adapter %2 was disconnected f
System	eventlog	6008	Warning	1	0	The previous system shutdown at %1 on %2 was unexpected.
System	eventlog	7007	Error	1	0	The system reverted to its last known good configuration. The syst
System	eventlog	9005	Error	1	0	%2 failed to bind to network adapter %3.
System	eventlog	9006	Error	1	0	%2 could not find network adapter %3.
System	eventlog	12502	Error	1	0	Service failed to start. Error = %1
System	Processor	111	Warning	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	Processor	112	Informat...	1	0	Machine Check Event reported is a CPU thermal throttling event re
System	SNMP	1001	Informat...	1	0	The SNMP Service has started successfully.
System	SNMP	1003	Informat...	1	0	The SNMP Service has stopped successfully.

Figura No.6.17-Lista de eventos que generan traps

Con ésta lista se concluye la explicación del procedimiento para configurar los traps SNMP en un sistema operativo Windows. Es el turno de explicar cuáles son los pasos a seguir para que al igual que los Windows Server 2008, Red Hat Enterprise Linux pueda generar y enviar traps a sí mismo.

6.5.2. Configuración de traps en Red Hat Enterprise Linux

El procedimiento inicia anexando las siguientes líneas en el archivo snmpd.conf, ubicado en el directorio /etc/snmp/snmpd.conf.

```
authtrapenable 1
trapcommunity SER2
trapsink 192.168.1.11
informsink 192.168.1.11
trap2sink 192.168.1.11

monitor -r 300 CargaAlta hrProcessorLoad > 20
monitor –r 300 MemoriaRAMAlta hrStorageUsed.2 > 31484880
```

La primera línea permite la generación de traps provenientes de un error de autenticación. Si no se deseara que éste tipo de traps se generara, el valor de authtrapenable debería ser 2.

Trapcommunity define la comunidad que se utilizará cuando se envíen los traps. Por su parte los comandos, trapsink, trap2sink e informsink, definen el host que recibirá los traps. El demonio envía un trap de tipo Cold Start cuando se inicia. Trap2sink se utiliza para enviar traps SNMPv2. Como se puede observar el host que recibirá los traps es el 192.168.1.11 y la comunidad trap es SER2.

Las líneas que comienzan con monitor, representan los traps que se configuran manualmente, esto quiere decir, que se les puede asignar el valor que se desee. Para ejemplificar se utilizará la línea de:

```
monitor –r 300 CargaAlta hrProcessorLoad > 20
```

Dónde:

-r 300, significa que cada 300 segundos se obtendrá el valor de la variable hrProcessorLoad, y en caso de que éste sea mayor a 20, enviará un trap que tendrá como título Carga Alta.

El último paso para poner a funcionar los traps en Red Hat Linux es reiniciar el servicio snmp, a través del comando `service snmpd restart.`

Como se puede notar, los traps de Red Hat Enterprise Linux son limitados en comparación con Windows Server 2008. La solución a esta limitación es configurar los traps de cada Blade y del Chassis, a través de la ILOM.

6.5.3. Configuración de traps a través de la ILOM

El procedimiento inicia con el ingreso a la ILOM y la activación de los traps dentro de la rama CMM del árbol cuya raíz es Chassis, el cual se encuentra en a parte superior izquierda de la página principal de la ILOM.

Cuando se selecciona CMM, se muestran una serie de pestañas correspondiente a la configuración de dicho elemento. Se debe elegir la pestaña de nombre “Configuration (Configuración)”, para posteriormente seleccionar la pestaña “Alert Management (Administración de Alertas)”, tal como se muestra en la Figura No.6.18.

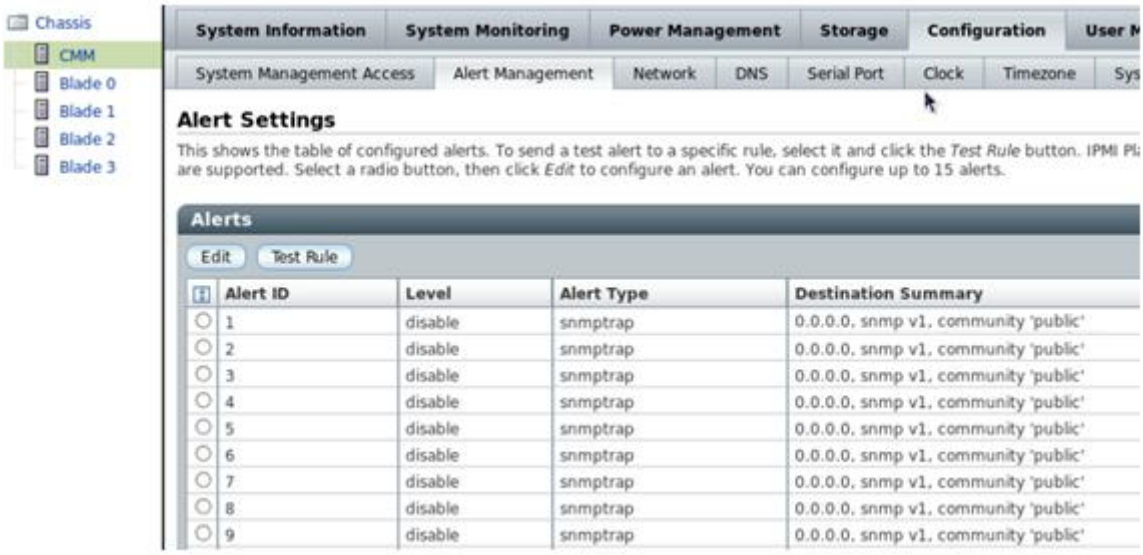


Figura No.6.18-Configuración de alertas

Las alertas se encuentran desactivadas por default, para activar las alertas se debe elegir la que se desee y dar click sobre el botón “Edit (Editar)”, ésta acción provocará que se muestre en pantalla una ventana como la que muestra la Figura No.6.19. En dicha ventana se debe seleccionar el nivel de importancia y el tipo de alerta, además de especificar hacia donde serán dirigidos los traps y cuál es el nombre de la comunidad.

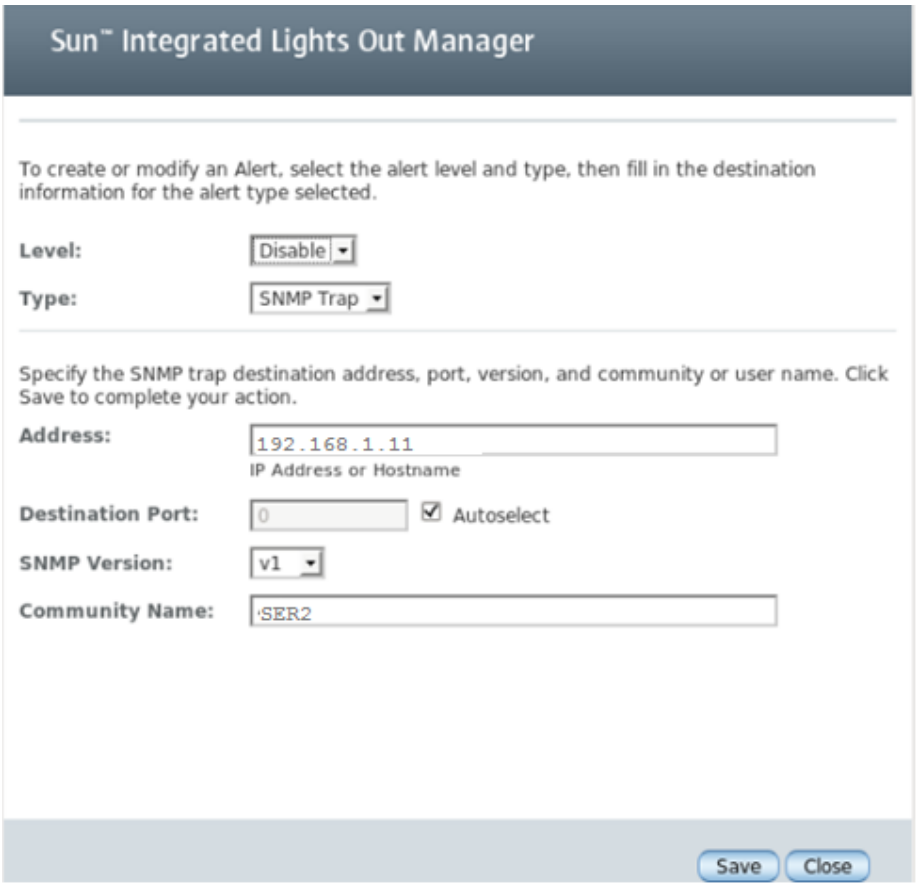


Figura No.6.19-Edición de las alertas

Los traps que la ILOM es capaz de generar se especificaron en el tema 5.4. Notificaciones TRAPS, donde también se indicó el nivel de importancia que tenía cada trap.

Los niveles de alertas que se pueden crear en la ILOM son: down, critical, major y minor. En el caso del sistema de monitoreo, se activará una de cata nivel de tipo SNMP Trap con la dirección IP 192.168.1.11 como destino para los traps y con el nombre de comunidad SER2.

Para que se apliquen y guarden los cambios, se debe dar click sobre el botón “Save (Guardar)” y posteriormente sobre “Close (Cerrar)”.

Es así como se termina la configuración de los traps, los cuales se recibirán si ocurre alguno de los eventos que fueron configurados en esta sección.

El siguiente paso es corroborar que el software, las gráficas y los traps hayan sido configurados correctamente, de tal modo que se hayan logrado obtener un sistema de monitoreo óptimo.

CAPÍTULO 7.

Pruebas y resultados

7. PRUEBAS Y RESULTADOS

En éste capítulo se describen las pruebas que se realizaron para comprobar el correcto funcionamiento del sistema de monitoreo, saber si realmente se están mostrando los valores reales de las variables, si se está obteniendo respuesta de cada sistema operativo y por último saber si los traps están siendo recibidos en el correo electrónico deseado. Además se muestra y explica el contenido de las gráficas creadas.

7.1. Pruebas para las gráficas

Cuando MRTG comienza a trabajar, genera una gráfica por cada Target que encuentre en el archivo de configuración mrtg.cfg, simultáneamente se crean los archivos log que llevan el nombre según su definición en Target. Por ejemplo:

`Target[192.168.1.10_10]: 10:SER1@192.168.1.10`, implica que se generará una gráfica, una página web y un archivo de registro (log) con el nombre "192.168.1.10_10".

Los archivos log servirán para saber si MRTG está funcionando correctamente y si está recolectando los datos adecuados, dichos archivos se encuentran en el directorio /var/www/html/mrtg.

Para abrir los archivos log, se puede realizar con cualquier editor de textos. Dentro de estos archivos se debe encontrar una lista de números, en su mayoría cero. El primer valor de la lista es de suma importancia para saber si MRTG está obteniendo los datos correctos, dicho valor debe ser diferente de -1, éste número indica que MRTG no puede obtener el valor de la variable deseada o que no puede borrar archivos pasados que le obstaculizan la creación de los archivos logs.

En caso de tener algún archivo log con valores de -1, se debe rectificar la configuración de los archivos MRTG y hacer los cambios pertinentes. Para saber que errores se están produciendo, además de acelerar el proceso de obtención de variables en MRTG, se debe ejecutar la siguiente línea:

```
env LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg
```

Esta línea envía la orden de ejecutar el proceso mrtg en base a lo establecido en el archivo mrtg.cfg, en el momento en que se ejecuta la línea, probablemente aparezcan una serie de advertencias y errores que evitan el correcto funcionamiento de MRTG.

Los errores se eliminan según la descripción de éstos, posiblemente alguna variable esté mal escrita o definida, éstos cambios se realizan manualmente. En caso de que no existan errores, pero si advertencias, sólo se debe ejecutar la línea `env LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg` las veces que sea necesario, hasta que ya no aparezcan las advertencias.

Una vez corregidos los errores y advertencias, los archivos log de cada variable deben tener un valor diferente a cero, tal como lo muestra la Figura No.7.1.

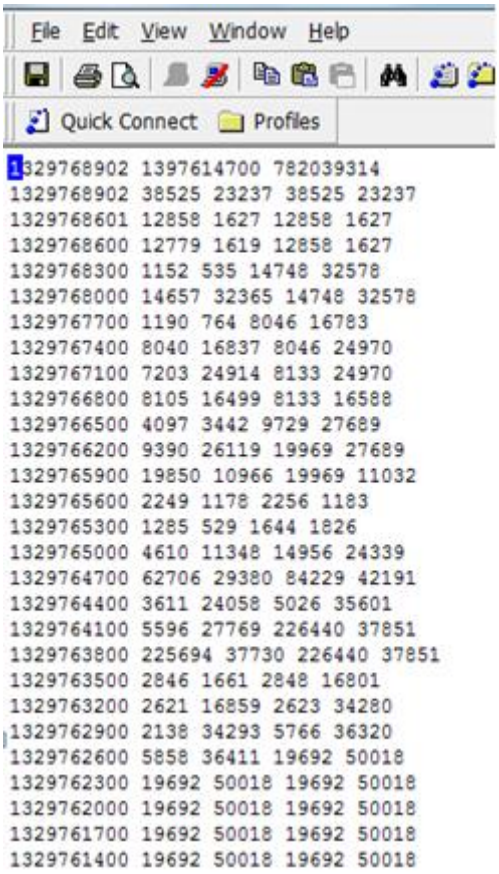


Figura No.7.1-Ejemplo de archivo 192.168.1.13_11.log

Con la comprobación del funcionamiento de MRTG se iniciará el periodo de pruebas para saber si SNMP y MRTG están brindando y obteniendo los datos deseados sobre la temperatura, memoria RAM, carga de CPU, tráfico Web y el tráfico de las tarjetas de red.

Para dichas variables, es fácil saber si realmente se están mostrando los valores correctos de cada variable en las gráficas y en los archivos de registro. Basta con realizar un snmpget de la variable deseada y checar que el valor de respuesta que aparece sea el mismo que el que esté dentro del archivo log y en la gráfica.

Además del método anterior, con ayuda del Administrador de tareas en Windows y el Monitor del sistema en Red Hat, se puede corroborar que las gráficas creadas muestran datos reales.

Otra manera de verificar el funcionamiento de MRTG respecto a la carga de CPU es a través de la utilización de muchos procesos dentro del servidor deseado, esto aumentará la carga en el CPU y se debe reflejar en las gráficas.

7.2. Pruebas de Traps

Para comprobar que cuando se genere un evento inesperado se envíe un trap al correo indicado, se realizarán dos pruebas:

1. La primera se realizará mediante la ILOM. Para iniciar con la prueba, se debe seleccionar la pestaña de "Configuration (Configuración)" y enseguida "Alert Management (Administración de Alertas)".
   Para lograr enviar el trap de prueba se debe seleccionar una de las alertas que previamente fueron activadas y dar click sobre el botón "Test Rule". Con esta acción se debe recibir un email con el siguiente contenido:

```
Host: <UNKNOWN> (UDP: [192.168.1.12]:4825->[192.168.1.11]:162)
DISMAN-EVENT-MIB::sysUpTimeInstance  0:0:02:06.68
SNMPv2-MIB::snmpTrapOID.0  SNMPv2-SMI::enterprises.42.2.175.103.2.0.63
SNMPv2-SMI::enterprises.42.2.175.103.2.1.1.0  ""
SNMPv2-SMI::enterprises.42.2.175.103.2.1.14.0  "1053BD1A7C::0816QAW0E0"
SNMPv2-SMI::enterprises.42.2.175.103.2.1.15.0  "SUN BLADE 6000 MODULAR
SYSTEM::Sun Blade X6250 Server Module"
SNMPv2-SMI::enterprises.42.2.175.103.2.1.20.0  "This is a test trap"
SNMP-COMMUNITY-MIB::snmpTrapAddress.0  192.168.1.1
SNMP-COMMUNITY-MIB::snmpTrapCommunity.0  "SER2"
SNMPv2-MIB::snmpTrapEnterprise.0  SNMPv2-SMI::enterprises.42.2.175.103.2
```

2. La segunda manera de revisar si los traps están funcionando correctamente, es iniciar cualquiera de los sistemas operativos Windows, provocando que se genere un trap como el que muestra la Figura No.7.2.

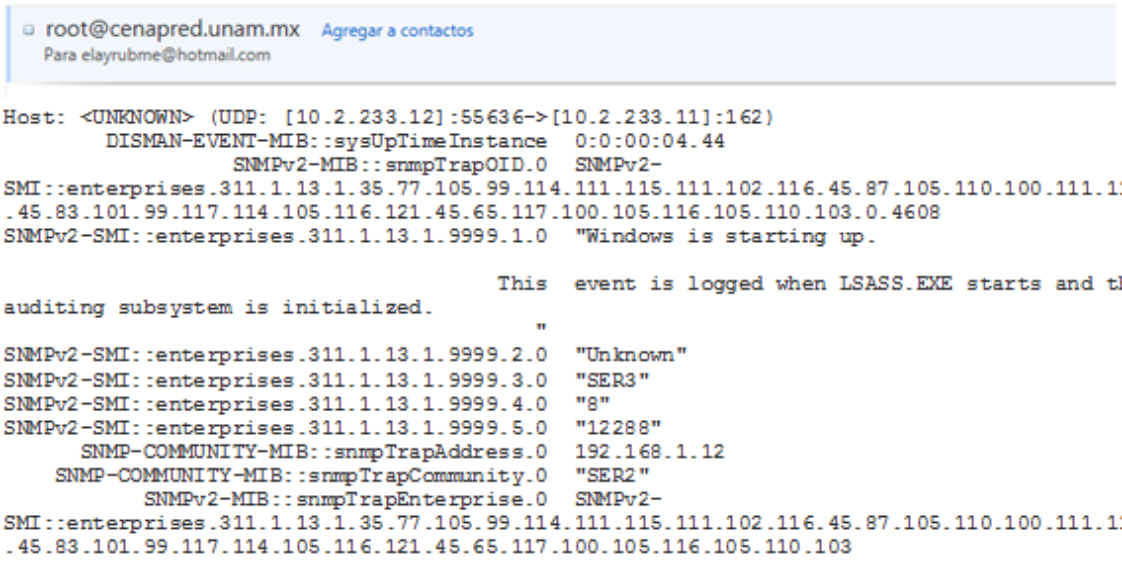


Figura No.7.2-Prueba de la recepción de traps.

Con la realización de las pruebas anteriores se rectifica que el sistema de monitoreo está funcionando como se desea y que está mostrando los resultados que se esperaban.

El sistema de monitoreo quedó correctamente configurado, monitorea, gráfica variables importantes como el tráfico de red, uso de la memoria RAM y además envía alertas en caso de que se genere un evento inesperado.

Ahora si es tiempo de conocer cuáles fueron los resultados obtenidos con la implementación del sistema de monitoreo Sun Blade 6000.

7.3. Productos generados

La página principal del sistema de monitoreo muestra cuatro gráficas correspondientes a las tarjetas de red de SER1, SER2, SER3 y SER4 respectivamente (Ver Figura No.7.3).

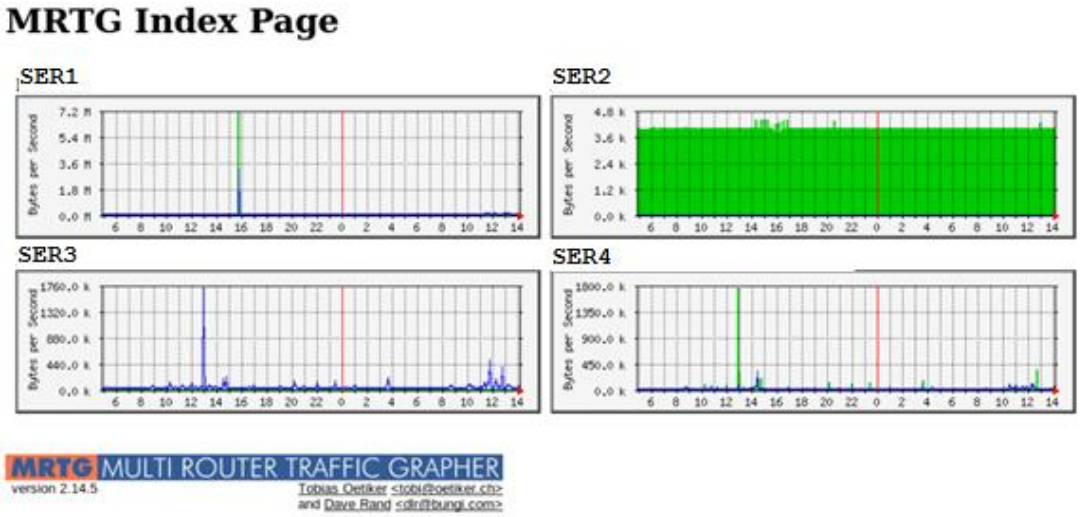


Figura No.7.3-Página de inicio del sistema de monitoreo.

En el momento que se selecciona SER1, se muestra en pantalla la Figura No.7.4, la cual enlista una serie de gráficas correspondientes a las variables seleccionadas en el tema 5.3. El archivo html que le da formato a la página de SER1 es el que lleva el nombre de SER1.html.

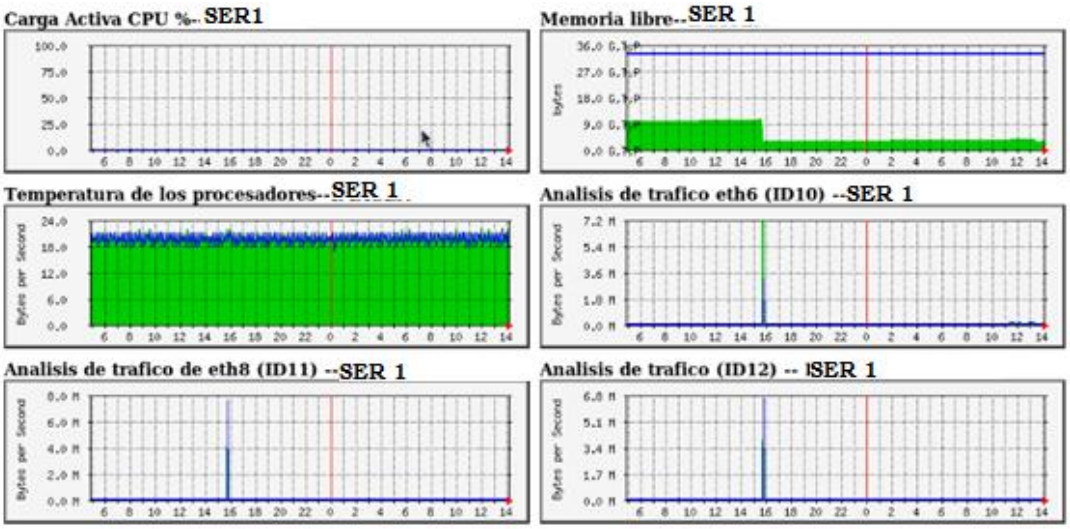


Figura No.7.4-Página SER1.html

En el caso de SER2 el archivo encargado de dar el formato html es SER2.html, dando por resultado las gráficas que se muestran en la Figura No.7.5.

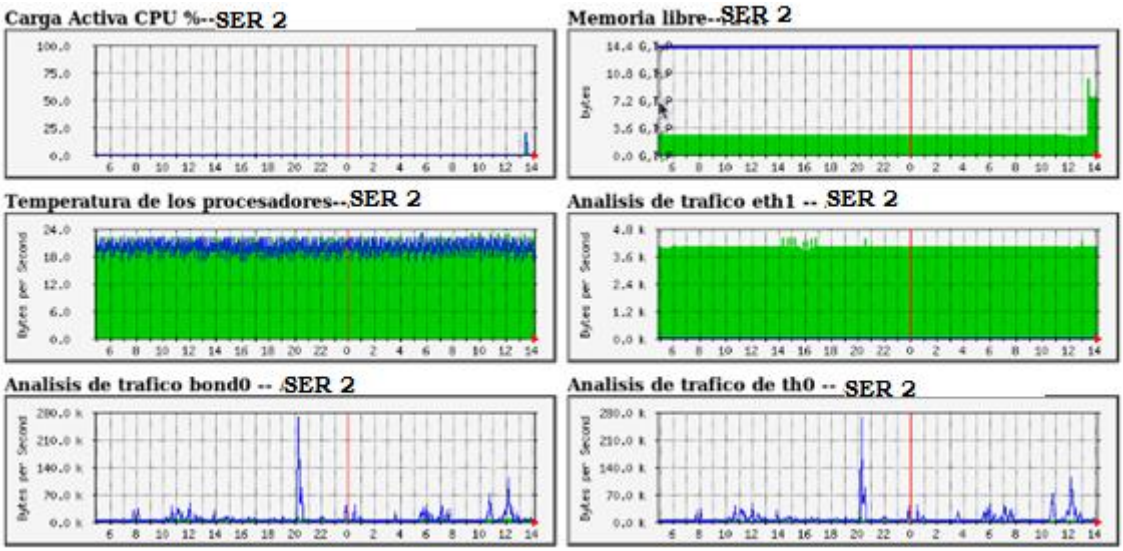


Figura No.7.5-Página SER2.html

El archivo SER3.html se ocupa de la estructura de la página correspondiente a SER3, la cual quedó como se muestra en la Figura No.7.6.

Figura No.7.6- Página específica de SER3.

Por último la página web de SER4, proviene del archivo SER4.html, el cual muestra el formato de la Figura No.7.7.

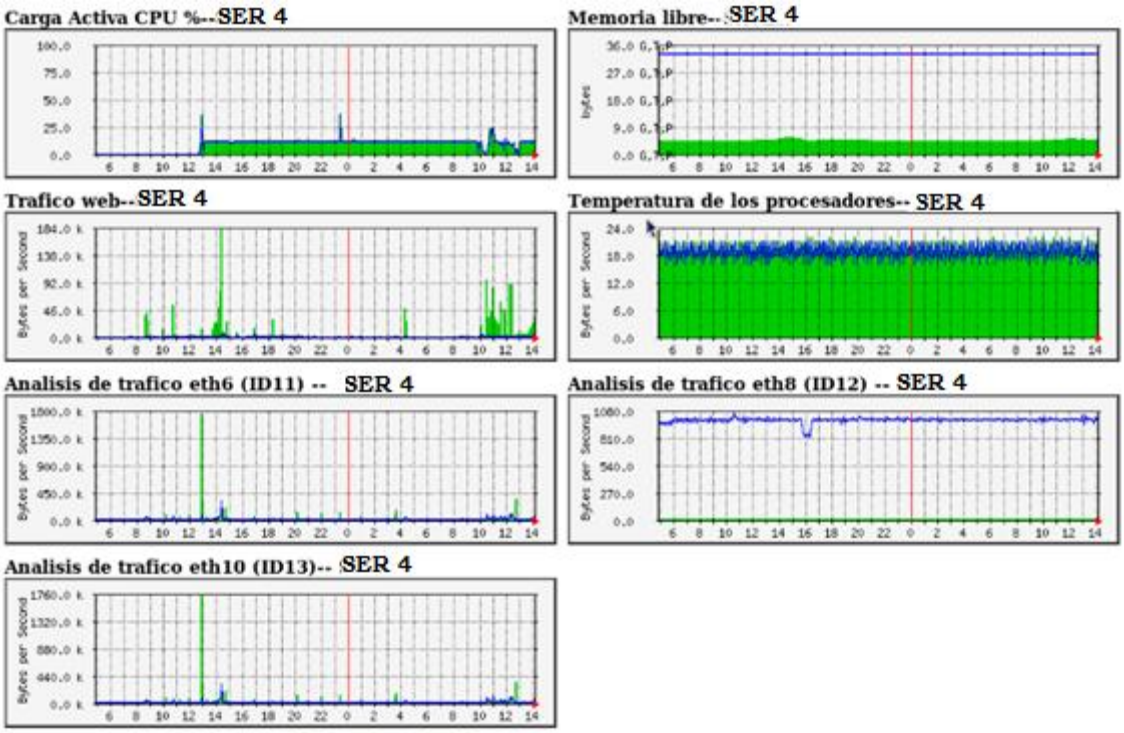


Figura No.7.7-Página web de SER4.

Para obtener más detalles gráficos sobre la variable que se desee, se da click en la gráfica correspondiente a la variable elegida. Por ejemplo si se quiere saber el comportamiento gráfico de las temperaturas, se debe seleccionar la gráfica de nombre “Temperatura de los procesadores”, ésta acción provoca que se muestre en pantalla una página web que contiene una gráfica diaria, semanal, mensual y anual del comportamiento de las temperaturas de procesador (Ver Figura No.7.8).

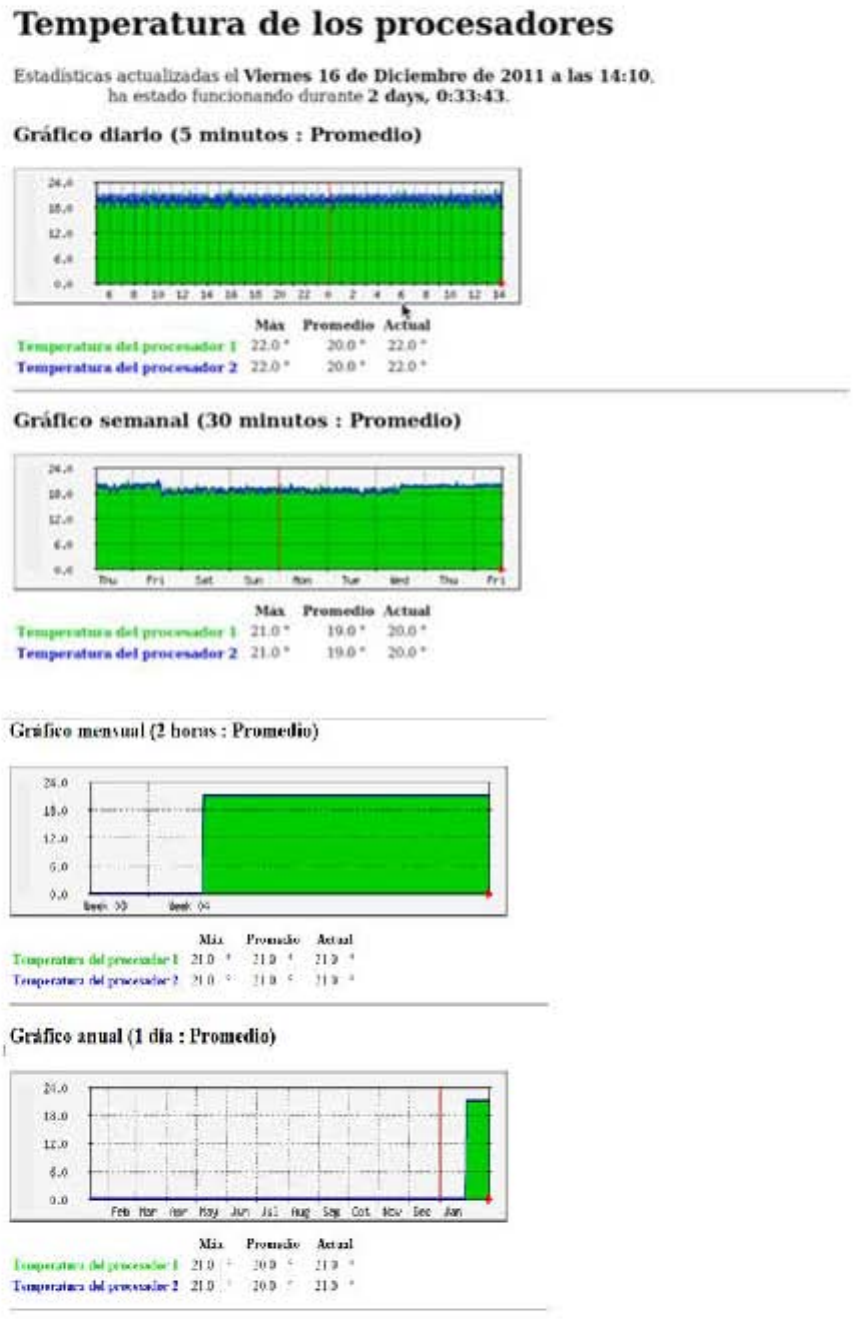


Figura No.7.8-Gráficas individuales de la temperatura de los procesadores.

En general, la página de cualquier variable seleccionada, muestra cuando fue la última actualización y por cuanto tiempo ha estado funcionando. Además cada gráfica cuenta con un valor máximo, promedio y actual.

La gráfica diaria muestra el comportamiento que ha tenido la variable durante el día, tomando su valor cada cinco minutos. Los números que aparecen en el eje “x”, corresponden a las horas del día, mientras que los números del eje “y”, representan los valores que la variable puede alcanzar, tal como lo muestra la Figura No.7.9.

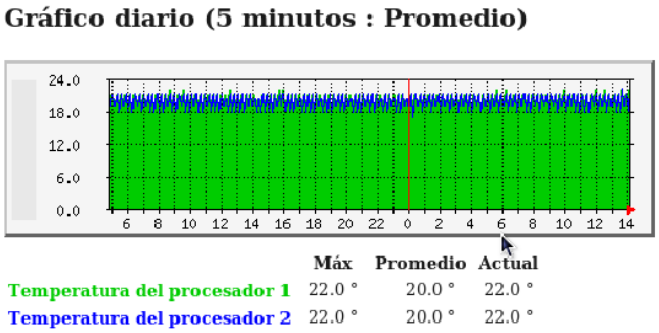


Figura No.7.9-Gráfica diaria de las temperaturas de los procesadores de SER1.

En seguida de la gráfica diaria, se encuentra la gráfica semanal en donde la acotación del eje “x” corresponde a los días de la semana y la acotación del eje “y” representa el valor que las temperaturas pueden alcanzar. Ésta gráfica obtiene los datos cada 30 minutos (Ver Figura No.7.10).

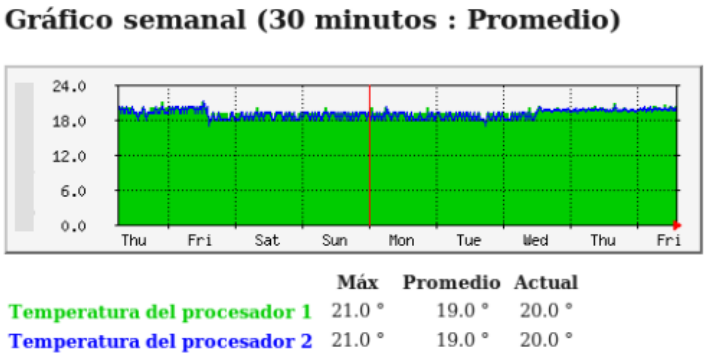


Figura No.7.10-Gráfica semanal de las temperaturas de los procesadores de SER1.

Después de la gráfica semanal, se encuentra la gráfica mensual, dicha gráfica toma los datos de la temperatura cada 2 horas y como se puede observar en la Figura No.7.11, el eje “x” representa las semanas transcurridas y el eje “y”, los valores de temperatura que puede llegar a alcanzar.

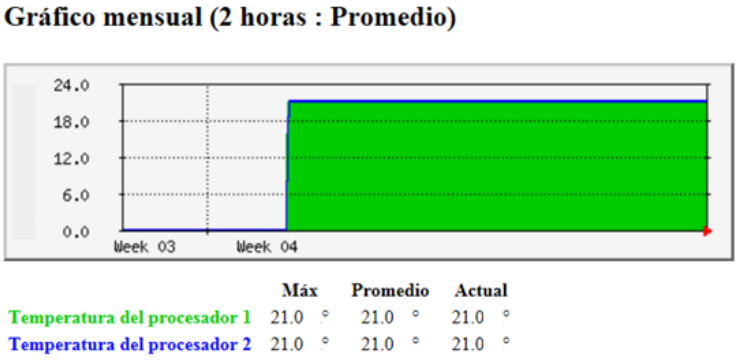


Figura No.7.11. Gráfica mensual de las temperaturas de los procesadores de SER1

Por último se encuentra la gráfica anual, la cual diario toma un solo valor, en el eje “x” muestra los meses del año y en el eje “y” el valor de la temperatura (Ver Figura No.7.12).

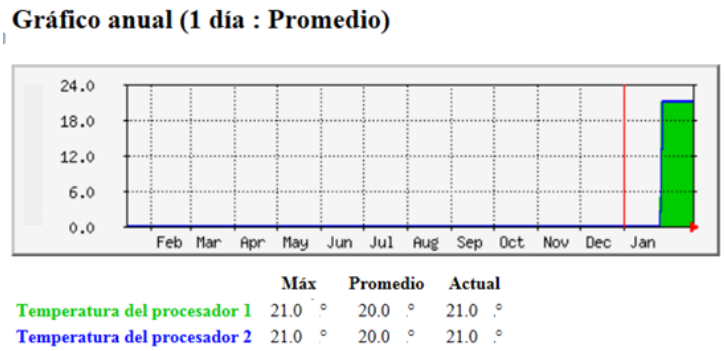


Figura No.7.12. Gráfica anual de las temperaturas de los procesadores de SER1

La interpretación de las otras gráficas de SER1, SER2, SER3 y SER4 es similar a la gráfica de temperatura de SER1. Para el caso de la carga activa del CPU (Ver Figura No.7.13) el eje “x”, según la gráfica que se observe, representa las 24 horas del día, los días de la semana, las semanas transcurridas o los meses del años, y el eje “y” el valor en porcentaje de la carga del CPU.

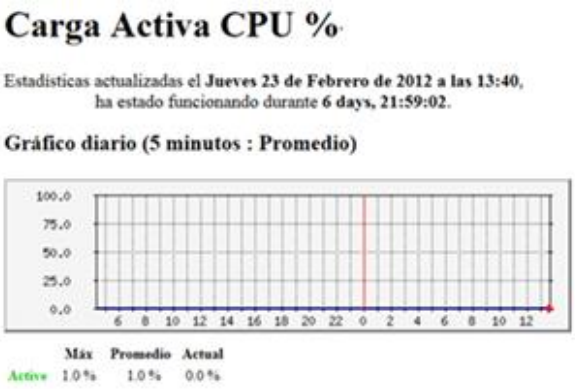


Figura No.7.13-Carga activa CPU

Para la gráfica de la memoria libre el eje x representa lo mismo que en las gráficas anteriores y el eje “y”, simboliza el tamaño de la Memoria RAM en uso y la memoria RAM total (Ver Figura No.7.14).

Figura No.7.14-Gráfica de Memoria libre.

La última gráfica que se muestra en la Figura No.7.15, corresponde al análisis de tráfico en las tarjetas de red.

Figura No.7.15.Análisis de tráfico web.

Para la parte de los traps, se obtuvieron los resultados esperados. A pesar de las dificultades para lograr que el servidor Sun Blade 6000 fallara, para comprobar que los traps estaban funcionando correctamente, se decidió que los traps con los que se realizarían las pruebas para obtener un resultado claro y específico serían los de error de autenticación, inicio de sistema, reinicio de servicio snmp y cambio de estados en las interfaces.

Para el caso del reinicio del sistema, SNMP cuenta con un trap que se envía por default cuando se inicia el servicio snmp, por lo tanto, para lograr que se reciba un trap de este tipo, se debe detener e iniciar el servicio snmp, acción que enviará un mail con el contenido que se muestra enseguida, el cual indica que el servicio SNMP se ha iniciado correctamente, así como el servidor sobre el cuál se realizó dicha acción.

```
Host: <UNKNOWN> (UDP: [192.168.1.12]:55636->[192.168.1.11]:162)
        DISMAN-EVENT-MIB::sysUpTimeInstance  0:0:00:04.44
                  SNMPv2-MIB::snmpTrapOID.0  SNMPv2-
SMI::enterprises.311.1.13.1.4.83.78.77.80.0.1090454505
SNMPv2-SMI::enterprises.311.1.13.1.9999.1.0  "The SNMP Service has
started successfully.
                                            "
SNMPv2-SMI::enterprises.311.1.13.1.9999.2.0  "Unknown"
SNMPv2-SMI::enterprises.311.1.13.1.9999.3.0  "SER3"
SNMPv2-SMI::enterprises.311.1.13.1.9999.4.0  "4"
SNMPv2-SMI::enterprises.311.1.13.1.9999.5.0  "0"
      SNMP-COMMUNITY-MIB::snmpTrapAddress.0  192.168.1.12
    SNMP-COMMUNITY-MIB::snmpTrapCommunity.0  "SER2"
           SNMPv2-MIB::snmpTrapEnterprise.0  SNMPv2-
SMI::enterprises.311.1.13.1.4.83.78.77.80
```

El segundo trap que se recibió, fue cuando un usuario ingresó mal su contraseña, generando el envío del mail con el contenido que se presenta a continuación, el cual muestra el Blade al que se intentó acceder, el nombre de la computadora y la dirección IP con la que quiso acceder.

```
Host: <UNKNOWN> (UDP: [192.168.1.12]:55636->[192.168.1.11]:162)
 DISMAN-EVENT-MIB::sysUpTimeInstance 0:14:11:21.82
 SNMPv2-MIB::snmpTrapOID.0 SNMPv2-
SMI::enterprises.311.1.13.1.35.77.105.99.114.111.115.111.102.116.45.87.10
5.110.100.111.119.115.45.83.101.99.117.114.105.116.121.45.65.117.100.105.
116.105.110.103.0.4625
 SNMPv2-SMI::enterprises.311.1.13.1.9999.1.0 "An account failed to log
on.

Subject:
     Security  ID:          S-1-0-0
     Account  Name:         -
     Account  Domain:               -
     Logon  ID:             0x0

     Logon  Type:                   3

     Account  For Which Logon Failed:
     Security  ID:          S-1-0-0
     Account  Name:         aframirez
     Account  Domain:               SECGOB

     Failure  Information:
     Failure  Reason:               Unknown user name or bad password.

    Status:  0xc000006d
    Sub  Status:            0xc0000064

    Process  Information:
    Caller  Process ID:     0x0
    Caller  Process Name:   -

    Network  Information:
      Workstation  Name:    H0001RAMSOTAN00
      Source  Network Address:      192.168.2.50
      Source  Port:         52054

   Detailed  Authentication Information:
      Logon  Process:               NtLmSsp
      Authentication  Package:      NTLM
      Transited  Services:  -
      Package  Name (NTLM only):    -
      Key  Length:          0
                                              "
 SNMPv2-SMI::enterprises.311.1.13.1.9999.2.0  "Unknown"
 SNMPv2-SMI::enterprises.311.1.13.1.9999.3.0  "SER3"
 SNMPv2-SMI::enterprises.311.1.13.1.9999.4.0  "16"
 SNMPv2-SMI::enterprises.311.1.13.1.9999.5.0  "12544"
 SNMPv2-SMI::enterprises.311.1.13.1.9999.6.0  "S-1-0-0"
 SNMPv2-SMI::enterprises.311.1.13.1.9999.7.0  "-"
 SNMPv2-SMI::enterprises.311.1.13.1.9999.8.0  "-"
 SNMPv2-SMI::enterprises.311.1.13.1.9999.9.0  "0x0"
SNMPv2-SMI::enterprises.311.1.13.1.9999.10.0  "S-1-0-0"
SNMPv2-SMI::enterprises.311.1.13.1.9999.11.0  "aframirez"
SNMPv2-SMI::enterprises.311.1.13.1.9999.12.0  "SECGOB"
```

```
SNMPv2-SMI::enterprises.311.1.13.1.9999.13.0  "0xc000006d"
SNMPv2-SMI::enterprises.311.1.13.1.9999.14.0  "Unknown user name or bad
password.
                                              "
SNMPv2-SMI::enterprises.311.1.13.1.9999.15.0  "0xc0000064"
SNMPv2-SMI::enterprises.311.1.13.1.9999.16.0  "3"
SNMPv2-SMI::enterprises.311.1.13.1.9999.17.0  "NtLmSsp "
SNMPv2-SMI::enterprises.311.1.13.1.9999.18.0  "NTLM"
SNMPv2-SMI::enterprises.311.1.13.1.9999.19.0  "H0001RAMSOTAN00"
SNMPv2-SMI::enterprises.311.1.13.1.9999.20.0  "-"
SNMPv2-SMI::enterprises.311.1.13.1.9999.21.0  "-"
SNMPv2-SMI::enterprises.311.1.13.1.9999.22.0  "0"
SNMPv2-SMI::enterprises.311.1.13.1.9999.23.0  "0x0"
SNMPv2-SMI::enterprises.311.1.13.1.9999.24.0  "-"
SNMPv2-SMI::enterprises.311.1.13.1.9999.25.0  "192.168.2.50"
SNMPv2-SMI::enterprises.311.1.13.1.9999.26.0  "52054"
       SNMP-COMMUNITY-MIB::snmpTrapAddress.0  192.168.1.12
     SNMP-COMMUNITY-MIB::snmpTrapCommunity.0  "SER2"
           SNMPv2-MIB::snmpTrapEnterprise.0  SNMPv2-
SMI::enterprises.311.1.13.1.35.77.105.99.114.111.115.111.102.116.45.87.10
5.110.100.111.119.115.45.83.101.99.117.114.105.116.121.45.65.117.100.105.
116.105.110.103
```

Será difícil que ocurra un error mayor dentro del Blade, ya que analizando el comportamiento de las gráficas se pueden prevenir muchos errores, sin embargo, las pruebas realizadas y los resultados obtenidos, comprueban que el sistema de monitoreo realmente está funcionando como se esperaba.

Durante la elaboración del proyecto se fueron pensando algunas ideas para mejorarlo, e incluso se decidió hacer alguno cambios para obtener un mejor resultado, con el fin de aumentar la eficiencia del sistema. Estos cambios, mejoras e implementaciones de seguridad serán descritos en el capítulo 8.

CAPÍTULO 8.

Mejoras al proyecto

8. MEJORAS AL PROYECTO

El proyecto es completamente exitoso, se alcanzó el objetivo de crear un sistema de monitoreo gráfico, capaz de enviar alertas SNMP vía correo electrónico, en caso de que ocurran eventos inesperados. Sin embargo existen dos problemas fundamentales dentro del sistema de monitoreo:

1. Cualquier usuario puede observar las gráficas de monitoreo.
2. El sistema de monitoreo fue instalado dentro del mismo Sun Blade 6000.

Las soluciones a los problemas anteriores, se explicarán en los temas 9.1 y 9.2 respectivamente.

8.1. Implementación de algunas medidas de seguridad

Todo el acceso a los blades está controlado por medio de contraseñas, firewalls, entre otras medidas de seguridad. El problema principal de seguridad del sistema de monitoreo es que cualquier usuario puede tener acceso a las páginas web donde se muestran las gráficas. Este hecho atenta contra la confidencialidad de los datos y hace al sistema de monitoreo muy vulnerable a los ataques pasivos, los cuales pueden llegar a convertirse en ataques activos.

Afortunadamente para solucionar el problema anterior, MRTG cuenta con un archivo en donde se puede configurar la seguridad mediante IPTABLES. Dicho archivo se encuentra en el directorio /etc/httpd/conf.d/mrtg.conf, el cual maneja una política prohibitiva, lo que implica que se prohíbe el acceso a todos los hosts que no estén especificados en el archivo.

El archivo mrtg.conf se puede abrir con cualquier editor de texto, y el contenido debe ser similar al siguiente:

```
# This configuration file maps the mrtg output (generated daily)
# into the URL space.  By default these results are only
accessible
# from the local host.
#
Alias /mrtg /var/www/html/mrtg

<Location /mrtg>
    Order deny,allow
    Allow from 192.168.2.131

    Allow from 192.168.2.159
    Deny from all
    # Allow from .example.com
</Location>
```

La línea `Alias /mrtg /var/www/html/mrtg` refiere el directorio sobre el que se aplicarán las IPTABLES. Se observa que sólo existen dos direcciones IP que tienen permiso para ver las gráficas, cualquier host con una IP diferente a 192.168.2.131 o 192.168.2.159 no podrá tener acceso a la página web en donde se muestran las gráficas.

Si se desea brindar privilegio a otro host, basta con agregar la línea `Allow from [dirección IP del host deseado]` debajo de la última línea con el mismo formato, guardar los cambios y reiniciar el servicio httpd.

Con este archivo queda restringido el acceso a las gráficas, mejorando la seguridad en el sistema de monitoreo del Sun Blade 6000.

Hasta este momento se ha solucionado el problema de seguridad, sin embargo, aún existe el inconveniente de tener instalado el sistema de monitoreo dentro del Sun Blade 6000, la solución a dicho problema se abordará en el siguiente tema.

8.2. Migración del sistema de monitoreo

El sistema de monitoreo se encuentra instalado dentro del Sun Blade 6000, lo que implica que el sistema operativo Red Hat funge como administrador SNMP y entidad administrada a la vez. Mientras Red Hat funcione correctamente no hay ningún problema, pero, ¿qué sucede si Red Hat falla y se apaga?, la respuesta es simple: el sistema de monitoreo deja de funcionar.

Para evitar la situación de que el sistema de monitoreo falle, se decidió mudarlo a otro servidor dentro de la red local con sistema operativo OpenSuse, el cual también es una distribución de Linux, por lo tanto la configuración será prácticamente igual.

El servidor con OpenSuse será el encargado de ser el administrador SNMP, mostrará las gráficas en su página web local y recibirá los traps que se envíen desde cualquier Blade o del Chassis.

La configuración inicia con la instalación del servidor web, que al igual que en el caso de Red Hat, será apache, la cual se realiza ejecutando el comando:

```
zypper install apache2
```

Posteriormente se debe indicar que apache2 inicie automáticamente cuando el sistema arranque a través del comando:

```
chkconfig –add apache2
```

Para concluir con la instalación del servidor http, se debe iniciar el servicio apache mediante el comando:

```
/etc/init.d/apache2 start.
```

Ahora es tiempo de instalar snmp y mrtg con ayuda de los comandos:

- `zypper install net-snmp`
- `zypper install mtrg`

A diferencia de Red Hat Enterprise Linux que requiere de la instalación de dos paqueterías SNMP, Open Suse sólo necesita la paquetería net-snmp, es por ello que solamente se instalan las dos paqueterías anteriores, una correspondiente a SNMP y otra a MRTG.

La instalación de los archivos generarán los archivos snmpd.conf, snmptrapd.conf, de los cuales sólo se configurará snmptrapd.conf, el contenido de este archivo debe quedar igual que para el caso de Red Hat Enterprise, el cual es el siguiente:

```
authCommunity log,execute, OPEN

traphandle default /usr/bin/perl /usr/bin/traptoemail -f root -s
192.168.1.141 elayrubme@hotmail.com
```

Se puede notar, que la comunidad para los traps cambió, esto debido a que se cambió de servidor, sin embargo todo lo demás continúa igual que en el archivo snmptrapd.conf de Red Hat Enterprise Linux.

Para el caso de MRTG, se debe crear una carpeta de nombre mrtg dentro del directorio /srv/www/htdocs/mrtg, que es donde se encuentran los archivos que se presentan en la página web local. Además se debe generar otra carpeta del mismo nombre en el directorio /etc/mrtg/ para que en ella se almacenen los archivos de configuración mrtg.cfg, mrtg1.cfg, mrtg2.cfg, mrtg3.cfg y mrtg4.cfg.

Los archivos de configuración de MRTG para OpenSuse sólo manejarán los OID numéricos, si se desea ver el contenido de dichos archivos, se debe ir a los Anexos 10, 11, 12, 13 y 14.

Por otro lado, para generar las páginas web en OpenSuse, se hará del mismo modo como se realizó para Red Hat Enterprise Linux, sólo que con algunas diferencias:

- Para la página web de SER1:

```
indexmaker /etc/mrtg/mrtg1.cfg >> /srv/www/htdocs/mrtg/SER1.html
```

- Para la página web de SER2 :

```
indexmaker /etc/mrtg/mrtg2.cfg >> /srv/www/htdocs/mrtg/SER2.html
```

- Para la página web de SER3 :

```
indexmaker /etc/mrtg/mrtg3.cfg >> /srv/www/htdocs/mrtg/SER3.html
```

- Para la página web de SER4 :

```
indexmaker /etc/mrtg/mrtg1.cfg >> /srv/www/htdocs/mrtg/SER4.html
```

Los archivos SER1.html, SER2.html, SER3.html, SER4.html e index.html quedan con el mismo formato que para RHEL. Para implementar seguridad en todas las páginas web, es necesario crea el archivo mrtg.conf dentro del directorio /etc/apache2/conf.d/ cuyo contenido es el siguiente:

```
Alias /mrtg /srv/www/htdocs/mrtg

<Location /mrtg>
    Order deny,allow
```

```
    Allow from 192.168.2.131

    Allow from 192.168.2.159
    Deny from all
    # Allow from .example.com
</Location>
```

Este archivo permite que los host 192.168.2.131 y 192.168.2.159 tengan acceso a las gráficas, todos los demás host que intenten verlas, no podrán hacerlo.

El último paso es la configuración del envío de los traps en los sistemas operativos Red Hat Enterprise Linux, Windows Server 2008 y en la ILOM.

El procedimiento de los traps inicia anexando las siguientes líneas en el archivo snmpd.conf, ubicado en el directorio /etc/snmp/snmpd.conf, en el sistema operativo Red Hat Enterprises Linux (Ver Anexo 19).

```
authtrapenable 1
trapcommunity OPENSUSE
trapsink 192.168.1.160
informsink 192.168.1.160
trap2sink 192.168.1.160
```

La configuración en OpenSuse concluye con el reinicio de los servicios, apache2 y snmpd.

Para la configuración en Windows, se debe abrir el Servicio SNMP, ir a la pestaña que lleva el nombre de Traps (Capturas), agregar el nombre de la comunidad para enviar los traps y la dirección IP hacia donde se enviarán los traps.

Para agregar la comunidad basta con dar click sobre el botón “Add to list (Agregar a la lista)”, e ingresar el nombre de la comunidad deseada. Por otro lado, para especificar hacia donde se dirigirán los traps que se generen, se debe dar click sobre el botón “Add (Agregar)”, que se encuentra en el campo de “Trap Destinations (Destinos Trap)”, y definir la dirección IP del host que recibirá los traps.

En este caso, se establece que la dirección encargada de recibir los traps es la 192.168.1.160 con el nombre de comunidad OPENSUSE.

Para guardar dicha configuración, se debe dar click sobre el botón OK y con ello Windows será capaz de enviar los traps que se generen hacia la dirección configurada. Además se debe reiniciar el servicio SNMP.

Con respecto a la ILOM, se debe ir la pestaña de nombre “Configuration (Configuración)”, para posteriormente seleccionar la pestaña “Alert Management (Administración de Alertas)”.

Para modificar las alertas se debe elegir la que se desee y dar click sobre el botón “Edit (Editar)”, ésta acción provocará que se muestre en pantalla una ventana donde se debe seleccionar el nivel de importancia y el tipo de alerta, además de especificar hacia donde serán dirigidos los traps y cuál es el nombre de la comunidad.

En esta ocasión la dirección IP 192.168.1.160 se utilizará como destino para los traps y el nombre de comunidad OPENSUSE.

Para que se apliquen y guarden los cambios, se debe dar click sobre el botón “Save (Guardar)” y posteriormente sobre “Close (Cerrar)”.

Con estas mejoras, logramos obtener un sistema de monitoreo más seguro, con mayor eficiencia y una mejor estabilidad, así mismo, se concluye con la explicación teórica del proyecto que actualmente está siendo usado por el Centro Nacional de Prevención de Desastres, administrado por la Ingeniera Alejandra Zuñiga Medel.

CONCLUSIONES

CONCLUSIONES

Con base en los objetivos específicados al inicio de este trabajo, se puede concluir que el proyecto es un éxito total debido a que:

- ✓ Se logró planear, organizar, integrar, dirigir y controlar un sistema de monitoreo del servidor ORACLE-SUN Blade 6000, a través del protocolo SNMP y la herramienta MRTG.
- ✓ El sistema de monitoreo puede solucionar problemas de red, problemas de software y/o problemas de hardware que se presenten, permitiendo tomar las medidas necesarias para disminuir el impacto en caso de falla de los sistemas, así como reducir el tiempo de localización de errores.
- ✓ Se creó un sistema de monitoreo gráfico, amigable y fácil de interpretar.
- ✓ Se graficó el comportamiento de la temperatura de los procesadores, el tráfico web, la carga del CPU, la memoria RAM y el tráfico en las tarjetas de red.
- ✓ Se ensambló el sistema de monitoreo en una página web, donde se puede observar el comportamiento de las variables de hardware y software que se mencionaron en el punto anterior.
- ✓ Se logró enviar alertas SNMP a cualquier correo electrónico que se desee cuando ocurran eventos inesperados en el servidor ORACLE-SUN Blade 6000.

GLOSARIO

GLOSARIO

A

ACL (Access Control List, Lista de Control de Acceso). Listas que permiten controlar el flujo del tráfico en equipos de redes, tales como routers y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

Aplicación cliente/servidor. Aplicación que se almacena en una posición central en un servidor y a la que tienen acceso lsa estaciones de trabajo, lo que hace que sean fáciles de mantener y proteger.

Amenaza. Todo aquello que intenta o pretende destruir.

Ataque activo. Implican algún tipo de modificación del flujo de datos o la creación de un falso flujo de datos.

Ataque pasivo. El atacante no altera la información, únicamente la observa, escucha , obtiene o monitorea miestras está siendo transmitida.

B

Backbone. (Núcleo Estructural de la Red). Es el cable que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

Broadcast. Paquete de datos enciado a todos los nodos de una red.

Byte. Serie de dígitos binarios consecutivos que operan como una unidad.

C

Cable coaxial. Cable que consta de un conductor cilíndrico externo hueco, que reviste a un conductor con un solo cable interno.

CDMA (Code Division Multiple Access, Acceso Múltiple por División de Código). Es un término genérico que define una interface inalámbrica basada en la tecnología de espectro extendido. Para la telefonía celular, CDMA es una técnica de acceso múltiple especificada por la TIA (Telecommunications Industry Association).

CIDR (Classless Inter-Domain Routing: Enrutamiento sin Clase entre Dominios). Técnica que permite que los routers agrupen rutas para reducir la cantidad de información de enrutamiento transportada por los routers principales.

Cifrado. Método para proteger los datos de un acceso no autorizado a los mismos.

Circuito. Ruta de comunicaciones entre dos o más puntos

Cliente. Nodo o programa de software que requiere servicios de un servidor.

Cliente/Servidor. Arquitectura de la relación entre una estación de trabajo y un servidor en una red.

Colisión. Resultado de dos nodos que transmiten simultáneamente. Las tramas de cada dispositivo impactan y se dañan cuando se encuentran en el medio físico.

Conmutación. Proceso de tomar una trama entrante de una interface y enviarla a través de otra interfaz.

Confiabilidad. Proporción entre los mensajes de actividad esperados y recibidos de un enlace. Si la relación es alta, la línea es confiable. Es utilizada como métrica de enrutamiento.

CSMA/CD. (Carrier Sense Multiple Access with Collision Detection, Acceso Multiple con Detección de Portadora y Detección de Colisiones) Mecanismo de acceso a medios dentro de la cual los dispositivos que están listos para transmitir datos primero verifican el canal, en busca de una portadora. El dispositivo puede transmitir si no se detecta ninguna portadora durante un periodo de tiempo determinado. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que colisionan, Esta colisión, subsecuentemente demora las retransmisiones desde esos dispositivos durante un periodo de tiempo de duración aleatoria.

D

Datagrama. Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son unidades de información primaria de la Internet.

Dirección. Estructura de datos o convención lógica utilizada para identificar una entidad única, como un proceso o un dispositivo de red en particular.

Dirección IP. Dirección de 32 bits asignada a los host mediante TCP/IP. Una dirección IP se escribe en forma de 4 octetos separados por puntos. Cada dirección consta de un número de red, un número opcional de subred y un número de host.

Dirección origen. Dirección de un dispositivo de red que encía datos.

DSL. (Digital Suscriber Line) Tecnología de red que permite conexiones de banda ancha sobre el cable de cobre a distancias limitadas. Existen cuatro tipos de DSL: ADSL, HDSL, SDSL y VDSL. Todas estas tecnologías funcionan a través de pares de módems, con un módem localizado en la oficina central y el otro en el lugar del cliente.

DWDM. (Dense Wavelength Division Multiplexing, Multiplexación por División de Longitud de Onda) Es una tecnología que emplea múltiples ondas para transmitir señales sobre una sola fibra óptica.

E

Encabezado. Información de control colocada antes de los datos al encapsularlos para la transmisión en la red.

Encapsulamiento. Proceso que consiste en colocar un cifrado en los datos de un encabezado de un protocolo en particular.

Escalabilidad. Capacidad de una red para aumentar de tamaño sin que sea necesario realizar cambios importantes en el diseño general.

Estándar. Conjunto de reglas o procedimientos de uso generalizado o de carácter oficial.

Ethernet. Método de conexión más común en las redes de área local. En el caso de Ethernet, todas las estaciones del segmento comparten el ancho de banda total, que es de 10 Megabits por segundo (Mbps), 100 Mbps para FastEthernet o 1000 Mbps para Gigabit Ethernet.

F

FastEthernet. Cualquiera de varias especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10Base-T, aunque preserva características tales como formato de trama, mecanismos MAC y MTU.

FDDI. (Fiber Distributed Data Interface, Interfaz de Datos Distribuida por Fibra). Estándar de LAN, definido por ANSI X3T9.5, que especifica una red de transmisión de token de 100 Mbps que utiliza cable de fibra óptica, con distancias de transmisión de hasta dos kilómetros. FDDI usa una arquitectura de anillo doble para brindar redundancia.

Fibra óptica. Fibra basada en el vidrio, que sustituye a los clásicos cables de cobre y permite transmitir un gran volumen de información a alta velocidad y a gran distancia. La información no se transmite mediante impulsos eléctricos, sino que se modula en una onda de luz generada por un láser.

Firewall. Colección de componentes colocados entre una red interna y una red externa para que sólo el tráfico que es autorizado por la política de seguridad de la red interna esté permitido pasar.

Frame Relay. Protocolo conmutado de la capa de enlace de datos, de norma industrial, que administra varios circuitos virtuales utilizando un encapsulamiento HDLC entre dispositivos conectados.

G

Gateway. Nodo de interconexión entre dos redes incompatibles, es un sistema capaz de enviar información entre dos o más redes con estándares, arquitecturas y protocolos diferentes.

H

HDLC. (High Level Data Link Control, Control de Enlace de Datos de Alto Nivel) Protocolo síncrono de la capa de enlace de datos, orientado a bit, desarrollado por ISO. HDLC especifica un método de encapsulamiento de datos en enlaces síncronos seriales que utiliza caracteres de trama y sumas de comprobación.

HDSL. (High Data-Rate Digital Suscriber Line, Línea Digital del Suscriptor de Alta Velocidad)

Host. Término general que se utiliza para describir computadoras centrales y microcomputadoras.

HTML. (Hyper Text Markup Language, Lenguaje de Etiquetas por Hipertexto) Formato simple de documentos en hipertexto que usa etiquetas para indicar cómo un aplicación de visualización, como por ejemplo un navegador de la web, debe interpretar una parte determinada de un documento.

HTTP. (Hypertext Transfer Protocol, Protocolo de Transferencia de Hipertexto) Protocolo utilizado por los navegadores y servidores de la web para transferir archivos.

Hub. Dispositivo que sirve como centro de una topología en estrella, también denominado repetidor.

I

ICMP. (Internet Control Message Protocol, Protocolo de Mensajes de Control en Internet) Protocolo de internet de capa de red que informa de errores y brinda información relativa al procesamiento de paquetes IP.

Interfaz. Conexión entre dos sistemas o dispositivos.

Interoperabilidad. Capacidad de los equipos de diferentes fabricantes de comunicarse entre sí.

L

Loopback. Dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí.

M

Mensaje. Agrupación lógica de información de la capa de aplicación, a menudo compuesta por una cantidad de agrupaciones lógicas de las capas inferiores.

Multicast. Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red.

N

NAT. (Network Address Translation, Traducción de Direcciones de Red) Mecanismo que reduce la necesidad de tener direcciones IP exclusivas globales. NAT permite que las organizaciones cuyas direcciones no son globalmente exclusivas, se conecten a interntet, transformando esas direcciones en espacio de direccionamiento enrutable global.

NCP. (Network Control Program, Programa de Control de Red) Programa que enruta y controla el flujo de datos entre un controlador de comunicaciones y otros recursos de red.

Nodo. Punto final de una conexión de red o una unión que es común para dos o más líneas de una red.

P

Política de seguridad. Conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de la seguridad.

Protocolo. Descripción formal de un conjunto de normas y convenciones que establecen la forma en que los dispositivos de una red intercambian información.

Puerto. Interfaz en un dispositivo de interconexión.

R

Redundancia. Duplicación de dispositivos, servicios o conexiones de modo que, en caso de que se produzca una falla, los equipos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce el error.

Router. Dispositivo de la capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red.

S

Segmentación. Proceso de división de un solo dominio de colisión en dos o más dominios de colisión para reducir las colisiones y la congestión de red.

Seguridad. Confianza, tranquilidad, certidumbre procedente de la idea de que no hay peligro que temer.

Seguridad de la red. Es la protección de los recursos de la red, la información y servicios en contra de las amenazas de seguridad.

Servidor. Nodo o programa de software que suministra servicios a los clientes.

Switch. Dispositivo que conecta computadoras.

T

Telnet. Protocolo de emulación de terminal estándar de la pila de protocolo TCP/IP. Telnet se usa para la conexión de terminales remotas, permitiendo que los usuarios se registren en sistemas remotos y utilicen los recursos como si estuviesen conectados a un sistema local.

U

Unicast. Mensaje que se envía a un solo destino de red.

LITERATURA CITADA

LITERATURA CITADA

1) ALONSO Gonzalo, *"Auditoria Informática"*, Madrid: Editorial Díaz de Santos, 1988; 39-45.
2) ANDREU Joaquín, *"Redes locales"*, 1ª Edición, España: Editorial Editex, 2011; 170.
3) ANDREU Joaquín, *"Servicios en red",* 1ª Edición, España: Editorial Editex,2010; 215-218
4) AREITIO Javier, *"Seguridad de la Información"*, 1ª Edición, España: Editorial Paraninfo, 2008; 130-131
5) BARBA Antoni, *"Gestión de red",* 1ª Edición, Barcelona: Editorial Edicions UPC, 1999: 1-231.
6) BARBA Antoni, "*Inteligencia de red",* 1ª Edición, Barcelona: Editorial Edicions UPC, 2002; 63-70, 213-224.
7) BARCELÓ José, *"Protocolos y aplicaciones internet"*, 1ª Edición, Barcelona: Editorial UOC, 2008; 205-220.
8) BATEMAN Andy, *"Comunicaciones digitales, Diseño para el mundo real"*, 1ª edición, España: Editorial marcombo, 2003; 22.
9) CABEZAS José Damián, *"Sistemas de telefonía"*, 1ª Edición, España: Editorial Thomson, 2007; 122-132.
10) CASTRO Antonio, *"Teleinformática para Ingenieros en Sistemas de Información"*, 2ª Edición, España: Editorial Reverte, 1999; 246-260.
11) Currícula CCNA Exploration 4.0. Aspectos básicos de networking.
12) DESONGLES Juan, *"Técnicos de soporte informático",* 1ª Edición, España: Editorial MAD, S.L, 2005; 285-291.
13) DOUGLAS Mauro, *"Essential SNMP"*, 2ª Edición, USA: Editorial O´Reilly, 2005, 1-315
14) ESPAÑA María Carmen, *"Servicios avanzados de telecomunicación"*, 1ª Edición, España: Editorial Díaz de Santos, 2003; 108-117
15) GIL Pablo; POMARES Jorge; CANDELAS Francisco, "*Redes y Transmisión de Datos",* 1ª edición, España: Editorial Servicio de Publicaciones de la Universidad de Alicante, 2010; 15.
16) HERRERA Enrique, *"Introducción a las telecomunicaciones modernas"*, 1ª Edición, México: Editorial Limusa, 2004; 29-30.
17) HERRERA Enrique, *"Tecnologías y redes de transmisión de datos"*, 1ª Edición, México: Editorial Limusa, 2003; 1-312.
18) HESSELBACH Xavier; ALTES Jordi, *"Análisis de redes y sistemas de comunicaciones",* 1ª edición, Barcelona: Editorial Edicions UPC, 2002; 27-30.
19) http://dgpt.sct.gob.mx/index.php?id=456 (Fecha de última revisión 01-03-2012)
20) http://docs.oracle.com/cd/E21925_01/html/821-3616/giwte.html (Fecha de última revisión 01-03-2012)
21) http://dgpt.sct.gob.mx/index.php?id=456 (Fecha de última revisión 01-03-2012)
22) http://e-ciencia.com/recursos/enciclopedia/Jerarqu%C3%ADa_Digital_Plesiocrona (Fecha de última revisión 01-03-2012)
23) http://es.wikipedia.org/wiki/Anexo:Comparaci%C3%B3n_de_Windows_y_Linux (Fecha de última revisión 01-03-2012)
24) http://geneura.ugr.es/internet/section3_2.html (Fecha de última revisión 01-03-2012)
25) http://ieeestandards.galeon.com/aficiones1573328.html (Fecha de última revisión 01-03-2012)

26) http://java.sun.com/developer/onlineTraining/corba/corba.html (Fecha de última revisión 01-03-2012)
27) http://networkmonitor-info.com/monitoreo-de-red-%C2%BFen-que-consiste/ (Fecha de última revisión 01-03-2012)
28) http://oss.oetiker.ch/mrtg/doc/mrtg.en.html (Fecha de última revisión 01-03-2012)
29) http://profesores.fi-b.unam.mx/heriolg/Organiz3.pdf (Fecha de última revisión 01-03-2012)
30) http://repositorio.bib.upct.es/dspace/bitstream/10317/122/1/pfc2540.pdf (Fecha de última revisión 01-03-2012)
31) http://sx-de-tx.wikispaces.com/DWDM+y+CWDM (Fecha de última revisión 01-03-2012)
32) http://uvirtual.usach.cl/file.php/287/Archivos/Redes05.pdf (Fecha de última revisión 01-03-2012)
33) http://www.ansi.org/about_ansi/overview/overview_sp.aspx?menuid=1 (Fecha de última revisión 01-03-2012)
34) http://www.ansi.org/about_ansi/overview/overview_sp.aspx?menuid=1 (Fecha de última revisión 01-03-2012)
35) http://www.cenapred.unam.mx/es/QuienesSomos/ (Fecha de última revisión 01-03-2012)
36) http://www.channelplanet.com/?idcategoria=18311 (Fecha de última revisión 01-03-2012)
37) http://www.cisco.com/en/US/tech/tk652/tk701/tk419/tsd_technology_support_sub-protocol_home.html (Fecha de última revisión 01-03-2012)
38) http://www.cns.nyu.edu/~fan/sun-docs/st2530-spec/datasheet2530.pdf (Fecha de última revisión 01-03-2012)
39) http://www.diputados.gob.mx/LeyesBiblio/pdf/130.pdf (Fecha de última revisión 01-03-2012)
40) http://www.etsi.org/WebSite/AboutETSI/AboutEtsi.aspx (Fecha de última revisión 01-03-2012)
41) http://www.frm.utn.edu.ar/comunicaciones/redes.html#2 (Fecha de última revisión 01-03-2012)
42) http://www.iso.org/iso/about.htm (Fecha de última revisión 01-03-2012)
43) http://www.microsoft.com/latam/technet/windowsserver/longhorn/evaluate/whitepaper.mspx (Fecha de última revisión 01-03-2012)
44) http://www.oracle.com/us/products/servers-storage/servers/blades/033609.pdf (Fecha de última revisión 01-03-2012)
45) http://www.oracle.com/us/products/servers-storage/servers/blades/033613.pdf (Fecha de última revisión 01-03-2012)
46) http://www.ramonmillan.com/tutoriales/corba.php (Fecha de última revisión 01-03-2012)
47) http://www.rcim.sld.cu/revista_7/articulo_htm/segurinfsalud.htm (Fecha de última revisión 01-03-2012)
48) http://www.redhat.com/products/enterprise-linux/server/ (Fecha de última revisión 01-03-2012)
49) http://www.usbmed.edu.co/Servicios/web/Laboratorios_tecnologicos/Telecomunicaciones.aspx (Fecha de última revisión 01-03-2012)
50) HUIDOBRO José Manuel, *"Redes y servicios de Telecomunicaciones", 4ª Edición,* España: Editorial Paraninfo, 2007; 12-14.
51) HUIDOBRO José Manuel, *"Sistemas telemáticos"*, 3ª Edición, España: Editorial Paraninfo, 2005; 92-135.

52) JAMRICH June; OJA Dan, *"Conceptos de computación, nuevas perspectivas"* 10ª edición, México: Editorial Cengage Learning, 2008; 242.
53) JAVVIN, *"Network Protocols Handbook"*, 2ª Edición, USA: Editorial Javvin Technologies, 2005; 37-44.
54) JEREMIAH O'SULLIVAN-RYAN, "*La comunicación humana: grandes temas contemporáneos de la comunicación",* 3ª edición, Venezuela: Editorial UCAB, 1996; 15.
55) LÓPEZ Jaquelina, QUEZADA Cintia, *"Fundamentos de seguridad informática"*, 1ª Edición, México: Editorial Facultad de Ingeniería, 2006; 1-5, 127-133
56) MACÍAS Ríos María Eugenia, Apuntes "*Administración de redes",* 2010, Facultad de Ingeniería, UNAM.
57) MACÍAS Ríos María Eugenia, Tesis: "*Manual de Prácticas para el Laboratorio de Administración de Redes*", Facultad de Ingeniería, UNAM, CU.
58) MARTÍNEZ P., CABELLO M., *"Sistemas operativos"*, 1ª Edición, Madrid: Editorial Díaz de Santos, 1997:1-24.
59) MILLÁN Tejedor Ramón Jesús, Artículo: *"Tendencias en gestión de red",*publicado en Comunicaciones World nº 189, IDG Communications S.A., 2004.
60) MORERA Juan, PÉREZ Juan, *"Conceptos de sistemas operativos",* 1ª Edición, España: Editorial Comillas, 2002, 1-25.
61) ORTEGA Beatriz, *"Redes ópticas"*, 1ª Edición, Valencia: Editorial Universidad Politécnica de Valencia, 2007; 48-67
62) RAMÍREZ Martínez Carlos Leonel, Tesis: *"Evolución de las tecnologías de núcleo en las redes de telefonía móvil",* Facultad de Ingeniería, USCG, Facultad de Ingeniería, Guatemala.
63) REYES Agustín, *"Administración Moderna",* 1ª Edición, México: Editorial Limusa, 2004; 387-390
64) RODRÍGUEZ Joaquín, *"Introducción a la administración con enfoque de sistemas"*, 4ª Edición, México: Editorial International Thomson Editores, 2003; 318.
65) ROMERO Ma. Del Carmen; BARBANCHO Julio; BENJUMEA Jaime, *"Redes Locales"* , 1ª edición, España: Editorial Paraninfo, 2010; 1-58
66) STAIR Ralph, REYNOLDS George, *"Principios de sistemas de información: enfoque administrativo"*, 4 ª Edicion, México: Editorial International Thomson Editores, 2000; 242-281.
67) STURT Eduard, "*Network management: concepts and tools"*, 1ª Edición, Londres: Editorial Hall and Masson, 1994; 1-19
68) *"Sun Blade 6000 Modular System Service Manual",* Sun Mycrosystems, Inc, Part No. 820-0051-10, Marzo 2007, Revisión A.
69) TANENBAUM Andrew, *"Redes de computadoras",* 4ª Edición, México: Editorial Prentice Hall, 2003; 14-75, 293-300
70) TERÁN David, *"Redes convergentes, Diseño e implementación"*, 1 ª Edición, México: Editorial Alfaomega, 2010; 4-35, 97-107,246-346
71) ZÚÑIGA Medel María Alejandra, Apuntes, "*Redes de Datos",* 2011, Facultad de Ingeniería, UNAM.

ANEXOS

ANEXOS

Anexo 1. Archivo de configuración mrtg1.cfg RHEL

El archivo mrtg1.cfg específica las variables correspondientes a SER1 que serán graficadas.

```
WorkDir: /var/www/html/mrtg
Language: spanish
LoadMIBS:                                                    /usr/share/snmp/mibs/UCD-SNMP
MIB.txt,/usr/share/snmp/mibs/TCP_MIB.txt,/usr/share/snmp/HOST-RESOURCES-MIB.txt

######################################################################
# System: SER1
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 #AT/AT COMPATIBLE - Software:
Windows Version 6.0 (Build 6002 #Multiprocessor Free)
######################################################################

#####Grafica del rendimiento del CPU#####
Target[192.168.1.10_cpu]:       (hrProcessorLoad.2&hrProcessorLoad.2:SER1@192.168.1.10       +
hrProcessorLoad.3&hrProcessorLoad.3:SER1@192.168.1.10                                        +
hrProcessorLoad.4&hrProcessorLoad.4:SER1@192.168.1.10                                        +
hrProcessorLoad.5&hrProcessorLoad.5:SER1@192.168.1.10                                        +
hrProcessorLoad.6&hrProcessorLoad.6:SER1@192.168.1.10                                        +
hrProcessorLoad.7&hrProcessorLoad.7:SER1@192.168.1.10                                        +
hrProcessorLoad.8&hrProcessorLoad.8:SER1@192.168.1.10                                        +
hrProcessorLoad.9&hrProcessorLoad.9:SER1@192.168.1.10) / (8)
MaxBytes[192.168.1.10_cpu]: 100
Title[192.168.1.10_cpu]: Carga CPU--SER1
PageTop[192.168.1.10_cpu]: <H1>Carga Activa CPU %--SER1</H1>
ShortLegend[192.168.1.10_cpu]: %
YLegend[192.168.1.10_cpu]: Utilización del CPU
Legend1[192.168.1.10_cpu]: CPU activa %
LegendI[192.168.1.10_cpu]: Active
LegendO[192.168.1.10_cpu]:
Options[192.168.1.10_cpu]: growright,nopercent,gauge

######Monitoreo de memoria######
Target[192.168.1.10_mem]:          hrStorageUsed.5&hrStorageSize.5:SER1@192.168.1.10         *
hrStorageAllocationUnits.5&hrStorageAllocationUnits.5:SER1@192.168.1.10 * 1000 / 1048576
PageTop[192.168.1.10_mem]: <H1>Memoria libre--SER1</H1>
Options[192.168.1.10_mem]: nopercent,gauge,growright
Title[192.168.1.10_mem]: Memoria libre--SER1
MaxBytes[192.168.1.10_mem]: 100000000000000
YLegend[192.168.1.10_mem]: bytes
ShortLegend[192.168.1.10_mem]: bytes
LegendI[192.168.1.10_mem]: Memoria en uso
LegendO[192.168.1.10_mem]: Memoria total


###Temperatura procesadores#######
Target[192.168.1.1_tem-proc-im]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.124&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.125:SER1@192.168.1.1
PageTop[192.168.1.1_tem-proc-im]: <H1>Temperatura de los procesadores--SER1</H1>
Options[192.168.1.1_tem-proc-im]: gauge,nopercent,growright
Title[192.168.1.1_tem-proc-im]: Temperaturas de procesadores--SER1
MaxBytes[192.168.1.1_tem-proc-im]: 50
LegendI[192.168.1.1_tem-proc-im]: Temperatura del procesador 1
LegendO[192.168.1.1_tem-proc-im]:Temperatura del procesador 2
ShortLegend[192.168.1.1_tem-proc-im]: Â°

### Interface 10 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S   ' |
Name: 'ethernet 6' | Ip: '' | Eth: '00-23-8b-17-a7-34' ###

Target[192.168.1.10_10]: 10:SER1@192.168.1.10:
SetEnv[192.168.1.10_10]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S "
MaxBytes[192.168.1.10_10]: 125000000
Options[192.168.1.10_10]: growright,nopercent
Title[192.168.1.10_10]: Análisis de tráfico eth6 (ID10) -- SER1
PageTop[192.168.1.10_10]: <h1>Análisis de trafico eth6 (ID10) -- SER1</h1>
              <div id="sysdetails">
                     <table>
```

```
                                <tr>
                                        <td>Sistema:</td>
                                        <td>SER1</td>
                                </tr>
                                <tr>
                                        <td>Administrador:</td>
                                        <td>Elizabeth</td>
                                </tr>
                                <tr>
                                        <td>Descripcion:</td>
                                        <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S  </td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>Ethernet 6</td>
                                </tr>
                                <tr>
                                        <td>Velocidad Maxima:</td>
                                        <td>125.0 MBytes/s</td>
                                </tr>
                        </table>
                </div>


### Interface 11 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S -#2' |
Name: 'ethernet 8' | Ip: '' | Eth: '00-23-8b-17-a7-35' ###

Target[192.168.1.10_11]: 11:SER1@192.168.1.10:
SetEnv[192.168.1.10_11]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S -#2"
Options[192.168.1.10_11]: growright,nopercent
MaxBytes[192.168.1.10_11]: 125000000
Title[192.168.1.10_11]: Análisis de trafico de eth8 (ID11) -- SER1
PageTop[192.168.1.10_11]: <h1>Análisis de trafico de eth8 (ID11) -- SER1</h1>
                <div id="sysdetails">
                        <table>
                                <tr>
                                        <td>Sistema:</td>
                                        <td>SER1</td>
                                </tr>
                                <tr>
                                        <td>Administrador:</td>
                                        <td>Elizabeth</td>
                                </tr>
                                <tr>
                                        <td>Descripción:</td>
                                        <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S -#2  </td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>Ethernet 8</td>
                                </tr>
                                <tr>
                                        <td>Velocidad Maxima:</td>
                                        <td>125.0 MBytes/s</td>
                                </tr>
                        </table>
                </div>


### Interface 12 >> Descr: 'Puente MAC' | Name: 'ethernet_10' | Ip: '192.168.1.10' | Eth: ''
###

Target[192.168.1.10_12]: 12:SER1@192.168.1.10:
SetEnv[192.168.1.10_12]: MRTG_INT_IP="192.168.1.10" MRTG_INT_DESCR="Puente MAC"
MaxBytes[192.168.1.10_12]: 125000000
Options[192.168.1.10_12]: growright,nopercent
```

```
Title[192.168.1.10_12]: Análisis de trafico eth10 (ID12) -- SER1
PageTop[192.168.1.10_12]: <h1>Análisis de tráfico (ID12) -- SER1</h1>
              <div id="sysdetails">
                     <table>
                            <tr>
                                   <td>Sistema:</td>
                                   <td>SER1</td>
                            </tr>
                            <tr>
                                   <td>Administrador:</td>
                                   <td>Elizabeth</td>
                            </tr>
                            <tr>
                                   <td>Descripcion:</td>
                                   <td>Puente MAC  </td>
                            </tr>
                            <tr>
                                   <td>Tipo de interfaz:</td>
                                   <td>ethernetCsmacd (6)</td>
                            </tr>
                            <tr>
                                   <td>Nombre de interfaz:</td>
                                   <td>ethernet_10</td>
                            </tr>
                            <tr>
                                   <td>Velocidad Maxima:</td>
                                   <td>125.0 MBytes/s</td>
                            </tr>
                            <tr>
                                   <td>Ip:</td>
                                   <td>192.168.1.10 ()</td>
                            </tr>
                     </table>
              </div>
```

Anexo 2. Archivo de configuración mrtg2.cfg RHEL

El archivo de configuración mrtg2.cfg es ligeramente diferente a los demás archivos, debido a que es el único sistema Linux dentro del Sun Blade. La estructura de dicho archivo es la siguiente:

```
WorkDir: /var/www/html/mrtg
Language: spanish
LoadMIBS:                                                              /usr/share/snmp/mibs/UCD-SNMP
MIB.txt,/usr/share/snmp/mibs/TCP_MIB.txt,/usr/share/snmp/HOST-RESOURCES-MIB.txt

######################################################################
# System: SER2
# Description: Linux SER2 2.6.18-53.el5xen #1 SMP Wed Oct 10 #17:06:12 EDT 2007 i686
######################################################################

#####Grafica del rendimiento del CPU#####
Target[192.168.1.11_cpu]: (hrProcessorLoad.768&hrProcessorLoad.768:SER2@192.168.1.11 +
hrProcessorLoad.769&hrProcessorLoad.769:SER2@192.168.1.11 +
hrProcessorLoad.770&hrProcessorLoad.770:SER2@192.168.1.11 +
hrProcessorLoad.771&hrProcessorLoad.771:SER2@192.168.1.11 +
hrProcessorLoad.772&hrProcessorLoad.772:SER2@192.168.1.11 +
hrProcessorLoad.773&hrProcessorLoad.773:SER2@192.168.1.11 +
hrProcessorLoad.774&hrProcessorLoad.774:SER2@192.168.1.11 +
hrProcessorLoad.775&hrProcessorLoad.775:SER2@192.168.1.11) / (8)
MaxBytes[192.168.1.11_cpu]: 100
Title[192.168.1.11_cpu]: Carga CPU--SER2
PageTop[192.168.1.11_cpu]: <H1>Carga Activa CPU %--SER2</H1>
ShortLegend[192.168.1.11_cpu]: %
YLegend[192.168.1.11_cpu]: Utilizacion del CPU
Legend1[192.168.1.11_cpu]: CPU activa %
LegendI[192.168.1.11_cpu]: Active
LegendO[192.168.1.11_cpu]:
Options[192.168.1.11_cpu]: growright,nopercent,gauge


######Monitoreo de memoria######
Target[192.168.1.11_mem]: hrStorageUsed.2&hrStorageSize.2:SER2@192.168.1.11 *
hrStorageAllocationUnits.2&hrStorageAllocationUnits.2:SER2@192.168.1.11 * 1000/ 1048576
PageTop[192.168.1.11_mem]: <H1>Memoria libre--SER2</H1>
```

```
Options[192.168.1.11_mem]: nopercent,gauge,growright
Title[192.168.1.11_mem]: Memoria libre--SER2
MaxBytes[192.168.1.11_mem]: 100000000000000
YLegend[192.168.1.11_mem]: bytes
ShortLegend[192.168.1.11_mem]: bytes
LegendI[192.168.1.11_mem]: Memoria en uso
LegendO[192.168.1.11_mem]: Memoria total
Legend1[192.168.1.11_mem]: Memoria en uso, no incluye swap, en bytes

###Temperatura procesadores#######
Target[192.168.1.2_tem-proc-at]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.124&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.125:SER2@192.168.1.2
PageTop[192.168.1.2_tem-proc-at]: <H1>Temperatura de los procesadores--SER2</H1>
Options[192.168.1.2_tem-proc-at]: gauge,nopercent,growright
Title[192.168.1.2_tem-proc-at]: Temperaturas de procesadores--SER2
MaxBytes[192.168.1.2_tem-proc-at]: 50
LegendI[192.168.1.2_tem-proc-at]: Temperatura del procesador 1
LegendO[192.168.1.2_tem-proc-at]:Temperatura del procesador 2
ShortLegend[192.168.1.2_tem-proc-at]: Â°

### Interface 3 >> Descr: 'eth1' | Name: 'eth1' | Ip: '' | Eth: '' ###

Target[192.168.1.11_3]: 3:SER2@192.168.1.11:
SetEnv[192.168.1.11_3]: MRTG_INT_IP="" MRTG_INT_DESCR="eth1"
Options[192.168.1.11_3]: growright,nopercent
MaxBytes[192.168.1.11_3]: 125000000
Title[192.168.1.11_3]: Análisis de trafico eth1 SER2
PageTop[192.168.1.11_3]: <h1>Análisis de trafico eth1 -- SER2</h1>
               <div id="sysdetails">
                       <table>
                               <tr>
                                       <td>Sistema:</td>
                                       <td>SER2</td>
                               </tr>
                               <tr>
                                       <td>Administrador:</td>
                                       <td>Elizabeth; (configure /etc/snmp/snmp.local.conf)</td>
                               </tr>
                               <tr>
                                       <td>Descripcion:</td>
                                       <td>eth1  </td>
                               </tr>
                               <tr>
                                       <td>Tipo de interfaz:</td>
                                       <td>ethernetCsmacd (6)</td>
                               </tr>
                               <tr>
                                       <td>Mombre de la interfaz:</td>
                                       <td>eth1</td>
                               </tr>
                               <tr>
                                       <td>Velocidad Maxima:</td>
                                       <td>125.0 MBytes/s</td>
                               </tr>
                       </table>
               </div>

### Interface 5 >> Descr: 'bond0' | Name: 'bond0' | Ip: '192.168.1.11' | Eth: '' ###

Target[192.168.1.11_5]: 5:SER2@192.168.1.11:
SetEnv[192.168.1.11_5]: MRTG_INT_IP="192.168.1.11" MRTG_INT_DESCR="bond0"
Options[192.168.1.11_5]: growright,nopercent
MaxBytes[192.168.1.11_5]: 1250000
Title[192.168.1.11_5]: Análisis de trafico bond0 -- SER2
PageTop[192.168.1.11_5]: <h1>Análisis de trafico bond0 -- SER2</h1>
               <div id="sysdetails">
                       <table>
                               <tr>
                                       <td>Sistema:</td>
                                       <td>SER2</td>
                               </tr>
                               <tr>
                                       <td>Administrador:</td>
                                       <td>Elizabeth</td>
                               </tr>
                               <tr>
                                       <td>Descripcion:</td>
```

```
                                <td>bond0  </td>
                        </tr>
                        <tr>
                                <td>Tipo de interfaz:</td>
                                <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                                <td>Nombre de interfaz:</td>
                                <td>bond0</td>
                        </tr>
                        <tr>
                                <td>Velocidad Maxima:</td>
                                <td>1250.0 kBytes/s</td>
                        </tr>
                        <tr>
                                <td>Ip:</td>
                                <td>192.168.1.11 (www.SER2nacionalderiesgos.gob.mx)</td>
                        </tr>
                </table>
        </div>

### Interface 8 >> Descr: 'eth0' | Name: 'eth0' | Ip: '' | Eth: '' ###

Target[192.168.1.11_8]: 8:SER2@192.168.1.11:
SetEnv[192.168.1.11_8]: MRTG_INT_IP="" MRTG_INT_DESCR="eth0"
Options[192.168.1.11_8]: growright,nopercent
MaxBytes[192.168.1.11_8]: 1250000
Title[192.168.1.11_8]: Análisis de trafico de th0 -- SER2
PageTop[192.168.1.11_8]: <h1>Análisis de trafico de th0 -- SER2</h1>
        <div id="sysdetails">
                <table>
                        <tr>
                                <td>Sistema:</td>
                                <td>SER2</td>
                        </tr>
                        <tr>
                                <td>Administradorr:</td>
                                <td>Elizabeth</td>
                        </tr>
                        <tr>
                                <td>Descripcion:</td>
                                <td>eth0  </td>
                        </tr>
                        <tr>
                                <td>Tipo de interfaz:</td>
                                <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                                <td>Nombre de interfaz:</td>
                                <td>eth0</td>
                        </tr>
                        <tr>
                                <td>Velocidad Maxima:</td>
                                <td>1250.0 kBytes/s</td>
                        </tr>
                </table>
        </div>
```

Anexo 3. Archivo de configuración mrtg3.cfg RHEL

El archivo de configuración mrtg3.cfg corresponde a las variables de SER3 y su sintaxis es la siguiente.

```
WorkDir: /var/www/html/mrtg
Language: spanish
LoadMIBS:                                                       /usr/share/snmp/mibs/UCD-SNMP
MIB.txt,/usr/share/snmp/mibs/TCP_MIB.txt,/usr/share/snmp/HOST-RESOURCES-MIB.txt

######################################################################
#System: SER3
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 AT/AT COMPATIBLE - Software:
Windows Version 6.0 (Build 6002 Multiprocessor Free)
######################################################################
```

```
#####Grafica del rendimiento del CPU#####
Target[192.168.1.12_cpu]: (hrProcessorLoad.2&hrProcessorLoad.2:SER3@192.168.1.12 +
hrProcessorLoad.3&hrProcessorLoad.3:SER3@192.168.1.12 +
hrProcessorLoad.4&hrProcessorLoad.4:SER3@192.168.1.12 +
hrProcessorLoad.5&hrProcessorLoad.5:SER3@192.168.1.12 +
hrProcessorLoad.6&hrProcessorLoad.6:SER3@192.168.1.12 +
hrProcessorLoad.7&hrProcessorLoad.7:SER3@192.168.1.12 +
hrProcessorLoad.8&hrProcessorLoad.8:SER3@192.168.1.12 +
hrProcessorLoad.9&hrProcessorLoad.9:SER3@192.168.1.12) / (8)
MaxBytes[192.168.1.12_cpu]: 100
Title[192.168.1.12_cpu]: Carga CPU--SER3
PageTop[192.168.1.12_cpu]: <H1>Carga Activa CPU %--SER3</H1>
ShortLegend[192.168.1.12_cpu]: %
YLegend[192.168.1.12_cpu]: Utilizacion del CPU
Legend1[192.168.1.12_cpu]: CPU activa %
LegendI[192.168.1.12_cpu]: Active
LegendO[192.168.1.12_cpu]:
Options[192.168.1.12_cpu]: growright,nopercent,gauge

######Monitoreo de memoria######
Target[192.168.1.12_mem]: hrStorageUsed.7&hrStorageSize.7:SER3@192.168.1.12 *
hrStorageAllocationUnits.7&hrStorageAllocationUnits.7:SER3@192.168.1.12 * 1000 / 1048576
PageTop[192.168.1.12_mem]: <H1>Memoria libre--SER3</H1>
Options[192.168.1.12_mem]: nopercent,gauge,growright
Title[192.168.1.12_mem]: Memoria libre--SER3
MaxBytes[192.168.1.12_mem]: 100000000000000
YLegend[192.168.1.12_mem]: bytes
ShortLegend[192.168.1.12_mem]: bytes
LegendI[192.168.1.12_mem]: Memoria en uso
LegendO[192.168.1.12_mem]: Memoria total


###Temperatura procesadores#######
Target[192.168.1.3_tem-proc-in]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.100&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.101:SER3@192.168.1.3
PageTop[192.168.1.3_tem-proc-in]: <H1>Temperatura de los procesadores--SER3</H1>
Options[192.168.1.3_tem-proc-in]: gauge,nopercent,growright
Title[192.168.1.3_tem-proc-in]: Temperaturas de procesadores--SER3
MaxBytes[192.168.1.3_tem-proc-in]: 50
LegendI[192.168.1.3_tem-proc-in]: Temperatura del procesador 1
LegendO[192.168.1.3_tem-proc-in]:Temperatura del procesador 2
ShortLegend[192.168.1.3_tem-proc-in]: Â°

###Interface 10 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S
Aceleracion' | Name: 'ethernet_6' | Ip: '' | Eth: '00-1e-68-57-71-be' ###

Target[192.168.1.12_10]: 10:SER3@192.168.1.12:
SetEnv[192.168.1.12_10]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S "
Options[192.168.1.12_10]: growright,nopercent
MaxBytes[192.168.1.12_10]: 125000000
Title[192.168.1.12_10]: Análisis de trafico eth6 (ID10) -- SER3
PageTop[192.168.1.12_10]: <h1>Análisis de trafico eth6 (ID10) -- SER3</h1>
     <div id="sysdetails">
     <table>
           <tr>
               <td>Sistema:</td>
               <td>SER3</td>
           </tr>
           <tr>
               <td>Administrador:</td>
               <td>Elizabeth</td>
           </tr>
           <tr>
               <td>Descripcion:</td>
               <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S </td>
           </tr>
           <tr>
               <td>Tipo de interfaz:</td>
               <td>ethernetCsmacd (6)</td>
           </tr>
           <tr>
               <td>Nombre de interfaz:</td>
                <td>ethernet_6</td>
            </tr>
            <tr>
```

```
                <td>Velocidad Maxima:</td>
                <td>125.0 MBytes/s</td>
            </tr>
        </table>
        </div>


### Interface 11 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S -#2' |
Name: 'ethernet_8' | Ip: '' | Eth: '00-1e-68-57-71-bf' ###

Target[192.168.1.12_11]: 11:SER3@192.168.1.12:
SetEnv[192.168.1.12_11]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S -#2"
Options[192.168.1.12_11]: growright,nopercent
MaxBytes[192.168.1.12_11]: 125000000
Title[192.168.1.12_11]: Análisis de trafico eth8 (ID11) -- SER3
PageTop[192.168.1.12_11]: <h1>Análisis de trafico eth8 (ID11) -- SER3</h1>
     <div id="sysdetails">
          <table>
                <tr>
                    <td>Sistema:</td>
                    <td>SER3</td>
                </tr>
                <tr>
                    <td>Administrador:</td>
                    <td>Elizabeth</td>
                </tr>
                <tr>
                     <td>Descripcion:</td>
                     <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S -#2  </td>
                </tr>
                <tr>
                      <td>Tipo de interfaz:</td>
                      <td>ethernetCsmacd (6)</td>
                </tr>
                <tr>
                      <td>Nombre de interfaz:</td>
                      <td>Ethernet 8</td>
                </tr>
                <tr>
                      <td>Velocidad Maxima:</td>
                      <td>125.0 MBytes/s</td>
                </tr>
          </table>
        </div>

### Interface 12 >> Descr: 'Puente MAC' | Name: 'ethernet_10' | Ip: '192.168.1.12' | Eth: ''
###

Target[192.168.1.12_12]: 12:SER3@192.168.1.12:
SetEnv[192.168.1.12_12]: MRTG_INT_IP="192.168.1.12" MRTG_INT_DESCR="Puente MAC"
Options[192.168.1.12_12]: growright,nopercent
MaxBytes[192.168.1.12_12]: 125000000
Title[192.168.1.12_12]: Análisis de trafico eth10 (ID12) -- SER3
PageTop[192.168.1.12_12]: <h1>Análisis de trafico eth10 (ID12) -- SER3</h1>
        <div id="sysdetails">
             <table>
                   <tr>
                       <td>Sistema:</td>
                       <td>SER3</td>
                   </tr>
                   <tr>
                       <td>Administrador:</td>
                       <td>Elizabeth</td>
                   </tr>
                   <tr>
                       <td>Descripcion:</td>
                       <td>Puente MAC </td>
                   </tr>
                   <tr>
                       <td>Tipo de interfaz:</td>
                       <td>ethernetCsmacd (6)</td>
                   </tr>
                   <tr>
                       <td>Nombre de interfaz:</td>
                       <td>Ethernet 10</td>
                   </tr>
```

```
                <tr>
                    <td>Velocidad maxima:</td>
                    <td>125.0 MBytes/s</td>
                </tr>
                <tr>
                     <td>Ip:</td>
                     <td>192.168.1.12 ()</td>
                </tr>
            </table>
        </div>
```

Anexo 4. Archivo de configuración mrtg4.cfg RHEL

SER4 también cuenta con su propio archivo de configuración, el cual lleva el nombre de mrt4.cfg, en él se definen las variables y sus características para cuando sean graficadas. Su contenido es el siguiente.

```
WorkDir: /var/www/html/mrtg
Language: spanish
LoadMIBS:                                                          /usr/share/snmp/mibs/UCD-SNMP
MIB.txt,/usr/share/snmp/mibs/TCP_MIB.txt,/usr/share/snmp/HOST-RESOURCES-MIB.txt


######################################################################
# System: SER4
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 #AT/AT COMPATIBLE - Software:
Windows Version 6.0 (Build 6002 #Multiprocessor Free)
######################################################################


#####Grafica del rendimiento del CPU#####
Target[192.168.1.13_cpu]: (hrProcessorLoad.2&hrProcessorLoad.2:SER4@192.168.1.13 +
hrProcessorLoad.3&hrProcessorLoad.3:SER4@192.168.1.13 +
hrProcessorLoad.4&hrProcessorLoad.4:SER4@192.168.1.13 +
hrProcessorLoad.5&hrProcessorLoad.5:SER4@192.168.1.13 +
hrProcessorLoad.6&hrProcessorLoad.6:SER4@192.168.1.13 +
hrProcessorLoad.7&hrProcessorLoad.7:SER4@192.168.1.13 +
hrProcessorLoad.8&hrProcessorLoad.8:SER4@192.168.1.13 +
hrProcessorLoad.9&hrProcessorLoad.9:SER4@192.168.1.13) / (8)
MaxBytes[192.168.1.13_cpu]: 100
Title[192.168.1.13_cpu]: Carga CPU--SER4
PageTop[192.168.1.13_cpu]: <H1>Carga Activa CPU %--SER4</H1>
ShortLegend[192.168.1.13_cpu]: %
YLegend[192.168.1.13_cpu]: Utilizacion del CPU
Legend1[192.168.1.13_cpu]: CPU activa %
LegendI[192.168.1.13_cpu]: Active
LegendO[192.168.1.13_cpu]:
Options[192.168.1.13_cpu]: growright,nopercent,gauge

######Monitoreo de memoria######
Target[192.168.1.13_mem]: hrStorageUsed.5&hrStorageSize.5:SER4@192.168.1.13 *
hrStorageAllocationUnits.5&hrStorageAllocationUnits.5:SER4@192.168.1.13 * 1000 / 1048576
PageTop[192.168.1.13_mem]: <H1>Memoria libre--SER4</H1>
Options[192.168.1.13_mem]: nopercent,gauge,growright
Title[192.168.1.13_mem]: Memoria libre--SER4
MaxBytes[192.168.1.13_mem]: 100000000000000
YLegend[192.168.1.13_mem]: bytes
ShortLegend[192.168.1.13_mem]: bytes
LegendI[192.168.1.13_mem]: Memoria en uso
LegendO[192.168.1.13_mem]: Memoria total
Legend1[192.168.1.13_mem]: Memoria en uso, no incluye swap, en bytes

#####Trafico web de SER4############
Target[192.168.1.13_web]:
1.3.6.1.4.1.311.1.7.3.1.2.0&1.3.6.1.4.1.311.1.7.3.1.4.0:SER4@192.168.1.13
PageTop[192.168.1.13_web]: <H1>Trafico web--SER4</H1>
Options[192.168.1.13_web]: growright,nopercent
Title[192.168.1.13_web]: Trafico web--SER4
MaxBytes[192.168.1.13_web]: 125000000

###Temperatura procesador 1#######
Target[192.168.1.4_tem-proc-1]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.136&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.137:SER4@192.168.1.4
```

```
PageTop[192.168.1.4_tem-proc-1]: <H1>Temperatura de los procesadores--SER4</H1>
Options[192.168.1.4_tem-proc-1]: gauge,nopercent,growright
Title[192.168.1.4_tem-proc-1]: Temperaturas de procesadores--SER4
MaxBytes[192.168.1.4_tem-proc-1]: 50
LegendI[192.168.1.4_tem-proc-1]: Temperatura del procesador 1
LegendO[192.168.1.4_tem-proc-1]:Temperatura del procesador 2
ShortLegend[192.168.1.4_tem-proc-1]: Â°


### Interface 11 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S' | Name:
'ethernet 6' | Ip: '' | Eth: '00-26-9e-9b-f6-78' ###

Target[192.168.1.13_11]: 11:SER4@192.168.1.13:
SetEnv[192.168.1.13_11]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S"
Options[192.168.1.13_11]: growright,nopercent
MaxBytes[192.168.1.13_11]: 125000000
Title[192.168.1.13_11]: Analisis de trafico eth6 (ID11) -- SER4
PageTop[192.168.1.13_11]: <h1>Analisis de trafico eth6 (ID11) -- SER4</h1>
               <div id="sysdetails">
                       <table>
                               <tr>
                                       <td>Sistema:</td>
                                       <td>SER4</td>
                               </tr>
                               <tr>
                                       <td>Administrador:</td>
                                       <td>CENAPRED</td>
                               </tr>
                               <tr>
                                       <td>Descripcion:</td>
                                       <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S  </td>
                               </tr>
                               <tr>
                                       <td>Tipo de interfaz:</td>
                                       <td>ethernetCsmacd (6)</td>
                               </tr>
                               <tr>
                                       <td>Nombre de interfaz:</td>
                                       <td>Ethernet 6</td>
                               </tr>
                               <tr>
                                       <td>Velocidad maxima:</td>
                                       <td>125.0 MBytes/s</td>
                               </tr>
                       </table>
               </div>


### Interface 12 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S  -#2' |
Name: 'ethernet_8' | Ip: '' | Eth: '00-26-9e-9b-f6-79' ###

Target[192.168.1.13_12]: 12:SER4@192.168.1.13:
SetEnv[192.168.1.13_12]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S  -#2"
Options[192.168.1.13_12]: growright,nopercent
MaxBytes[192.168.1.13_12]: 125000000
Title[192.168.1.13_12]: Analisis de trafico eth8 (ID12) -- SER4
PageTop[192.168.1.13_12]: <h1>Analisis de trafico eth8 (ID12) -- SER4</h1>
               <div id="sysdetails">
                       <table>
                               <tr>
                                       <td>Sistema:</td>
                                       <td>SER4</td>
                               </tr>
                               <tr>
                                       <td>Administrador:</td>
                                       <td>CENAPRED</td>
                               </tr>
                               <tr>
                                       <td>Descripcion:</td>
                                       <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S  -#2  </td>
                               </tr>
                               <tr>
                                       <td>Tipo de interfaz:</td>
```

```
                                <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                                <td>Nombre de interfaz:</td>
                                <td>Ethernet 8</td>
                        </tr>
                        <tr>
                                <td>Velocidad maxima:</td>
                                <td>125.0 MBytes/s</td>
                        </tr>
                </table>
        </div>


### Interface 13 >> Descr: 'Puente MAC' | Name: 'ethernet_10' | Ip: '192.168.1.13' | Eth: ''
###

Target[192.168.1.13_13]: 13:SER4@192.168.1.13:
SetEnv[192.168.1.13_13]: MRTG_INT_IP="192.168.1.13" MRTG_INT_DESCR="Puente MAC"
Options[192.168.1.13_13]: growright,nopercent
MaxBytes[192.168.1.13_13]: 125000000
Title[192.168.1.13_13]: Analisis de trafico eth10 (ID13) -- SER4
PageTop[192.168.1.13_13]: <h1>Analisis de trafico eth10 (ID13)-- SER4</h1>
        <div id="sysdetails">
                <table>
                        <tr>
                                <td>Sistema:</td>
                                <td>SER4</td>
                        </tr>
                        <tr>
                                <td>Administrador:</td>
                                <td>CENAPRED</td>
                        </tr>
                        <tr>
                                <td>Descripcion:</td>
                                <td>Puente MAC</td>
                        </tr>
                        <tr>
                                <td>Tipo de interfaz:</td>
                                <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                                <td>Nombre de interfaz:</td>
                                <td>Ethernet 10</td>
                        </tr>
                        <tr>
                                <td>Velocidad maxima:</td>
                                <td>125.0 MBytes/s</td>
                        </tr>
                        <tr>
                                <td>Ip:</td>
                                <td>192.168.1.13 ()</td>
                        </tr>
                </table>
        </div>
```

Anexo 5. Archivo de configuración mrtg.cfg RHEL

Este archivo es sobre el que MRTG se basará para la creación de las gráficas, el almacenamiento de los datos y las consultas. Cada variable que se decida monitorear deberá ser declarada en este archivo. El contenido de este archivo es el siguiente:

```
WorkDir: /var/www/html/mrtg
Language: spanish
LoadMIBS:                                                       /usr/share/snmp/mibs/UCD-SNMP
MIB.txt,/usr/share/snmp/mibs/TCP_MIB.txt,/usr/share/snmp/HOST-RESOURCES-MIB.txt

######################################################################
# System: SER1
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 #AT/AT COMPATIBLE - Software:
Windows Version 6.0 (Build 6002 #Multiprocessor Free)
######################################################################

#####Grafica del rendimiento del CPU#####
Target[192.168.1.10_cpu]:       (hrProcessorLoad.2&hrProcessorLoad.2:SER1@192.168.1.10       +
hrProcessorLoad.3&hrProcessorLoad.3:SER1@192.168.1.10                                        +
```

```
hrProcessorLoad.4&hrProcessorLoad.4:SER1@192.168.1.10                                    +
hrProcessorLoad.5&hrProcessorLoad.5:SER1@192.168.1.10                                    +
hrProcessorLoad.6&hrProcessorLoad.6:SER1@192.168.1.10                                    +
hrProcessorLoad.7&hrProcessorLoad.7:SER1@192.168.1.10                                    +
hrProcessorLoad.8&hrProcessorLoad.8:SER1@192.168.1.10                                    +
hrProcessorLoad.9&hrProcessorLoad.9:SER1@192.168.1.10) / (8)
MaxBytes[192.168.1.10_cpu]: 100
Title[192.168.1.10_cpu]: Carga CPU--SER1
PageTop[192.168.1.10_cpu]: <H1>Carga Activa CPU %--SER1</H1>
ShortLegend[192.168.1.10_cpu]: %
YLegend[192.168.1.10_cpu]: Utilización del CPU
Legend1[192.168.1.10_cpu]: CPU activa %
LegendI[192.168.1.10_cpu]: Active
LegendO[192.168.1.10_cpu]:
Options[192.168.1.10_cpu]: growright,nopercent,gauge

######Monitoreo de memoria######
Target[192.168.1.10_mem]:          hrStorageUsed.5&hrStorageSize.5:SER1@192.168.1.10         *
hrStorageAllocationUnits.5&hrStorageAllocationUnits.5:SER1@192.168.1.10 * 1000 / 1048576
PageTop[192.168.1.10_mem]: <H1>Memoria libre--SER1</H1>
Options[192.168.1.10_mem]: nopercent,gauge,growright
Title[192.168.1.10_mem]: Memoria libre--SER1
MaxBytes[192.168.1.10_mem]: 100000000000000
YLegend[192.168.1.10_mem]: bytes
ShortLegend[192.168.1.10_mem]: bytes
LegendI[192.168.1.10_mem]: Memoria en uso
LegendO[192.168.1.10_mem]: Memoria total


###Temperatura procesadores#######
Target[192.168.1.1_tem-proc-im]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.124&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.125:SER1@192.168.1.1
PageTop[192.168.1.1_tem-proc-im]: <H1>Temperatura de los procesadores--SER1</H1>
Options[192.168.1.1_tem-proc-im]: gauge,nopercent,growright
Title[192.168.1.1_tem-proc-im]: Temperaturas de procesadores--SER1
MaxBytes[192.168.1.1_tem-proc-im]: 50
LegendI[192.168.1.1_tem-proc-im]: Temperatura del procesador 1
LegendO[192.168.1.1_tem-proc-im]:Temperatura del procesador 2
ShortLegend[192.168.1.1_tem-proc-im]: Â°

### Interface 10 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S   ' |
Name: 'ethernet 6' | Ip: '' | Eth: '00-23-8b-17-a7-34' ###

Target[192.168.1.10_10]: 10:SER1@192.168.1.10:
SetEnv[192.168.1.10_10]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S "
MaxBytes[192.168.1.10_10]: 125000000
Options[192.168.1.10_10]: growright,nopercent
Title[192.168.1.10_10]: Análisis de tráfico eth6 (ID10) -- SER1
PageTop[192.168.1.10_10]: <h1>Análisis de trafico eth6 (ID10) -- SER1</h1>
              <div id="sysdetails">
                     <table>
                            <tr>
                                   <td>Sistema:</td>
                                   <td>SER1</td>
                            </tr>
                            <tr>
                                   <td>Administrador:</td>
                                   <td>Elizabeth</td>
                            </tr>
                            <tr>
                                   <td>Descripcion:</td>
                                   <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S  </td>
                            </tr>
                            <tr>
                                   <td>Tipo de interfaz:</td>
                                   <td>ethernetCsmacd (6)</td>
                            </tr>
                            <tr>
                                   <td>Nombre de interfaz:</td>
                                   <td>Ethernet 6</td>
                            </tr>
                            <tr>
                                   <td>Velocidad Maxima:</td>
                                   <td>125.0 MBytes/s</td>
                            </tr>
```

```
                </table>
        </div>


### Interface 11 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S -#2' |
Name: 'ethernet 8' | Ip: '' | Eth: '00-23-8b-17-a7-35' ###

Target[192.168.1.10_11]: 11:SER1@192.168.1.10:
SetEnv[192.168.1.10_11]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S -#2"
Options[192.168.1.10_11]: growright,nopercent
MaxBytes[192.168.1.10_11]: 125000000
Title[192.168.1.10_11]: Análisis de trafico de eth8 (ID11) -- SER1
PageTop[192.168.1.10_11]: <h1>Análisis de trafico de eth8 (ID11) -- SER1</h1>
        <div id="sysdetails">
                <table>
                        <tr>
                                <td>Sistema:</td>
                                <td>SER1</td>
                        </tr>
                        <tr>
                                <td>Administrador:</td>
                                <td>Elizabeth</td>
                        </tr>
                        <tr>
                                <td>Descripción:</td>
                                <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S -#2  </td>
                        </tr>
                        <tr>
                                <td>Tipo de interfaz:</td>
                                <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                                <td>Nombre de interfaz:</td>
                                <td>Ethernet 8</td>
                        </tr>
                        <tr>
                                <td>Velocidad Maxima:</td>
                                <td>125.0 MBytes/s</td>
                        </tr>
                </table>
        </div>


### Interface 12 >> Descr: 'Puente MAC' | Name: 'ethernet_10' | Ip: '192.168.1.10' | Eth: ''
###

Target[192.168.1.10_12]: 12:SER1@192.168.1.10:
SetEnv[192.168.1.10_12]: MRTG_INT_IP="192.168.1.10" MRTG_INT_DESCR="Puente MAC"
MaxBytes[192.168.1.10_12]: 125000000
Options[192.168.1.10_12]: growright,nopercent
Title[192.168.1.10_12]: Análisis de trafico eth10 (ID12) -- SER1
PageTop[192.168.1.10_12]: <h1>Análisis de tráfico (ID12) -- SER1</h1>
        <div id="sysdetails">
                <table>
                        <tr>
                                <td>Sistema:</td>
                                <td>SER1</td>
                        </tr>
                        <tr>
                                <td>Administrador:</td>
                                <td>Elizabeth</td>
                        </tr>
                        <tr>
                                <td>Descripcion:</td>
                                <td>Puente MAC  </td>
                        </tr>
                        <tr>
                                <td>Tipo de interfaz:</td>
                                <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                                <td>Nombre de interfaz:</td>
                                <td>ethernet_10</td>
                        </tr>
                        <tr>
```

```
                                <td>Velocidad Maxima:</td>
                                <td>125.0 MBytes/s</td>
                        </tr>
                        <tr>
                                <td>Ip:</td>
                                <td>192.168.1.10 ()</td>
                        </tr>
                </table>
        </div>

######################################################################
# System: SER2
# Description: Linux SER2 2.6.18-53.el5xen #1 SMP Wed Oct 10 #17:06:12 EDT 2007 i686
######################################################################

#####Grafica del rendimiento del CPU#####
Target[192.168.1.11_cpu]: (hrProcessorLoad.768&hrProcessorLoad.768:SER2@192.168.1.11 +
hrProcessorLoad.769&hrProcessorLoad.769:SER2@192.168.1.11 +
hrProcessorLoad.770&hrProcessorLoad.770:SER2@192.168.1.11 +
hrProcessorLoad.771&hrProcessorLoad.771:SER2@192.168.1.11 +
hrProcessorLoad.772&hrProcessorLoad.772:SER2@192.168.1.11 +
hrProcessorLoad.773&hrProcessorLoad.773:SER2@192.168.1.11 +
hrProcessorLoad.774&hrProcessorLoad.774:SER2@192.168.1.11 +
hrProcessorLoad.775&hrProcessorLoad.775:SER2@192.168.1.11) / (8)
MaxBytes[192.168.1.11_cpu]: 100
Title[192.168.1.11_cpu]: Carga CPU--SER2
PageTop[192.168.1.11_cpu]: <H1>Carga Activa CPU %--SER2</H1>
ShortLegend[192.168.1.11_cpu]: %
YLegend[192.168.1.11_cpu]: Utilizacion del CPU
Legend1[192.168.1.11_cpu]: CPU activa %
LegendI[192.168.1.11_cpu]: Active
LegendO[192.168.1.11_cpu]:
Options[192.168.1.11_cpu]: growright,nopercent,gauge


######Monitoreo de memoria######
Target[192.168.1.11_mem]: hrStorageUsed.2&hrStorageSize.2:SER2@192.168.1.11 *
hrStorageAllocationUnits.2&hrStorageAllocationUnits.2:SER2@192.168.1.11 * 1000/ 1048576
PageTop[192.168.1.11_mem]: <H1>Memoria libre--SER2</H1>
Options[192.168.1.11_mem]: nopercent,gauge,growright
Title[192.168.1.11_mem]: Memoria libre--SER2
MaxBytes[192.168.1.11_mem]: 100000000000000
YLegend[192.168.1.11_mem]: bytes
ShortLegend[192.168.1.11_mem]: bytes
LegendI[192.168.1.11_mem]: Memoria en uso
LegendO[192.168.1.11_mem]: Memoria total
Legend1[192.168.1.11_mem]: Memoria en uso, no incluye swap, en bytes

###Temperatura procesadores#######
Target[192.168.1.2_tem-proc-at]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.124&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.125:SER2@192.168.1.2
PageTop[192.168.1.2_tem-proc-at]: <H1>Temperatura de los procesadores--SER2</H1>
Options[192.168.1.2_tem-proc-at]: gauge,nopercent,growright
Title[192.168.1.2_tem-proc-at]: Temperaturas de procesadores--SER2
MaxBytes[192.168.1.2_tem-proc-at]: 50
LegendI[192.168.1.2_tem-proc-at]: Temperatura del procesador 1
LegendO[192.168.1.2_tem-proc-at]:Temperatura del procesador 2
ShortLegend[192.168.1.2_tem-proc-at]: Â°

### Interface 3 >> Descr: 'eth1' | Name: 'eth1' | Ip: '' | Eth: '' ###

Target[192.168.1.11_3]: 3:SER2@192.168.1.11:
SetEnv[192.168.1.11_3]: MRTG_INT_IP="" MRTG_INT_DESCR="eth1"
Options[192.168.1.11_3]: growright,nopercent
MaxBytes[192.168.1.11_3]: 125000000
Title[192.168.1.11_3]: Análisis de trafico eth1 SER2
PageTop[192.168.1.11_3]: <h1>Análisis de trafico eth1 -- SER2</h1>
        <div id="sysdetails">
                <table>
                        <tr>
                                <td>Sistema:</td>
                                <td>SER2</td>
                        </tr>
                        <tr>
                                <td>Administrador:</td>
                                <td>Elizabeth; (configure /etc/snmp/snmp.local.conf)</td>
                        </tr>
```

```
                                <tr>
                                        <td>Descripcion:</td>
                                        <td>eth1  </td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Mombre de la interfaz:</td>
                                        <td>eth1</td>
                                </tr>
                                <tr>
                                        <td>Velocidad Maxima:</td>
                                        <td>125.0 MBytes/s</td>
                                </tr>
                        </table>
                </div>

### Interface 5 >> Descr: 'bond0' | Name: 'bond0' | Ip: '192.168.1.11' | Eth: '' ###

Target[192.168.1.11_5]: 5:SER2@192.168.1.11:
SetEnv[192.168.1.11_5]: MRTG_INT_IP="192.168.1.11" MRTG_INT_DESCR="bond0"
Options[192.168.1.11_5]: growright,nopercent
MaxBytes[192.168.1.11_5]: 1250000
Title[192.168.1.11_5]: Análisis de trafico bond0 -- SER2
PageTop[192.168.1.11_5]: <h1>Análisis de trafico bond0 -- SER2</h1>
                <div id="sysdetails">
                        <table>
                                <tr>
                                        <td>Sistema:</td>
                                        <td>SER2</td>
                                </tr>
                                <tr>
                                        <td>Administrador:</td>
                                        <td>Elizabeth</td>
                                </tr>
                                <tr>
                                        <td>Descripcion:</td>
                                        <td>bond0  </td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>bond0</td>
                                </tr>
                                <tr>
                                        <td>Velocidad Maxima:</td>
                                        <td>1250.0 kBytes/s</td>
                                </tr>
                                <tr>
                                        <td>Ip:</td>
                                        <td>192.168.1.11 (www.SER2nacionalderiesgos.gob.mx)</td>
                                </tr>
                        </table>
                </div>

### Interface 8 >> Descr: 'eth0' | Name: 'eth0' | Ip: '' | Eth: '' ###

Target[192.168.1.11_8]: 8:SER2@192.168.1.11:
SetEnv[192.168.1.11_8]: MRTG_INT_IP="" MRTG_INT_DESCR="eth0"
Options[192.168.1.11_8]: growright,nopercent
MaxBytes[192.168.1.11_8]: 1250000
Title[192.168.1.11_8]: Análisis de trafico de th0 -- SER2
PageTop[192.168.1.11_8]: <h1>Análisis de trafico de th0 -- SER2</h1>
                <div id="sysdetails">
                        <table>
                                <tr>
                                        <td>Sistema:</td>
                                        <td>SER2</td>
                                </tr>
                                <tr>
                                        <td>Administradorr:</td>
                                        <td>Elizabeth</td>
```

```
                        </tr>
                        <tr>
                                <td>Descripcion:</td>
                                <td>eth0  </td>
                        </tr>
                        <tr>
                                <td>Tipo de interfaz:</td>
                                <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                                <td>Nombre de interfaz:</td>
                                <td>eth0</td>
                        </tr>
                        <tr>
                                <td>Velocidad Maxima:</td>
                                <td>1250.0 kBytes/s</td>
                        </tr>
                </table>
        </div>

##################################################################
#System: SER3
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 AT/AT COMPATIBLE - Software:
Windows Version 6.0 (Build 6002 Multiprocessor Free)
##################################################################


#####Grafica del rendimiento del CPU#####
Target[192.168.1.12_cpu]: (hrProcessorLoad.2&hrProcessorLoad.2:SER3@192.168.1.12 +
hrProcessorLoad.3&hrProcessorLoad.3:SER3@192.168.1.12 +
hrProcessorLoad.4&hrProcessorLoad.4:SER3@192.168.1.12 +
hrProcessorLoad.5&hrProcessorLoad.5:SER3@192.168.1.12 +
hrProcessorLoad.6&hrProcessorLoad.6:SER3@192.168.1.12 +
hrProcessorLoad.7&hrProcessorLoad.7:SER3@192.168.1.12 +
hrProcessorLoad.8&hrProcessorLoad.8:SER3@192.168.1.12 +
hrProcessorLoad.9&hrProcessorLoad.9:SER3@192.168.1.12) / (8)
MaxBytes[192.168.1.12_cpu]: 100
Title[192.168.1.12_cpu]: Carga CPU--SER3
PageTop[192.168.1.12_cpu]: <H1>Carga Activa CPU %--SER3</H1>
ShortLegend[192.168.1.12_cpu]: %
YLegend[192.168.1.12_cpu]: Utilizacion del CPU
Legend1[192.168.1.12_cpu]: CPU activa %
LegendI[192.168.1.12_cpu]: Active
LegendO[192.168.1.12_cpu]:
Options[192.168.1.12_cpu]: growright,nopercent,gauge

######Monitoreo de memoria######
Target[192.168.1.12_mem]: hrStorageUsed.7&hrStorageSize.7:SER3@192.168.1.12 *
hrStorageAllocationUnits.7&hrStorageAllocationUnits.7:SER3@192.168.1.12 * 1000 / 1048576
PageTop[192.168.1.12_mem]: <H1>Memoria libre--SER3</H1>
Options[192.168.1.12_mem]: nopercent,gauge,growright
Title[192.168.1.12_mem]: Memoria libre--SER3
MaxBytes[192.168.1.12_mem]: 100000000000000
YLegend[192.168.1.12_mem]: bytes
ShortLegend[192.168.1.12_mem]: bytes
LegendI[192.168.1.12_mem]: Memoria en uso
LegendO[192.168.1.12_mem]: Memoria total


###Temperatura procesadores#######
Target[192.168.1.3_tem-proc-in]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.100&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.101:SER3@192.168.1.3
PageTop[192.168.1.3_tem-proc-in]: <H1>Temperatura de los procesadores--SER3</H1>
Options[192.168.1.3_tem-proc-in]: gauge,nopercent,growright
Title[192.168.1.3_tem-proc-in]: Temperaturas de procesadores--SER3
MaxBytes[192.168.1.3_tem-proc-in]: 50
LegendI[192.168.1.3_tem-proc-in]: Temperatura del procesador 1
LegendO[192.168.1.3_tem-proc-in]:Temperatura del procesador 2
ShortLegend[192.168.1.3_tem-proc-in]: Â°

###Interface 10 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S
Aceleracion' | Name: 'ethernet_6' | Ip: '' | Eth: '00-1e-68-57-71-be' ###

Target[192.168.1.12_10]: 10:SER3@192.168.1.12:
SetEnv[192.168.1.12_10]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S "
Options[192.168.1.12_10]: growright,nopercent
```

```
MaxBytes[192.168.1.12_10]: 125000000
Title[192.168.1.12_10]: Análisis de trafico eth6 (ID10) -- SER3
PageTop[192.168.1.12_10]: <h1>Análisis de trafico eth6 (ID10) -- SER3</h1>
     <div id="sysdetails">
     <table>
           <tr>
               <td>Sistema:</td>
               <td>SER3</td>
           </tr>
           <tr>
               <td>Administrador:</td>
               <td>Elizabeth</td>
           </tr>
           <tr>
               <td>Descripcion:</td>
               <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S </td>
           </tr>
           <tr>
               <td>Tipo de interfaz:</td>
               <td>ethernetCsmacd (6)</td>
           </tr>
           <tr>
               <td>Nombre de interfaz:</td>
                <td>ethernet_6</td>
            </tr>
            <tr>
                <td>Velocidad Maxima:</td>
                <td>125.0 MBytes/s</td>
            </tr>
        </table>
        </div>


### Interface 11 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S -#2' |
Name: 'ethernet_8' | Ip: '' | Eth: '00-1e-68-57-71-bf' ###

Target[192.168.1.12_11]: 11:SER3@192.168.1.12:
SetEnv[192.168.1.12_11]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S -#2"
Options[192.168.1.12_11]: growright,nopercent
MaxBytes[192.168.1.12_11]: 125000000
Title[192.168.1.12_11]: Análisis de trafico eth8 (ID11) -- SER3
PageTop[192.168.1.12_11]: <h1>Análisis de trafico eth8 (ID11) -- SER3</h1>
     <div id="sysdetails">
          <table>
                <tr>
                    <td>Sistema:</td>
                    <td>SER3</td>
                </tr>
                <tr>
                    <td>Administrador:</td>
                    <td>Elizabeth</td>
                </tr>
                <tr>
                     <td>Descripcion:</td>
                     <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S -#2  </td>
                </tr>
                <tr>
                      <td>Tipo de interfaz:</td>
                      <td>ethernetCsmacd (6)</td>
                </tr>
                <tr>
                      <td>Nombre de interfaz:</td>
                      <td>Ethernet 8</td>
                </tr>
                <tr>
                      <td>Velocidad Maxima:</td>
                      <td>125.0 MBytes/s</td>
                </tr>
          </table>
        </div>

### Interface 12 >> Descr: 'Puente MAC' | Name: 'ethernet_10' | Ip: '192.168.1.12' | Eth: ''
###

Target[192.168.1.12_12]: 12:SER3@192.168.1.12:
SetEnv[192.168.1.12_12]: MRTG_INT_IP="192.168.1.12" MRTG_INT_DESCR="Puente MAC"
```

```
Options[192.168.1.12_12]: growright,nopercent
MaxBytes[192.168.1.12_12]: 125000000
Title[192.168.1.12_12]: Análisis de trafico eth10 (ID12) -- SER3
PageTop[192.168.1.12_12]: <h1>Análisis de trafico eth10 (ID12) -- SER3</h1>
        <div id="sysdetails">
             <table>
                    <tr>
                        <td>Sistema:</td>
                        <td>SER3</td>
                    </tr>
                    <tr>
                        <td>Administrador:</td>
                        <td>Elizabeth</td>
                    </tr>
                    <tr>
                        <td>Descripcion:</td>
                        <td>Puente MAC </td>
                    </tr>
                    <tr>
                        <td>Tipo de interfaz:</td>
                        <td>ethernetCsmacd (6)</td>
                    </tr>
                    <tr>
                        <td>Nombre de interfaz:</td>
                        <td>Ethernet 10</td>
                    </tr>
                    <tr>
                        <td>Velocidad maxima:</td>
                        <td>125.0 MBytes/s</td>
                    </tr>
                    <tr>
                         <td>Ip:</td>
                         <td>192.168.1.12 ()</td>
                    </tr>
             </table>
          </div>


######################################################################
# System: SER4
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 #AT/AT COMPATIBLE - Software:
Windows Version 6.0 (Build 6002 #Multiprocessor Free)
######################################################################


#####Grafica del rendimiento del CPU#####
Target[192.168.1.13_cpu]: (hrProcessorLoad.2&hrProcessorLoad.2:SER4@192.168.1.13 +
hrProcessorLoad.3&hrProcessorLoad.3:SER4@192.168.1.13 +
hrProcessorLoad.4&hrProcessorLoad.4:SER4@192.168.1.13 +
hrProcessorLoad.5&hrProcessorLoad.5:SER4@192.168.1.13 +
hrProcessorLoad.6&hrProcessorLoad.6:SER4@192.168.1.13 +
hrProcessorLoad.7&hrProcessorLoad.7:SER4@192.168.1.13 +
hrProcessorLoad.8&hrProcessorLoad.8:SER4@192.168.1.13 +
hrProcessorLoad.9&hrProcessorLoad.9:SER4@192.168.1.13) / (8)
MaxBytes[192.168.1.13_cpu]: 100
Title[192.168.1.13_cpu]: Carga CPU--SER4
PageTop[192.168.1.13_cpu]: <H1>Carga Activa CPU %--SER4</H1>
ShortLegend[192.168.1.13_cpu]: %
YLegend[192.168.1.13_cpu]: Utilizacion del CPU
Legend1[192.168.1.13_cpu]: CPU activa %
LegendI[192.168.1.13_cpu]: Active
LegendO[192.168.1.13_cpu]:
Options[192.168.1.13_cpu]: growright,nopercent,gauge

######Monitoreo de memoria######
Target[192.168.1.13_mem]: hrStorageUsed.5&hrStorageSize.5:SER4@192.168.1.13 *
hrStorageAllocationUnits.5&hrStorageAllocationUnits.5:SER4@192.168.1.13 * 1000 / 1048576
PageTop[192.168.1.13_mem]: <H1>Memoria libre--SER4</H1>
Options[192.168.1.13_mem]: nopercent,gauge,growright
Title[192.168.1.13_mem]: Memoria libre--SER4
MaxBytes[192.168.1.13_mem]: 100000000000000
YLegend[192.168.1.13_mem]: bytes
ShortLegend[192.168.1.13_mem]: bytes
LegendI[192.168.1.13_mem]: Memoria en uso
LegendO[192.168.1.13_mem]: Memoria total
Legend1[192.168.1.13_mem]: Memoria en uso, no incluye swap, en bytes
```

```
#####Trafico web de SER4############
Target[192.168.1.13_web]:
1.3.6.1.4.1.311.1.7.3.1.2.0&1.3.6.1.4.1.311.1.7.3.1.4.0:SER4@192.168.1.13
PageTop[192.168.1.13_web]: <H1>Trafico web--SER4</H1>
Options[192.168.1.13_web]: growright,nopercent
Title[192.168.1.13_web]: Trafico web--SER4
MaxBytes[192.168.1.13_web]: 125000000

###Temperatura procesador 1#######
Target[192.168.1.4_tem-proc-1]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.136&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.137:SER4@192.168.1.4
PageTop[192.168.1.4_tem-proc-1]: <H1>Temperatura de los procesadores--SER4</H1>
Options[192.168.1.4_tem-proc-1]: gauge,nopercent,growright
Title[192.168.1.4_tem-proc-1]: Temperaturas de procesadores--SER4
MaxBytes[192.168.1.4_tem-proc-1]: 50
LegendI[192.168.1.4_tem-proc-1]: Temperatura del procesador 1
LegendO[192.168.1.4_tem-proc-1]:Temperatura del procesador 2
ShortLegend[192.168.1.4_tem-proc-1]: Â°


### Interface 11 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S' | Name:
'ethernet 6' | Ip: '' | Eth: '00-26-9e-9b-f6-78' ###

Target[192.168.1.13_11]: 11:SER4@192.168.1.13:
SetEnv[192.168.1.13_11]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S"
Options[192.168.1.13_11]: growright,nopercent
MaxBytes[192.168.1.13_11]: 125000000
Title[192.168.1.13_11]: Analisis de trafico eth6 (ID11) -- SER4
PageTop[192.168.1.13_11]: <h1>Analisis de trafico eth6 (ID11) -- SER4</h1>
              <div id="sysdetails">
                     <table>
                            <tr>
                                   <td>Sistema:</td>
                                   <td>SER4</td>
                            </tr>
                            <tr>
                                   <td>Administrador:</td>
                                   <td>CENAPRED</td>
                            </tr>
                            <tr>
                                   <td>Descripcion:</td>
                                   <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S  </td>
                            </tr>
                            <tr>
                                   <td>Tipo de interfaz:</td>
                                   <td>ethernetCsmacd (6)</td>
                            </tr>
                            <tr>
                                   <td>Nombre de interfaz:</td>
                                   <td>Ethernet 6</td>
                            </tr>
                            <tr>
                                   <td>Velocidad maxima:</td>
                                   <td>125.0 MBytes/s</td>
                            </tr>
                     </table>
              </div>


### Interface 12 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S  -#2' |
Name: 'ethernet_8' | Ip: '' | Eth: '00-26-9e-9b-f6-79' ###

Target[192.168.1.13_12]: 12:SER4@192.168.1.13:
SetEnv[192.168.1.13_12]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S  -#2"
Options[192.168.1.13_12]: growright,nopercent
MaxBytes[192.168.1.13_12]: 125000000
Title[192.168.1.13_12]: Analisis de trafico eth8 (ID12) -- SER4
PageTop[192.168.1.13_12]: <h1>Analisis de trafico eth8 (ID12) -- SER4</h1>
              <div id="sysdetails">
                     <table>
                            <tr>
                                   <td>Sistema:</td>
                                   <td>SER4</td>
```

```
                                </tr>
                                <tr>
                                        <td>Administrador:</td>
                                        <td>CENAPRED</td>
                                </tr>
                                <tr>
                                        <td>Descripcion:</td>
                                        <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S  -#2  </td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>Ethernet 8</td>
                                </tr>
                                <tr>
                                        <td>Velocidad maxima:</td>
                                        <td>125.0 MBytes/s</td>
                                </tr>
                        </table>
                </div>


### Interface 13 >> Descr: 'Puente MAC' | Name: 'ethernet_10' | Ip: '192.168.1.13' | Eth: ''
###

Target[192.168.1.13_13]: 13:SER4@192.168.1.13:
SetEnv[192.168.1.13_13]: MRTG_INT_IP="192.168.1.13" MRTG_INT_DESCR="Puente MAC"
Options[192.168.1.13_13]: growright,nopercent
MaxBytes[192.168.1.13_13]: 125000000
Title[192.168.1.13_13]: Analisis de trafico eth10 (ID13) -- SER4
PageTop[192.168.1.13_13]: <h1>Analisis de trafico eth10 (ID13)-- SER4</h1>
                <div id="sysdetails">
                        <table>
                                <tr>
                                        <td>Sistema:</td>
                                        <td>SER4</td>
                                </tr>
                                <tr>
                                        <td>Administrador:</td>
                                        <td>CENAPRED</td>
                                </tr>
                                <tr>
                                        <td>Descripcion:</td>
                                        <td>Puente MAC</td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>Ethernet 10</td>
                                </tr>
                                <tr>
                                        <td>Velocidad maxima:</td>
                                        <td>125.0 MBytes/s</td>
                                </tr>
                                <tr>
                                        <td>Ip:</td>
                                        <td>192.168.1.13 ()</td>
                                </tr>
                        </table>
                </div>
```

Anexo 6. SER1.html RHEL

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
    <TITLE>SER1</TITLE>
```

```
    <!-- Command line is easier to read using "View Page Properties" of your browser -->
    <!-- But not all browsers show that SER3rmation. :-(                              -->
    <META NAME="Command-Line" CONTENT="/usr/bin/indexmaker /etc/mrtg/mrtg1.cfg">
    <META HTTP-EQUIV="Refresh" CONTENT="300">
    <META HTTP-EQUIV="Cache-Control" content="no-cache">
    <META HTTP-EQUIV="Pragma" CONTENT="no-cache">
    <META HTTP-EQUIV="Expires" CONTENT="Fri, 09 Dec 2011 17:08:43 GMT">
    <LINK HREF="favicon.ico" rel="shortcut icon" />

<style type="text/css">
<!--
/* commandline was: /usr/bin/indexmaker /etc/mrtg/mrtg1.cfg */
/* sorry, no style, just abusing this to place the commandline and pass validation */
-->
</style>
</HEAD>

<BODY bgcolor="#ffffff" text="#000000" link="#000000" vlink="#000000" alink="#000000">


<H1>MRTG Index Page</H1>

<TABLE BORDER=0 CELLPADDING=0 CELLSPACING=10>
<tr>
<td><DIV><B>Carga Activa CPU %--SER1</B></DIV>
<DIV><A HREF="192.168.1.10_cpu.html"><IMG BORDER=1 ALT="192.168.1.10_cpu Traffic Graph"
SRC="192.168.1.10_cpu-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.10_cpu.html" --></SMALL></DIV>
</td><td><DIV><B>Memoria libre--SER1</B></DIV>
<DIV><A HREF="192.168.1.10_mem.html"><IMG BORDER=1 ALT="192.168.1.10_mem Traffic Graph"
SRC="192.168.1.10_mem-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.10_mem.html" --></SMALL></DIV>
</td></tr>
<tr>
<td><DIV><B>Temperatura de los procesadores--SER1</B></DIV>
<DIV><A HREF="192.168.1.1_tem-proc-im.html"><IMG BORDER=1 ALT="192.168.1.1_tem-proc-im Traffic Graph"
SRC="192.168.1.1_tem-proc-im-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.1_tem-proc-im.html" --></SMALL></DIV>
</td><td><DIV><B>Analisis de trafico eth6 (ID10) -- SER1</B></DIV>
<DIV><A HREF="192.168.1.10_10.html"><IMG BORDER=1 ALT="192.168.1.10_10 Traffic Graph"
SRC="192.168.1.10_10-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.10_10.html" --></SMALL></DIV>
</td></tr>
<tr>
<td><DIV><B>Analisis de trafico de eth8 (ID11) -- SER1</B></DIV>
<DIV><A HREF="192.168.1.10_11.html"><IMG BORDER=1 ALT="192.168.1.10_11 Traffic Graph"
SRC="192.168.1.10_11-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.10_11.html" --></SMALL></DIV>
</td><td><DIV><B>Analisis de trafico (ID12) -- SER1</B></DIV>
<DIV><A HREF="192.168.1.10_12.html"><IMG BORDER=1 ALT="192.168.1.10_12 Traffic Graph"
SRC="192.168.1.10_12-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.10_12.html" --></SMALL></DIV>
</td></tr>
<tr>
<td></td>
</tr>
</TABLE>

<BR>
<TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0>
  <TR>
    <TD WIDTH=63><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-l.png" WIDTH=63 HEIGHT=25 ALT="MRTG"></A></TD>
    <TD WIDTH=25><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-m.png" WIDTH=25 HEIGHT=25 ALT=""></A></TD>
    <TD WIDTH=388><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-r.png" WIDTH=388 HEIGHT=25
    ALT="Multi Router Traffic Grapher"></A></TD>
  </TR>
</TABLE>
<TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0>
```

```
  <TR VALIGN=top>
  <TD WIDTH=88 ALIGN=RIGHT><FONT FACE="Arial,Helvetica" SIZE=2>
  version 2.14.5</FONT></TD>
  <TD WIDTH=388 ALIGN=RIGHT><FONT FACE="Arial,Helvetica" SIZE=2>
  <A HREF="http://tobi.oetiker.ch/">Tobias Oetiker</A>
  <A HREF="mailto:tobi+mrtglink@oetiker.ch">&lt;tobi@oetiker.ch&gt;</A>
  and <A HREF="http://www.bungi.com/">Dave Rand</A> <A
HREF="mailto:dlr@bungi.com">&lt;dlr@bungi.com&gt;</A></FONT>
  </TD>
</TR>
</TABLE>
</BODY>
</HTML>
```

Anexo 7. SER2.html RHEL

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
    <TITLE>SER2</TITLE>
    <!-- Command line is easier to read using "View Page Properties" of your browser -->
    <!-- But not all browsers show that SER3rmation. :-(                              -->
    <META NAME="Command-Line" CONTENT="/usr/bin/indexmaker /etc/mrtg/mrtg2.cfg">
    <META HTTP-EQUIV="Refresh" CONTENT="300">
    <META HTTP-EQUIV="Cache-Control" content="no-cache">
    <META HTTP-EQUIV="Pragma" CONTENT="no-cache">
    <META HTTP-EQUIV="Expires" CONTENT="Mon, 05 Dec 2011 19:49:21 GMT">
    <LINK HREF="favicon.ico" rel="shortcut icon" />

<style type="text/css">
<!--
/* commandline was: /usr/bin/indexmaker /etc/mrtg/mrtg2.cfg */
/* sorry, no style, just abusing this to place the commandline and pass validation */
-->
</style>
</HEAD>

<BODY bgcolor="#ffffff" text="#000000" link="#000000" vlink="#000000" alink="#000000">


<H1>MRTG Index Page</H1>

<TABLE BORDER=0 CELLPADDING=0 CELLSPACING=10>
<tr>
<td><DIV><B>Carga Activa CPU %--SER2</B></DIV>
<DIV><A HREF="192.168.1.11_cpu.html"><IMG BORDER=1 ALT="192.168.1.11_cpu Traffic Graph"
SRC="192.168.1.11_cpu-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.11_cpu.html" --></SMALL></DIV>
</td><td><DIV><B>Memoria libre--SER2</B></DIV>
<DIV><A HREF="192.168.1.11_mem.html"><IMG BORDER=1 ALT="192.168.1.11_mem Traffic Graph"
SRC="192.168.1.11_mem-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.11_mem.html" --></SMALL></DIV>
</td></tr>
<tr>
<td><DIV><B>Temperatura de los procesadores--SER2</B></DIV>
<DIV><A HREF="192.168.1.2_tem-proc-at.html"><IMG BORDER=1 ALT="192.168.1.2_tem-proc-at Traffic Graph"
SRC="192.168.1.2_tem-proc-at-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.2_tem-proc-at.html" --></SMALL></DIV>
</td><td><DIV><B>Analisis de trafico eth1 -- SER2</B></DIV>
<DIV><A HREF="192.168.1.11_3.html"><IMG BORDER=1 ALT="192.168.1.11_3 Traffic Graph"
SRC="192.168.1.11_3-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.11_3.html" --></SMALL></DIV>
</td></tr>
<tr>
<td><DIV><B>Analisis de trafico bond0 -- SER2</B></DIV>
<DIV><A HREF="192.168.1.11_5.html"><IMG BORDER=1 ALT="192.168.1.11_5 Traffic Graph"
SRC="192.168.1.11_5-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.11_5.html" --></SMALL></DIV>
</td><td><DIV><B>Analisis de trafico de th0 -- SER2</B></DIV>
<DIV><A HREF="192.168.1.11_8.html"><IMG BORDER=1 ALT="192.168.1.11_8 Traffic Graph"
SRC="192.168.1.11_8-day.png"></A><BR>
```

```
<SMALL><!--#flastmod file="192.168.1.11_8.html" --></SMALL></DIV>
</td></tr>
<tr>
<td></td>
</tr>
</TABLE>

<BR>
<TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0>
  <TR>
    <TD WIDTH=63><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-l.png" WIDTH=63 HEIGHT=25 ALT="MRTG"></A></TD>
    <TD WIDTH=25><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-m.png" WIDTH=25 HEIGHT=25 ALT=""></A></TD>
    <TD WIDTH=388><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-r.png" WIDTH=388 HEIGHT=25
    ALT="Multi Router Traffic Grapher"></A></TD>
  </TR>
</TABLE>
<TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0>
  <TR VALIGN=top>
  <TD WIDTH=88 ALIGN=RIGHT><FONT FACE="Arial,Helvetica" SIZE=2>
  version 2.14.5</FONT></TD>
  <TD WIDTH=388 ALIGN=RIGHT><FONT FACE="Arial,Helvetica" SIZE=2>
  <A HREF="http://tobi.oetiker.ch/">Tobias Oetiker</A>
  <A HREF="mailto:tobi+mrtglink@oetiker.ch">&lt;tobi@oetiker.ch&gt;</A>
  and <A HREF="http://www.bungi.com/">Dave Rand</A> <A
HREF="mailto:dlr@bungi.com">&lt;dlr@bungi.com&gt;</A></FONT>
  </TD>
</TR>
</TABLE>
</BODY>
</HTML>
```

Anexo 8. SER3.html RHEL

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
    <TITLE>SER3</TITLE>
    <!-- Command line is easier to read using "View Page Properties" of your browser -->
    <!-- But not all browsers show that SER3rmation. :-(                              -->
    <META NAME="Command-Line" CONTENT="/usr/bin/indexmaker /etc/mrtg/mrtg3.cfg">
    <META HTTP-EQUIV="Refresh" CONTENT="300">
    <META HTTP-EQUIV="Cache-Control" content="no-cache">
    <META HTTP-EQUIV="Pragma" CONTENT="no-cache">
    <META HTTP-EQUIV="Expires" CONTENT="Mon, 29 Aug 2011 17:17:49 GMT">
    <LINK HREF="favicon.ico" rel="shortcut icon" />

<style type="text/css">
<!--
/* commandline was: /usr/bin/indexmaker /etc/mrtg/mrtg3.cfg */
/* sorry, no style, just abusing this to place the commandline and pass validation */
-->
</style>
</HEAD>

<BODY bgcolor="#ffffff" text="#000000" link="#000000" vlink="#000000" alink="#000000">


<H1>MRTG Index Page</H1>

<TABLE BORDER=0 CELLPADDING=0 CELLSPACING=10>
<tr>
<td><DIV><B>Carga Activa CPU %--SER3</B></DIV>
<DIV><A HREF="192.168.1.12_cpu.html"><IMG BORDER=1 ALT="192.168.1.12_cpu Traffic Graph"
SRC="192.168.1.12_cpu-day.png"></A><BR>
```

```
<SMALL><!--#flastmod file="192.168.1.12_cpu.html" --></SMALL></DIV>
</td><td><DIV><B>Memoria libre--SER3</B></DIV>
<DIV><A HREF="192.168.1.12_mem.html"><IMG BORDER=1 ALT="192.168.1.12_mem Traffic Graph"
SRC="192.168.1.12_mem-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.12_mem.html" --></SMALL></DIV>
</td></tr>
<tr>
<td><DIV><B>Temperatura de los procesadores--SER3</B></DIV>
<DIV><A HREF="192.168.1.3_tem-proc-in.html"><IMG BORDER=1 ALT="192.168.1.3_tem-proc-in Traffic Graph"
SRC="192.168.1.3_tem-proc-in-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.3_tem-proc-in.html" --></SMALL></DIV>
</td><td><DIV><B>Analisis de trafico eth6 (ID10) -- SER3</B></DIV>
<DIV><A HREF="192.168.1.12_10.html"><IMG BORDER=1 ALT="192.168.1.12_10 Traffic Graph"
SRC="192.168.1.12_10-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.12_10.html" --></SMALL></DIV>
</td></tr>
<tr>
<td><DIV><B>Analisis de trafico eth8 (ID11) -- SER3</B></DIV>
<DIV><A HREF="192.168.1.12_11.html"><IMG BORDER=1 ALT="192.168.1.12_11 Traffic Graph"
SRC="192.168.1.12_11-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.12_11.html" --></SMALL></DIV>
</td><td><DIV><B>Analisis de trafico eth10 (ID12) -- SER3</B></DIV>
<DIV><A HREF="192.168.1.12_12.html"><IMG BORDER=1 ALT="192.168.1.12_12 Traffic Graph"
SRC="192.168.1.12_12-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.12_12.html" --></SMALL></DIV>
</td></tr>
<tr>
<td></td>
</tr>
</TABLE>

<BR>
<TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0>
  <TR>
    <TD WIDTH=63><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-l.png" WIDTH=63 HEIGHT=25 ALT="MRTG"></A></TD>
    <TD WIDTH=25><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-m.png" WIDTH=25 HEIGHT=25 ALT=""></A></TD>
    <TD WIDTH=388><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-r.png" WIDTH=388 HEIGHT=25
    ALT="Multi Router Traffic Grapher"></A></TD>
  </TR>
</TABLE>
<TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0>
  <TR VALIGN=top>
  <TD WIDTH=88 ALIGN=RIGHT><FONT FACE="Arial,Helvetica" SIZE=2>
  version 2.14.5</FONT></TD>
  <TD WIDTH=388 ALIGN=RIGHT><FONT FACE="Arial,Helvetica" SIZE=2>
  <A HREF="http://tobi.oetiker.ch/">Tobias Oetiker</A>
  <A HREF="mailto:tobi+mrtglink@oetiker.ch">&lt;tobi@oetiker.ch&gt;</A>
  and <A HREF="http://www.bungi.com/">Dave Rand</A> <A
HREF="mailto:dlr@bungi.com">&lt;dlr@bungi.com&gt;</A></FONT>
  </TD>
</TR>
</TABLE>
</BODY>
</HTML>
```

Anexo 9. SER4.html RHEL

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
    <TITLE>SER4</TITLE>
    <!-- Command line is easier to read using "View Page Properties" of your browser -->
    <!-- But not all browsers show that SER3rmation. :-(                              -->
    <META NAME="Command-Line" CONTENT="/usr/bin/indexmaker /etc/mrtg/mrtg4.cfg">
```

```
    <META HTTP-EQUIV="Refresh" CONTENT="300">
    <META HTTP-EQUIV="Cache-Control" content="no-cache">
    <META HTTP-EQUIV="Pragma" CONTENT="no-cache">
    <META HTTP-EQUIV="Expires" CONTENT="Wed, 30 Nov 2011 18:33:31 GMT">
    <LINK HREF="favicon.ico" rel="shortcut icon" />

<style type="text/css">
<!--
/* commandline was: /usr/bin/indexmaker /etc/mrtg/mrtg4.cfg */
/* sorry, no style, just abusing this to place the commandline and pass validation */
-->
</style>
</HEAD>

<BODY bgcolor="#ffffff" text="#000000" link="#000000" vlink="#000000" alink="#000000">


<H1>MRTG Index Page</H1>

<TABLE BORDER=0 CELLPADDING=0 CELLSPACING=10>
<tr>
<td><DIV><B>Carga Activa CPU %--SER4</B></DIV>
<DIV><A HREF="192.168.1.13_cpu.html"><IMG BORDER=1 ALT="192.168.1.13_cpu Traffic Graph"
SRC="192.168.1.13_cpu-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.13_cpu.html" --></SMALL></DIV>
</td><td><DIV><B>Memoria libre--SER4</B></DIV>
<DIV><A HREF="192.168.1.13_mem.html"><IMG BORDER=1 ALT="192.168.1.13_mem Traffic Graph"
SRC="192.168.1.13_mem-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.13_mem.html" --></SMALL></DIV>
</td></tr>
<tr>
<td><DIV><B>Trafico web--SER4</B></DIV>
<DIV><A HREF="192.168.1.13_web.html"><IMG BORDER=1 ALT="192.168.1.13_web Traffic Graph"
SRC="192.168.1.13_web-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.13_web.html" --></SMALL></DIV>
</td><td><DIV><B>Temperatura de los procesadores--SER4</B></DIV>
<DIV><A HREF="192.168.1.4_tem-proc-1.html"><IMG BORDER=1 ALT="192.168.1.4_tem-proc-1 Traffic Graph"
SRC="192.168.1.4_tem-proc-1-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.4_tem-proc-1.html" --></SMALL></DIV>
</td></tr>
<tr>
<td><DIV><B>Analisis de trafico eth6 (ID11) -- SER4</B></DIV>
<DIV><A HREF="192.168.1.13_11.html"><IMG BORDER=1 ALT="192.168.1.13_11 Traffic Graph"
SRC="192.168.1.13_11-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.13_11.html" --></SMALL></DIV>
</td><td><DIV><B>Analisis de trafico eth8 (ID12) -- SER4</B></DIV>
<DIV><A HREF="192.168.1.13_12.html"><IMG BORDER=1 ALT="192.168.1.13_12 Traffic Graph"
SRC="192.168.1.13_12-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.13_12.html" --></SMALL></DIV>
</td></tr>
<tr>
<td><DIV><B>Analisis de trafico eth10 (ID13)-- SER4</B></DIV>
<DIV><A HREF="192.168.1.13_13.html"><IMG BORDER=1 ALT="192.168.1.13_13 Traffic Graph"
SRC="192.168.1.13_13-day.png"></A><BR>
<SMALL><!--#flastmod file="192.168.1.13_13.html" --></SMALL></DIV>
</td><td></td>
</tr>
</TABLE>

<BR>
<TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0>
  <TR>
    <TD WIDTH=63><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-l.png" WIDTH=63 HEIGHT=25 ALT="MRTG"></A></TD>
    <TD WIDTH=25><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-m.png" WIDTH=25 HEIGHT=25 ALT=""></A></TD>
    <TD WIDTH=388><A
    HREF="http://oss.oetiker.ch/mrtg/"><IMG
    BORDER=0 SRC="mrtg-r.png" WIDTH=388 HEIGHT=25
    ALT="Multi Router Traffic Grapher"></A></TD>
  </TR>
</TABLE>
```

```
<TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0>
  <TR VALIGN=top>
  <TD WIDTH=88 ALIGN=RIGHT><FONT FACE="Arial,Helvetica" SIZE=2>
  version 2.14.5</FONT></TD>
  <TD WIDTH=388 ALIGN=RIGHT><FONT FACE="Arial,Helvetica" SIZE=2>
  <A HREF="http://tobi.oetiker.ch/">Tobias Oetiker</A>
  <A HREF="mailto:tobi+mrtglink@oetiker.ch">&lt;tobi@oetiker.ch&gt;</A>
  and <A HREF="http://www.bungi.com/">Dave Rand</A> <A
HREF="mailto:dlr@bungi.com">&lt;dlr@bungi.com&gt;</A></FONT>
  </TD>
</TR>
</TABLE>
</BODY>
</HTML>
```

Anexo 10. Archivo de configuración mrtg.cfg OpenSuse

```
### Global Defaults
#  to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits

WorkDir: /srv/www/htdocs/mrtg
Language: spanish
EnableIPv6: no

######################################################################
# System: SER1
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 AT/AT COMPATIBLE - Software:
Windows Version 6.0 (Build 6002 Multiprocessor Free)
# Contact: root
# Location: Cenapred
######################################################################

#####Grafica del rendimiento del CPU#####
Target[192.168.1.10_cpu]: (
.1.3.6.1.2.1.25.3.3.1.2.2&.1.3.6.1.2.1.25.3.3.1.2.2:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.3&.1.3.6.1.2.1.25.3.3.1.2.3:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.4&.1.3.6.1.2.1.25.3.3.1.2.4:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.5&.1.3.6.1.2.1.25.3.3.1.2.5:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.6&.1.3.6.1.2.1.25.3.3.1.2.6:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.7&.1.3.6.1.2.1.25.3.3.1.2.7:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.8&.1.3.6.1.2.1.25.3.3.1.2.8:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.9&.1.3.6.1.2.1.25.3.3.1.2.9:SER1@192.168.1.10) / (8)
MaxBytes[192.168.1.10_cpu]: 100
Title[192.168.1.10_cpu]: Carga CPU--SER1
PageTop[192.168.1.10_cpu]: <H1>Carga Activa CPU %--SER1</H1>
ShortLegend[192.168.1.10_cpu]: %
YLegend[192.168.1.10_cpu]: Carga CPU
Legend1[192.168.1.10_cpu]: CPU activa %
Legend2[192.168.1.10_cpu]:
Legend3[192.168.1.10_cpu]:
Legend4[192.168.1.10_cpu]:
LegendI[192.168.1.10_cpu]: Active
LegendO[192.168.1.10_cpu]:
Options[192.168.1.10_cpu]: growright,nopercent,gauge

######Monitoreo de memoria######
Target[192.168.1.10_mem]:
.1.3.6.1.2.1.25.2.3.1.6.5&.1.3.6.1.2.1.25.2.3.1.5.5:SER1@192.168.1.10 *
.1.3.6.1.2.1.25.2.3.1.4.5&.1.3.6.1.2.1.25.2.3.1.4.5:SER1@192.168.1.10 * 1000 / 1048576
PageTop[192.168.1.10_mem]: <H1>Memoria libre--SER1</H1>
Options[192.168.1.10_mem]: nopercent,gauge,growright
Title[192.168.1.10_mem]: Memoria libre--SER1
MaxBytes[192.168.1.10_mem]: 100000000000000
YLegend[192.168.1.10_mem]: bytes
ShortLegend[192.168.1.10_mem]: bytes
LegendI[192.168.1.10_mem]: Memoria en uso
LegendO[192.168.1.10_mem]: Memoria total



###Temperatura procesadores#######
```

```
Target[192.168.1.1_tem-proc-im]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.124&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.125:SER1@192.168.1.1
PageTop[192.168.1.1_tem-proc-im]: <H1>Temperatura de los procesadores--SER1</H1>
Options[192.168.1.1_tem-proc-im]: gauge,nopercent,growright
Title[192.168.1.1_tem-proc-im]: Temperaturas de procesadores--SER1
MaxBytes[192.168.1.1_tem-proc-im]: 50
YLegend[192.168.1.1_tem-proc-im]: grados
LegendI[192.168.1.1_tem-proc-im]: Temperatura del procesador 1
LegendO[192.168.1.1_tem-proc-im]:Temperatura del procesador 2
ShortLegend[192.168.1.1_tem-proc-im]: Â°


### Interface 10 >> Descr: 'Intel(R)-PRO/1000-EB-Network-Connection-with-I/O-Acceleration' |
Name: 'ethernet_6' | Ip: '' | Eth: '30-78-30-30-32-33-38-62-31-37-61-37-33-34' ###

Target[192.168.1.10_10]: 10:SER1@192.168.1.10:
SetEnv[192.168.1.10_10]: MRTG_INT_IP="" MRTG_INT_DESCR="Intel(R)-PRO/1000-EB-Network-
Connection-with-I/O-Acceleration"
MaxBytes[192.168.1.10_10]: 125000000
Title[192.168.1.10_10]: Analisis de trafico eth6 (ID 10) -- SER1
PageTop[192.168.1.10_10]: <h1>Analisis de trafico eth6 (ID 10) -- SER1</h1>
       <div id="sysdetails">
             <table>
                  <tr>
                      <td>Sistema:</td>
                      <td>SER1</td>
                  </tr>
                  <tr>
                        <td>Administrador:</td>
                        <td>Elizabeth Rubio</td>
                     </tr>
                     <tr>
                         <td>Descripcion:</td>
                         <td>Intel(R)-PRO/1000-EB-Conexion de red con Aceleracion E/S  </td>
                     </tr>
                     <tr>
                          <td>Tipo de interfaz:</td>
                          <td>ethernetCsmacd (6)</td>
                     </tr>
                     <tr>
                          <td>Nombre de interfaz:</td>
                          <td>ethernet 6</td>
                     </tr>
                     <tr>
                          <td>Velocidad Maxima:</td>
                          <td>125.0 MBytes/s</td>
                     </tr>
                </table>
           </div>


### Interface 11 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S -#2' |
Name: 'ethernet 8' | Ip: '' | Eth: '00-23-8b-17-a7-35' ###

Target[192.168.1.10_11]: 11:SER1@192.168.1.10:
SetEnv[192.168.1.10_11]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S -#2"
Options[192.168.1.10_11]: growright,nopercent
MaxBytes[192.168.1.10_11]: 125000000
Title[192.168.1.10_11]: Análisis de trafico de eth8 (ID11) -- SER1
PageTop[192.168.1.10_11]: <h1>Análisis de trafico de eth8 (ID11) -- SER1</h1>
              <div id="sysdetails">
                     <table>
                            <tr>
                                   <td>Sistema:</td>
                                   <td>SER1</td>
                            </tr>
                            <tr>
                                   <td>Administrador:</td>
                                   <td>Elizabeth</td>
                            </tr>
                            <tr>
                                   <td>Descripción:</td>
                                   <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S -#2  </td>
                            </tr>
                            <tr>
```

```
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>Ethernet 8</td>
                                </tr>
                                <tr>
                                        <td>Velocidad Maxima:</td>
                                        <td>125.0 MBytes/s</td>
                                </tr>
                        </table>
                </div>


### Interface 12 >> Descr: 'Puente MAC' | Name: 'ethernet_10' | Ip: '192.168.1.10' | Eth: ''
###

Target[192.168.1.10_12]: 12:SER1@192.168.1.10:
SetEnv[192.168.1.10_12]: MRTG_INT_IP="192.168.1.10" MRTG_INT_DESCR="Puente MAC"
MaxBytes[192.168.1.10_12]: 125000000
Options[192.168.1.10_12]: growright,nopercent
Title[192.168.1.10_12]: Análisis de trafico eth10 (ID12) -- SER1
PageTop[192.168.1.10_12]: <h1>Análisis de tráfico (ID12) -- SER1</h1>
                <div id="sysdetails">
                        <table>
                                <tr>
                                        <td>Sistema:</td>
                                        <td>SER1</td>
                                </tr>
                                <tr>
                                        <td>Administrador:</td>
                                        <td>Elizabeth</td>
                                </tr>
                                <tr>
                                        <td>Descripcion:</td>
                                        <td>Puente MAC  </td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>ethernet_10</td>
                                </tr>
                                <tr>
                                        <td>Velocidad Maxima:</td>
                                        <td>125.0 MBytes/s</td>
                                </tr>
                                <tr>
                                        <td>Ip:</td>
                                        <td>192.168.1.10 ()</td>
                                </tr>
                        </table>
                </div>


######################################################################
# System: SER2
# Description: Linux SER2 2.6.18-53.el5xen #1 SMP Wed Oct 10 17:06:12 EDT 2007 i686
# Contact: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
# Location: Unknown (edit /etc/snmp/snmpd.conf)
######################################################################



#####Grafica del rendimiento del CPU#####

Target[192.168.1.11_cpu]: (
.1.3.6.1.2.1.25.3.3.1.2.768&.1.3.6.1.2.1.25.3.3.1.2.768:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.769&.1.3.6.1.2.1.25.3.3.1.2.769:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.770&.1.3.6.1.2.1.25.3.3.1.2.770:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.771&.1.3.6.1.2.1.25.3.3.1.2.771:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.772&.1.3.6.1.2.1.25.3.3.1.2.772:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.773&.1.3.6.1.2.1.25.3.3.1.2.773:SER2@192.168.1.11 +
```

```
.1.3.6.1.2.1.25.3.3.1.2.774&.1.3.6.1.2.1.25.3.3.1.2.774:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.775&.1.3.6.1.2.1.25.3.3.1.2.775:SER2@192.168.1.11) / (8)
MaxBytes[192.168.1.11_cpu]: 100
Title[192.168.1.11_cpu]: Carga CPU—SER2
PageTop[192.168.1.11_cpu]: <H1>Carga Activa CPU %--SER2</H1>
ShortLegend[192.168.1.11_cpu]: %
YLegend[192.168.1.11_cpu]: Carga CPU
Legend1[192.168.1.11_cpu]: CPU activa %
Legend2[192.168.1.11_cpu]:
Legend3[192.168.1.11_cpu]:
Legend4[192.168.1.11_cpu]:
LegendI[192.168.1.11_cpu]: Active
LegendO[192.168.1.11_cpu]:
Options[192.168.1.11_cpu]: growright,nopercent,gauge


######Monitoreo de memoria######
Target[192.168.1.11_mem]:
.1.3.6.1.2.1.25.2.3.1.6.2&.1.3.6.1.2.1.25.2.3.1.5.2:SER2@192.168.1.11 *
.1.3.6.1.2.1.25.2.3.1.4.2&.1.3.6.1.2.1.25.2.3.1.4.2:SER2@192.168.1.11 * 1000 / 1048576
PageTop[192.168.1.11_mem]: <H1>Memoria libre—SER2</H1>
Options[192.168.1.11_mem]: nopercent,gauge,growright
Title[192.168.1.11_mem]: Memoria libre—SER2
MaxBytes[192.168.1.11_mem]: 100000000000000
YLegend[192.168.1.11_mem]: bytes
ShortLegend[192.168.1.11_mem]: bytes
LegendI[192.168.1.11_mem]: Memoria en uso
LegendO[192.168.1.11_mem]: Memoria total
Legend1[192.168.1.11_mem]: Memoria en uso, no incluye swap, en bytes


###Temperatura procesadores#######
Target[192.168.1.2_tem-proc-at]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.124&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.125:SER2@192.168.1.2
PageTop[192.168.1.2_tem-proc-at]: <H1>Temperatura de los procesadores--SER2</H1>
Options[192.168.1.2_tem-proc-at]: gauge,nopercent,growright
Title[192.168.1.2_tem-proc-at]: Temperaturas de procesadores--SER2
YLegend[192.168.1.2_tem-proc-at]: grados
MaxBytes[192.168.1.2_tem-proc-at]: 50
LegendI[192.168.1.2_tem-proc-at]: Temperatura del procesador 1
LegendO[192.168.1.2_tem-proc-at]: Temperatura del procesador 2
ShortLegend[192.168.1.2_tem-proc-at]: Â°


### Interface 3 >> Descr: 'eth1' | Name: 'eth1' | Ip: '' | Eth: '' ###

Target[192.168.1.11_3]: 3:SER2@192.168.1.11:
SetEnv[192.168.1.11_3]: MRTG_INT_IP="" MRTG_INT_DESCR="eth1"
Options[192.168.1.11_3]: growright,nopercent
MaxBytes[192.168.1.11_3]: 125000000
Title[192.168.1.11_3]: Análisis de trafico eth1 SER2
PageTop[192.168.1.11_3]: <h1>Análisis de trafico eth1 -- SER2</h1>
              <div id="sysdetails">
                     <table>
                            <tr>
                                   <td>Sistema:</td>
                                   <td>SER2</td>
                            </tr>
                            <tr>
                                   <td>Administrador:</td>
                                   <td>Elizabeth; (configure /etc/snmp/snmp.local.conf)</td>
                            </tr>
                            <tr>
                                   <td>Descripcion:</td>
                                   <td>eth1  </td>
                            </tr>
                            <tr>
                                   <td>Tipo de interfaz:</td>
                                   <td>ethernetCsmacd (6)</td>
                            </tr>
                            <tr>
                                   <td>Mombre de la interfaz:</td>
                                   <td>eth1</td>
                            </tr>
                            <tr>
                                   <td>Velocidad Maxima:</td>
                                   <td>125.0 MBytes/s</td>
```

```
                        </tr>
                    </table>
                </div>

### Interface 5 >> Descr: 'bond0' | Name: 'bond0' | Ip: '192.168.1.11' | Eth: '' ###

Target[192.168.1.11_5]: 5:SER2@192.168.1.11:
SetEnv[192.168.1.11_5]: MRTG_INT_IP="192.168.1.11" MRTG_INT_DESCR="bond0"
Options[192.168.1.11_5]: growright,nopercent
MaxBytes[192.168.1.11_5]: 1250000
Title[192.168.1.11_5]: Análisis de trafico bond0 -- SER2
PageTop[192.168.1.11_5]: <h1>Análisis de trafico bond0 -- SER2</h1>
                <div id="sysdetails">
                    <table>
                        <tr>
                            <td>Sistema:</td>
                            <td>SER2</td>
                        </tr>
                        <tr>
                            <td>Administrador:</td>
                            <td>Elizabeth</td>
                        </tr>
                        <tr>
                            <td>Descripcion:</td>
                            <td>bond0  </td>
                        </tr>
                        <tr>
                            <td>Tipo de interfaz:</td>
                            <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                            <td>Nombre de interfaz:</td>
                            <td>bond0</td>
                        </tr>
                        <tr>
                            <td>Velocidad Maxima:</td>
                            <td>1250.0 kBytes/s</td>
                        </tr>
                        <tr>
                            <td>Ip:</td>
                            <td>192.168.1.11 (www.SER2nacionalderiesgos.gob.mx)</td>
                        </tr>
                    </table>
                </div>

### Interface 8 >> Descr: 'eth0' | Name: 'eth0' | Ip: '' | Eth: '' ###

Target[192.168.1.11_8]: 8:SER2@192.168.1.11:
SetEnv[192.168.1.11_8]: MRTG_INT_IP="" MRTG_INT_DESCR="eth0"
Options[192.168.1.11_8]: growright,nopercent
MaxBytes[192.168.1.11_8]: 1250000
Title[192.168.1.11_8]: Análisis de trafico de th0 -- SER2
PageTop[192.168.1.11_8]: <h1>Análisis de trafico de th0 -- SER2</h1>
                <div id="sysdetails">
                    <table>
                        <tr>
                            <td>Sistema:</td>
                            <td>SER2</td>
                        </tr>
                        <tr>
                            <td>Administradorr:</td>
                            <td>Elizabeth</td>
                        </tr>
                        <tr>
                            <td>Descripcion:</td>
                            <td>eth0  </td>
                        </tr>
                        <tr>
                            <td>Tipo de interfaz:</td>
                            <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                            <td>Nombre de interfaz:</td>
                            <td>eth0</td>
                        </tr>
                        <tr>
                            <td>Velocidad Maxima:</td>
```

```
                                    <td>1250.0 kBytes/s</td>
                                </tr>
                            </table>
                </div>

######################################################################
#System: SER3
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 AT/AT COMPATIBLE - Software:
Windows Version 6.0 (Build 6002 Multiprocessor Free)
######################################################################

#####Grafica del rendimiento del CPU#####

Target[192.168.1.12_cpu]: (
.1.3.6.1.2.1.25.3.3.1.2.2&.1.3.6.1.2.1.25.3.3.1.2.2:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.3&.1.3.6.1.2.1.25.3.3.1.2.3:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.4&.1.3.6.1.2.1.25.3.3.1.2.4:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.5&.1.3.6.1.2.1.25.3.3.1.2.5:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.6&.1.3.6.1.2.1.25.3.3.1.2.6:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.7&.1.3.6.1.2.1.25.3.3.1.2.7:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.8&.1.3.6.1.2.1.25.3.3.1.2.8:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.9&.1.3.6.1.2.1.25.3.3.1.2.9:SER3@192.168.1.12) / (8)
MaxBytes[192.168.1.12_cpu]: 100
Title[192.168.1.12_cpu]: Carga CPU--SER3
PageTop[192.168.1.12_cpu]: <H1>Carga Activa CPU %--SER3</H1>
ShortLegend[192.168.1.12_cpu]: %
YLegend[192.168.1.12_cpu]: Carga CPU
Legend1[192.168.1.12_cpu]: CPU activa %
Legend2[192.168.1.12_cpu]:
Legend3[192.168.1.12_cpu]:
Legend4[192.168.1.12_cpu]:
LegendI[192.168.1.12_cpu]: Active
LegendO[192.168.1.12_cpu]:
Options[192.168.1.12_cpu]: growright,nopercent,gauge

######Monitoreo de memoria######
Target[192.168.1.12_mem]:
.1.3.6.1.2.1.25.2.3.1.6.7&.1.3.6.1.2.1.25.2.3.1.5.7:SER3@192.168.1.12 *
.1.3.6.1.2.1.25.2.3.1.4.7&.1.3.6.1.2.1.25.2.3.1.4.7:SER3@192.168.1.12 * 1000 / 1048576
PageTop[192.168.1.12_mem]: <H1>Memoria libre--SER3</H1>
Options[192.168.1.12_mem]: nopercent,gauge,growright
Title[192.168.1.12_mem]: Memoria libre--SER3
MaxBytes[192.168.1.12_mem]: 100000000000000
YLegend[192.168.1.12_mem]: bytes
ShortLegend[192.168.1.12_mem]: bytes
LegendI[192.168.1.12_mem]: Memoria en uso
LegendO[192.168.1.12_mem]: Memoria total


###Temperatura procesadores#######
Target[192.168.1.3_tem-proc-in]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.100&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.101:SER3@192.168.1.3
PageTop[192.168.1.3_tem-proc-in]: <H1>Temperatura de los procesadores--SER3</H1>
Options[192.168.1.3_tem-proc-in]: gauge,nopercent,growright
Title[192.168.1.3_tem-proc-in]: Temperaturas de procesadores--SER3
MaxBytes[192.168.1.3_tem-proc-in]: 50
YLegend[192.168.1.3_tem-proc-in]: grados
LegendI[192.168.1.3_tem-proc-in]: Temperatura del procesador 1
LegendO[192.168.1.3_tem-proc-in]:Temperatura del procesador 2
ShortLegend[192.168.1.3_tem-proc-in]: Â°



###Interface 10 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S
Aceleracion' | Name: 'ethernet_6' | Ip: '' | Eth: '00-1e-68-57-71-be' ###

Target[192.168.1.12_10]: 10:SER3@192.168.1.12:
SetEnv[192.168.1.12_10]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S "
Options[192.168.1.12_10]: growright,nopercent
MaxBytes[192.168.1.12_10]: 125000000
Title[192.168.1.12_10]: Análisis de trafico eth6 (ID10) -- SER3
PageTop[192.168.1.12_10]: <h1>Análisis de trafico eth6 (ID10) -- SER3</h1>
     <div id="sysdetails">
     <table>
           <tr>
               <td>Sistema:</td>
```

```
            <td>SER3</td>
          </tr>
          <tr>
            <td>Administrador:</td>
            <td>Elizabeth</td>
          </tr>
          <tr>
            <td>Descripcion:</td>
            <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S </td>
          </tr>
          <tr>
            <td>Tipo de interfaz:</td>
            <td>ethernetCsmacd (6)</td>
          </tr>
          <tr>
            <td>Nombre de interfaz:</td>
             <td>ethernet_6</td>
           </tr>
           <tr>
             <td>Velocidad Maxima:</td>
             <td>125.0 MBytes/s</td>
           </tr>
        </table>
        </div>


### Interface 11 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S -#2' |
Name: 'ethernet_8' | Ip: '' | Eth: '00-1e-68-57-71-bf' ###

Target[192.168.1.12_11]: 11:SER3@192.168.1.12:
SetEnv[192.168.1.12_11]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S -#2"
Options[192.168.1.12_11]: growright,nopercent
MaxBytes[192.168.1.12_11]: 125000000
Title[192.168.1.12_11]: Análisis de trafico eth8 (ID11) -- SER3
PageTop[192.168.1.12_11]: <h1>Análisis de trafico eth8 (ID11) -- SER3</h1>
     <div id="sysdetails">
          <table>
               <tr>
                   <td>Sistema:</td>
                   <td>SER3</td>
               </tr>
               <tr>
                   <td>Administrador:</td>
                   <td>Elizabeth</td>
               </tr>
               <tr>
                    <td>Descripcion:</td>
                    <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S -#2  </td>
               </tr>
               <tr>
                     <td>Tipo de interfaz:</td>
                     <td>ethernetCsmacd (6)</td>
               </tr>
               <tr>
                     <td>Nombre de interfaz:</td>
                     <td>Ethernet 8</td>
               </tr>
               <tr>
                     <td>Velocidad Maxima:</td>
                     <td>125.0 MBytes/s</td>
               </tr>
          </table>
        </div>

### Interface 12 >> Descr: 'Puente MAC' | Name: 'ethernet_10' | Ip: '192.168.1.12' | Eth: ''
###

Target[192.168.1.12_12]: 12:SER3@192.168.1.12:
SetEnv[192.168.1.12_12]: MRTG_INT_IP="192.168.1.12" MRTG_INT_DESCR="Puente MAC"
Options[192.168.1.12_12]: growright,nopercent
MaxBytes[192.168.1.12_12]: 125000000
Title[192.168.1.12_12]: Análisis de trafico eth10 (ID12) -- SER3
PageTop[192.168.1.12_12]: <h1>Análisis de trafico eth10 (ID12) -- SER3</h1>
        <div id="sysdetails">
             <table>
                    <tr>
```

```
                    <td>Sistema:</td>
                    <td>SER3</td>
                </tr>
                <tr>
                    <td>Administrador:</td>
                    <td>Elizabeth</td>
                </tr>
                <tr>
                    <td>Descripcion:</td>
                    <td>Puente MAC </td>
                </tr>
                <tr>
                    <td>Tipo de interfaz:</td>
                    <td>ethernetCsmacd (6)</td>
                </tr>
                <tr>
                    <td>Nombre de interfaz:</td>
                    <td>Ethernet 10</td>
                </tr>
                <tr>
                    <td>Velocidad maxima:</td>
                    <td>125.0 MBytes/s</td>
                </tr>
                <tr>
                     <td>Ip:</td>
                     <td>192.168.1.12 ()</td>
                </tr>
           </table>
        </div>

######################################################################
# System: SER4
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 #AT/AT COMPATIBLE - Software:
Windows Version 6.0 (Build 6002 #Multiprocessor Free)
######################################################################

Target[192.168.1.13_cpu]: (
.1.3.6.1.2.1.25.3.3.1.2.2&.1.3.6.1.2.1.25.3.3.1.2.2:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.3&.1.3.6.1.2.1.25.3.3.1.2.3:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.4&.1.3.6.1.2.1.25.3.3.1.2.4:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.5&.1.3.6.1.2.1.25.3.3.1.2.5:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.6&.1.3.6.1.2.1.25.3.3.1.2.6:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.7&.1.3.6.1.2.1.25.3.3.1.2.7:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.8&.1.3.6.1.2.1.25.3.3.1.2.8:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.9&.1.3.6.1.2.1.25.3.3.1.2.9:SER4@192.168.1.13) / (8)
MaxBytes[192.168.1.13_cpu]: 100
Title[192.168.1.13_cpu]: Carga CPU--SER4
PageTop[192.168.1.13_cpu]: <H1>Carga Activa CPU %--SER4</H1>
ShortLegend[192.168.1.13_cpu]: %
YLegend[192.168.1.13_cpu]: Carga CPU
Legend1[192.168.1.13_cpu]: CPU activa %
Legend2[192.168.1.13_cpu]:
Legend3[192.168.1.13_cpu]:
Legend4[192.168.1.13_cpu]:
LegendI[192.168.1.13_cpu]: Active
LegendO[192.168.1.13_cpu]:
Options[192.168.1.13_cpu]: growright,nopercent,gauge

######Monitoreo de memoria######
Target[192.168.1.13_mem]:
.1.3.6.1.2.1.25.2.3.1.6.5&.1.3.6.1.2.1.25.2.3.1.5.5:SER4@192.168.1.13 *
.1.3.6.1.2.1.25.2.3.1.4.5&.1.3.6.1.2.1.25.2.3.1.4.5:SER4@192.168.1.13 * 1000 / 1048576
PageTop[192.168.1.13_mem]: <H1>Memoria libre--SER4</H1>
Options[192.168.1.13_mem]: nopercent,gauge,growright
Title[192.168.1.13_mem]: Memoria libre--SER4
MaxBytes[192.168.1.13_mem]: 100000000000000
YLegend[192.168.1.13_mem]: bytes
ShortLegend[192.168.1.13_mem]: bytes

LegendI[192.168.1.13_mem]: Memoria en uso
LegendO[192.168.1.13_mem]: Memoria total
Legend1[192.168.1.13_mem]: Memoria en uso, no incluye swap, en bytes

#####Trafico web de SER4###########
Target[192.168.1.13_web]:
1.3.6.1.4.1.311.1.7.3.1.2.0&1.3.6.1.4.1.311.1.7.3.1.4.0:SER4@192.168.1.13
PageTop[192.168.1.13_web]: <H1>Trafico web--SER4</H1>
```

```
Options[192.168.1.13_web]: growright,nopercent
Title[192.168.1.13_web]: Trafico web--SER4
MaxBytes[192.168.1.13_web]: 125000000


###Temperatura procesador 1#######
Target[192.168.1.4_tem-proc-1]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.136&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.137:SER4@192.168.1.4
PageTop[192.168.1.4_tem-proc-1]: <H1>Temperatura de los procesadores--SER4</H1>
Options[192.168.1.4_tem-proc-1]: gauge,nopercent,growright
Title[192.168.1.4_tem-proc-1]: Temperaturas de procesadores--SER4
MaxBytes[192.168.1.4_tem-proc-1]: 50
YLegend[192.168.1.4_tem-proc-1]: grados
LegendI[192.168.1.4_tem-proc-1]: Temperatura del procesador 1
LegendO[192.168.1.4_tem-proc-1]:Temperatura del procesador 2
ShortLegend[192.168.1.4_tem-proc-1]: Â°


### Interface 11 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S' | Name:
'ethernet 6' | Ip: '' | Eth: '00-26-9e-9b-f6-78' ###

Target[192.168.1.13_11]: 11:SER4@192.168.1.13:
SetEnv[192.168.1.13_11]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S"
Options[192.168.1.13_11]: growright,nopercent
MaxBytes[192.168.1.13_11]: 125000000
Title[192.168.1.13_11]: Analisis de trafico eth6 (ID11) -- SER4
PageTop[192.168.1.13_11]: <h1>Analisis de trafico eth6 (ID11) -- SER4</h1>
              <div id="sysdetails">
                     <table>
                            <tr>
                                   <td>Sistema:</td>
                                   <td>SER4</td>
                            </tr>
                            <tr>
                                   <td>Administrador:</td>
                                   <td>CENAPRED</td>
                            </tr>
                            <tr>
                                   <td>Descripcion:</td>
                                   <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S  </td>
                            </tr>
                            <tr>
                                   <td>Tipo de interfaz:</td>
                                   <td>ethernetCsmacd (6)</td>
                            </tr>
                            <tr>
                                   <td>Nombre de interfaz:</td>
                                   <td>Ethernet 6</td>
                            </tr>
                            <tr>
                                   <td>Velocidad maxima:</td>
                                   <td>125.0 MBytes/s</td>
                            </tr>
                     </table>
              </div>


### Interface 12 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S  -#2' |
Name: 'ethernet_8' | Ip: '' | Eth: '00-26-9e-9b-f6-79' ###

Target[192.168.1.13_12]: 12:SER4@192.168.1.13:
SetEnv[192.168.1.13_12]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S  -#2"
Options[192.168.1.13_12]: growright,nopercent
MaxBytes[192.168.1.13_12]: 125000000
Title[192.168.1.13_12]: Analisis de trafico eth8 (ID12) -- SER4
PageTop[192.168.1.13_12]: <h1>Analisis de trafico eth8 (ID12) -- SER4</h1>
              <div id="sysdetails">
                     <table>
                            <tr>
                                   <td>Sistema:</td>
                                   <td>SER4</td>
                            </tr>
                            <tr>
                                   <td>Administrador:</td>
```

```
                                        <td>CENAPRED</td>
                                </tr>
                                <tr>
                                        <td>Descripcion:</td>
                                        <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S  -#2  </td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>Ethernet 8</td>
                                </tr>
                                <tr>
                                        <td>Velocidad maxima:</td>
                                        <td>125.0 MBytes/s</td>
                                </tr>
                        </table>
                </div>


### Interface 13 >> Descr: 'Puente MAC' | Name: 'ethernet_10' | Ip: '192.168.1.13' | Eth: ''
###

Target[192.168.1.13_13]: 13:SER4@192.168.1.13:
SetEnv[192.168.1.13_13]: MRTG_INT_IP="192.168.1.13" MRTG_INT_DESCR="Puente MAC"
Options[192.168.1.13_13]: growright,nopercent
MaxBytes[192.168.1.13_13]: 125000000
Title[192.168.1.13_13]: Analisis de trafico eth10 (ID13) -- SER4
PageTop[192.168.1.13_13]: <h1>Analisis de trafico eth10 (ID13)-- SER4</h1>
                <div id="sysdetails">
                        <table>
                                <tr>
                                        <td>Sistema:</td>
                                        <td>SER4</td>
                                </tr>
                                <tr>
                                        <td>Administrador:</td>
                                        <td>CENAPRED</td>
                                </tr>
                                <tr>
                                        <td>Descripcion:</td>
                                        <td>Puente MAC</td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>Ethernet 10</td>
                                </tr>
                                <tr>
                                        <td>Velocidad maxima:</td>
                                        <td>125.0 MBytes/s</td>
                                </tr>
                                <tr>
                                        <td>Ip:</td>
                                        <td>192.168.1.13 ()</td>
                                </tr>
                        </table>
                </div>
```

Anexo 11. Archivo de configuración mrtg1.cfg OpenSuse

```
### Global Defaults
#  to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits

EnableIPv6: no
```

```
######################################################################
# System: SER1
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 AT/AT COMPATIBLE - Software:
Windows Version 6.0 (Build 6002 Multiprocessor Free)
# Contact: root
# Location: Cenapred
######################################################################

#####Grafica del rendimiento del CPU#####
Target[192.168.1.10_cpu]: (
.1.3.6.1.2.1.25.3.3.1.2.2&.1.3.6.1.2.1.25.3.3.1.2.2:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.3&.1.3.6.1.2.1.25.3.3.1.2.3:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.4&.1.3.6.1.2.1.25.3.3.1.2.4:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.5&.1.3.6.1.2.1.25.3.3.1.2.5:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.6&.1.3.6.1.2.1.25.3.3.1.2.6:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.7&.1.3.6.1.2.1.25.3.3.1.2.7:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.8&.1.3.6.1.2.1.25.3.3.1.2.8:SER1@192.168.1.10 +
.1.3.6.1.2.1.25.3.3.1.2.9&.1.3.6.1.2.1.25.3.3.1.2.9:SER1@192.168.1.10) / (8)
MaxBytes[192.168.1.10_cpu]: 100
Title[192.168.1.10_cpu]: Carga CPU--SER1
PageTop[192.168.1.10_cpu]: <H1>Carga Activa CPU %--SER1</H1>
ShortLegend[192.168.1.10_cpu]: %
YLegend[192.168.1.10_cpu]: Carga CPU
Legend1[192.168.1.10_cpu]: CPU activa %
Legend2[192.168.1.10_cpu]:
Legend3[192.168.1.10_cpu]:
Legend4[192.168.1.10_cpu]:
LegendI[192.168.1.10_cpu]: Active
LegendO[192.168.1.10_cpu]:
Options[192.168.1.10_cpu]: growright,nopercent,gauge

######Monitoreo de memoria######
Target[192.168.1.10_mem]:
.1.3.6.1.2.1.25.2.3.1.6.5&.1.3.6.1.2.1.25.2.3.1.5.5:SER1@192.168.1.10 *
.1.3.6.1.2.1.25.2.3.1.4.5&.1.3.6.1.2.1.25.2.3.1.4.5:SER1@192.168.1.10 * 1000 / 1048576
PageTop[192.168.1.10_mem]: <H1>Memoria libre--SER1</H1>
Options[192.168.1.10_mem]: nopercent,gauge,growright
Title[192.168.1.10_mem]: Memoria libre--SER1
MaxBytes[192.168.1.10_mem]: 100000000000000
YLegend[192.168.1.10_mem]: bytes
ShortLegend[192.168.1.10_mem]: bytes
LegendI[192.168.1.10_mem]: Memoria en uso
LegendO[192.168.1.10_mem]: Memoria total



###Temperatura procesadores#######
Target[192.168.1.1_tem-proc-im]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.124&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.125:SER1@192.168.1.1
PageTop[192.168.1.1_tem-proc-im]: <H1>Temperatura de los procesadores--SER1</H1>
Options[192.168.1.1_tem-proc-im]: gauge,nopercent,growright
Title[192.168.1.1_tem-proc-im]: Temperaturas de procesadores--SER1
MaxBytes[192.168.1.1_tem-proc-im]: 50
YLegend[192.168.1.1_tem-proc-im]: grados
LegendI[192.168.1.1_tem-proc-im]: Temperatura del procesador 1
LegendO[192.168.1.1_tem-proc-im]:Temperatura del procesador 2
ShortLegend[192.168.1.1_tem-proc-im]: Â°


### Interface 10 >> Descr: 'Intel(R)-PRO/1000-EB-Network-Connection-with-I/O-Acceleration' |
Name: 'ethernet_6' | Ip: '' | Eth: '30-78-30-30-32-33-38-62-31-37-61-37-33-34' ###

Target[192.168.1.10_10]: 10:SER1@192.168.1.10:
SetEnv[192.168.1.10_10]: MRTG_INT_IP="" MRTG_INT_DESCR="Intel(R)-PRO/1000-EB-Network-
Connection-with-I/O-Acceleration"
MaxBytes[192.168.1.10_10]: 125000000
Title[192.168.1.10_10]: Analisis de trafico eth6 (ID 10) -- SER1
PageTop[192.168.1.10_10]: <h1>Analisis de trafico eth6 (ID 10) -- SER1</h1>
       <div id="sysdetails">
             <table>
                  <tr>
                      <td>Sistema:</td>
                      <td>SER1</td>
                  </tr>
                  <tr>
                        <td>Administrador:</td>
                        <td>Elizabeth Rubio</td>
```

```
                    </tr>
                    <tr>
                        <td>Descripcion:</td>
                        <td>Intel(R)-PRO/1000-EB-Conexion de red con Aceleracion E/S  </td>
                    </tr>
                    <tr>
                         <td>Tipo de interfaz:</td>
                         <td>ethernetCsmacd (6)</td>
                    </tr>
                    <tr>
                         <td>Nombre de interfaz:</td>
                         <td>ethernet 6</td>
                    </tr>
                    <tr>
                         <td>Velocidad Maxima:</td>
                         <td>125.0 MBytes/s</td>
                    </tr>
                </table>
            </div>


### Interface 11 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S -#2' |
Name: 'ethernet 8' | Ip: '' | Eth: '00-23-8b-17-a7-35' ###

Target[192.168.1.10_11]: 11:SER1@192.168.1.10:
SetEnv[192.168.1.10_11]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S -#2"
Options[192.168.1.10_11]: growright,nopercent
MaxBytes[192.168.1.10_11]: 125000000
Title[192.168.1.10_11]: Análisis de trafico de eth8 (ID11) -- SER1
PageTop[192.168.1.10_11]: <h1>Análisis de trafico de eth8 (ID11) -- SER1</h1>
              <div id="sysdetails">
                     <table>
                            <tr>
                                   <td>Sistema:</td>
                                   <td>SER1</td>
                            </tr>
                            <tr>
                                   <td>Administrador:</td>
                                   <td>Elizabeth</td>
                            </tr>
                            <tr>
                                   <td>Descripción:</td>
                                   <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S -#2  </td>
                            </tr>
                            <tr>
                                   <td>Tipo de interfaz:</td>
                                   <td>ethernetCsmacd (6)</td>
                            </tr>
                            <tr>
                                   <td>Nombre de interfaz:</td>
                                   <td>Ethernet 8</td>
                            </tr>
                            <tr>
                                   <td>Velocidad Maxima:</td>
                                   <td>125.0 MBytes/s</td>
                            </tr>
                     </table>
              </div>


### Interface 12 >> Descr: 'Puente MAC' | Name: 'ethernet_10' | Ip: '192.168.1.10' | Eth: ''
###

Target[192.168.1.10_12]: 12:SER1@192.168.1.10:
SetEnv[192.168.1.10_12]: MRTG_INT_IP="192.168.1.10" MRTG_INT_DESCR="Puente MAC"
MaxBytes[192.168.1.10_12]: 125000000
Options[192.168.1.10_12]: growright,nopercent
Title[192.168.1.10_12]: Análisis de trafico eth10 (ID12) -- SER1
PageTop[192.168.1.10_12]: <h1>Análisis de tráfico (ID12) -- SER1</h1>
              <div id="sysdetails">
                     <table>
                            <tr>
                                   <td>Sistema:</td>
                                   <td>SER1</td>
                            </tr>
```

```
                        <tr>
                                <td>Administrador:</td>
                                <td>Elizabeth</td>
                        </tr>
                        <tr>
                                <td>Descripcion:</td>
                                <td>Puente MAC  </td>
                        </tr>
                        <tr>
                                <td>Tipo de interfaz:</td>
                                <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                                <td>Nombre de interfaz:</td>
                                <td>ethernet_10</td>
                        </tr>
                        <tr>
                                <td>Velocidad Maxima:</td>
                                <td>125.0 MBytes/s</td>
                        </tr>
                        <tr>
                                <td>Ip:</td>
                                <td>192.168.1.10 ()</td>
                        </tr>
                </table>
        </div>
```

Anexo 12. Archivo de configuración mrtg2.cfg OpenSuse

```
WorkDir: /srv/www/htdocs/mrtg
Language: spanish
EnableIPv6: no

######################################################################
# System: SER2
# Description: Linux SER2 2.6.18-53.el5xen #1 SMP Wed Oct 10 17:06:12 EDT 2007 i686
# Contact: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
# Location: Unknown (edit /etc/snmp/snmpd.conf)
######################################################################



#####Grafica del rendimiento del CPU#####

Target[192.168.1.11_cpu]: (
.1.3.6.1.2.1.25.3.3.1.2.768&.1.3.6.1.2.1.25.3.3.1.2.768:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.769&.1.3.6.1.2.1.25.3.3.1.2.769:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.770&.1.3.6.1.2.1.25.3.3.1.2.770:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.771&.1.3.6.1.2.1.25.3.3.1.2.771:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.772&.1.3.6.1.2.1.25.3.3.1.2.772:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.773&.1.3.6.1.2.1.25.3.3.1.2.773:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.774&.1.3.6.1.2.1.25.3.3.1.2.774:SER2@192.168.1.11 +
.1.3.6.1.2.1.25.3.3.1.2.775&.1.3.6.1.2.1.25.3.3.1.2.775:SER2@192.168.1.11) / (8)
MaxBytes[192.168.1.11_cpu]: 100
Title[192.168.1.11_cpu]: Carga CPU--SER2
PageTop[192.168.1.11_cpu]: <H1>Carga Activa CPU %--SER2</H1>
ShortLegend[192.168.1.11_cpu]: %
YLegend[192.168.1.11_cpu]: Carga CPU
Legend1[192.168.1.11_cpu]: CPU activa %
Legend2[192.168.1.11_cpu]:
Legend3[192.168.1.11_cpu]:
Legend4[192.168.1.11_cpu]:
LegendI[192.168.1.11_cpu]: Active
LegendO[192.168.1.11_cpu]:
Options[192.168.1.11_cpu]: growright,nopercent,gauge


######Monitoreo de memoria######
Target[192.168.1.11_mem]:
.1.3.6.1.2.1.25.2.3.1.6.2&.1.3.6.1.2.1.25.2.3.1.5.2:SER2@192.168.1.11 *
.1.3.6.1.2.1.25.2.3.1.4.2&.1.3.6.1.2.1.25.2.3.1.4.2:SER2@192.168.1.11 * 1000 / 1048576
PageTop[192.168.1.11_mem]: <H1>Memoria libre--SER2</H1>
Options[192.168.1.11_mem]: nopercent,gauge,growright
Title[192.168.1.11_mem]: Memoria libre--SER2
```

```
MaxBytes[192.168.1.11_mem]: 100000000000000
YLegend[192.168.1.11_mem]: bytes
ShortLegend[192.168.1.11_mem]: bytes
LegendI[192.168.1.11_mem]: Memoria en uso
LegendO[192.168.1.11_mem]: Memoria total
Legend1[192.168.1.11_mem]: Memoria en uso, no incluye swap, en bytes


###Temperatura procesadores#######
Target[192.168.1.2_tem-proc-at]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.124&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.125:SER2@192.168.1.2
PageTop[192.168.1.2_tem-proc-at]: <H1>Temperatura de los procesadores--SER2</H1>
Options[192.168.1.2_tem-proc-at]: gauge,nopercent,growright
Title[192.168.1.2_tem-proc-at]: Temperaturas de procesadores--SER2
YLegend[192.168.1.2_tem-proc-at]: grados
MaxBytes[192.168.1.2_tem-proc-at]: 50
LegendI[192.168.1.2_tem-proc-at]: Temperatura del procesador 1
LegendO[192.168.1.2_tem-proc-at]: Temperatura del procesador 2
ShortLegend[192.168.1.2_tem-proc-at]: Â°


### Interface 3 >> Descr: 'eth1' | Name: 'eth1' | Ip: '' | Eth: '' ###

Target[192.168.1.11_3]: 3:SER2@192.168.1.11:
SetEnv[192.168.1.11_3]: MRTG_INT_IP="" MRTG_INT_DESCR="eth1"
Options[192.168.1.11_3]: growright,nopercent
MaxBytes[192.168.1.11_3]: 125000000
Title[192.168.1.11_3]: Análisis de trafico eth1 SER2
PageTop[192.168.1.11_3]: <h1>Análisis de trafico eth1 -- SER2</h1>
               <div id="sysdetails">
                      <table>
                             <tr>
                                    <td>Sistema:</td>
                                    <td>SER2</td>
                             </tr>
                             <tr>
                                    <td>Administrador:</td>
                                    <td>Elizabeth; (configure /etc/snmp/snmp.local.conf)</td>
                             </tr>
                             <tr>
                                    <td>Descripcion:</td>
                                    <td>eth1  </td>
                             </tr>
                             <tr>
                                    <td>Tipo de interfaz:</td>
                                    <td>ethernetCsmacd (6)</td>
                             </tr>
                             <tr>
                                    <td>Mombre de la interfaz:</td>
                                    <td>eth1</td>
                             </tr>
                             <tr>
                                    <td>Velocidad Maxima:</td>
                                    <td>125.0 MBytes/s</td>
                             </tr>
                      </table>
               </div>

### Interface 5 >> Descr: 'bond0' | Name: 'bond0' | Ip: '192.168.1.11' | Eth: '' ###

Target[192.168.1.11_5]: 5:SER2@192.168.1.11:
SetEnv[192.168.1.11_5]: MRTG_INT_IP="192.168.1.11" MRTG_INT_DESCR="bond0"
Options[192.168.1.11_5]: growright,nopercent
MaxBytes[192.168.1.11_5]: 1250000
Title[192.168.1.11_5]: Análisis de trafico bond0 -- SER2
PageTop[192.168.1.11_5]: <h1>Análisis de trafico bond0 -- SER2</h1>
               <div id="sysdetails">
                      <table>
                             <tr>
                                    <td>Sistema:</td>
                                    <td>SER2</td>
                             </tr>
                             <tr>
                                    <td>Administrador:</td>
                                    <td>Elizabeth</td>
                             </tr>
                             <tr>
```

```
                                        <td>Descripcion:</td>
                                        <td>bond0  </td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>bond0</td>
                                </tr>
                                <tr>
                                        <td>Velocidad Maxima:</td>
                                        <td>1250.0 kBytes/s</td>
                                </tr>
                                <tr>
                                        <td>Ip:</td>
                                        <td>192.168.1.11 (www.SER2nacionalderiesgos.gob.mx)</td>
                                </tr>
                        </table>
                </div>

### Interface 8 >> Descr: 'eth0' | Name: 'eth0' | Ip: '' | Eth: '' ###

Target[192.168.1.11_8]: 8:SER2@192.168.1.11:
SetEnv[192.168.1.11_8]: MRTG_INT_IP="" MRTG_INT_DESCR="eth0"
Options[192.168.1.11_8]: growright,nopercent
MaxBytes[192.168.1.11_8]: 1250000
Title[192.168.1.11_8]: Análisis de trafico de th0 -- SER2
PageTop[192.168.1.11_8]: <h1>Análisis de trafico de th0 -- SER2</h1>
                <div id="sysdetails">
                        <table>
                                <tr>
                                        <td>Sistema:</td>
                                        <td>SER2</td>
                                </tr>
                                <tr>
                                        <td>Administradorr:</td>
                                        <td>Elizabeth</td>
                                </tr>
                                <tr>
                                        <td>Descripcion:</td>
                                        <td>eth0  </td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>eth0</td>
                                </tr>
                                <tr>
                                        <td>Velocidad Maxima:</td>
                                        <td>1250.0 kBytes/s</td>
                                </tr>
                        </table>
                </div>
```

Anexo 13. Archivo de configuración mrtg3.cfg OpenSuse

```
EnableIPv6: no
WorkDir: /srv/www/htdocs/mrtg
Language: spanish

######################################################################
#System: SER3
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 AT/AT COMPATIBLE - Software:
Windows Version 6.0 (Build 6002 Multiprocessor Free)
######################################################################



#####Grafica del rendimiento del CPU#####
```

```
Target[192.168.1.12_cpu]: (
.1.3.6.1.2.1.25.3.3.1.2.2&.1.3.6.1.2.1.25.3.3.1.2.2:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.3&.1.3.6.1.2.1.25.3.3.1.2.3:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.4&.1.3.6.1.2.1.25.3.3.1.2.4:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.5&.1.3.6.1.2.1.25.3.3.1.2.5:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.6&.1.3.6.1.2.1.25.3.3.1.2.6:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.7&.1.3.6.1.2.1.25.3.3.1.2.7:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.8&.1.3.6.1.2.1.25.3.3.1.2.8:SER3@192.168.1.12 +
.1.3.6.1.2.1.25.3.3.1.2.9&.1.3.6.1.2.1.25.3.3.1.2.9:SER3@192.168.1.12) / (8)
MaxBytes[192.168.1.12_cpu]: 100
Title[192.168.1.12_cpu]: Carga CPU--SER3
PageTop[192.168.1.12_cpu]: <H1>Carga Activa CPU %--SER3</H1>
ShortLegend[192.168.1.12_cpu]: %
YLegend[192.168.1.12_cpu]: Carga CPU
Legend1[192.168.1.12_cpu]: CPU activa %
Legend2[192.168.1.12_cpu]:
Legend3[192.168.1.12_cpu]:
Legend4[192.168.1.12_cpu]:
LegendI[192.168.1.12_cpu]: Active
LegendO[192.168.1.12_cpu]:
Options[192.168.1.12_cpu]: growright,nopercent,gauge

######Monitoreo de memoria######
Target[192.168.1.12_mem]:
.1.3.6.1.2.1.25.2.3.1.6.7&.1.3.6.1.2.1.25.2.3.1.5.7:SER3@192.168.1.12 *
.1.3.6.1.2.1.25.2.3.1.4.7&.1.3.6.1.2.1.25.2.3.1.4.7:SER3@192.168.1.12 * 1000 / 1048576
PageTop[192.168.1.12_mem]: <H1>Memoria libre--SER3</H1>
Options[192.168.1.12_mem]: nopercent,gauge,growright
Title[192.168.1.12_mem]: Memoria libre--SER3
MaxBytes[192.168.1.12_mem]: 100000000000000
YLegend[192.168.1.12_mem]: bytes
ShortLegend[192.168.1.12_mem]: bytes
LegendI[192.168.1.12_mem]: Memoria en uso
LegendO[192.168.1.12_mem]: Memoria total


###Temperatura procesadores#######
Target[192.168.1.3_tem-proc-in]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.100&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.101:SER3@192.168.1.3
PageTop[192.168.1.3_tem-proc-in]: <H1>Temperatura de los procesadores--SER3</H1>
Options[192.168.1.3_tem-proc-in]: gauge,nopercent,growright
Title[192.168.1.3_tem-proc-in]: Temperaturas de procesadores--SER3
MaxBytes[192.168.1.3_tem-proc-in]: 50
YLegend[192.168.1.3_tem-proc-in]: grados
LegendI[192.168.1.3_tem-proc-in]: Temperatura del procesador 1
LegendO[192.168.1.3_tem-proc-in]:Temperatura del procesador 2
ShortLegend[192.168.1.3_tem-proc-in]: Â°



###Interface 10 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S
Aceleracion' | Name: 'ethernet_6' | Ip: '' | Eth: '00-1e-68-57-71-be' ###

Target[192.168.1.12_10]: 10:SER3@192.168.1.12:
SetEnv[192.168.1.12_10]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S "
Options[192.168.1.12_10]: growright,nopercent
MaxBytes[192.168.1.12_10]: 125000000
Title[192.168.1.12_10]: Análisis de trafico eth6 (ID10) -- SER3
PageTop[192.168.1.12_10]: <h1>Análisis de trafico eth6 (ID10) -- SER3</h1>
     <div id="sysdetails">
     <table>
           <tr>
               <td>Sistema:</td>
               <td>SER3</td>
           </tr>
           <tr>
               <td>Administrador:</td>
               <td>Elizabeth</td>
           </tr>
           <tr>
               <td>Descripcion:</td>
               <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S </td>
           </tr>
           <tr>
               <td>Tipo de interfaz:</td>
```

```
            <td>ethernetCsmacd (6)</td>
          </tr>
          <tr>
              <td>Nombre de interfaz:</td>
               <td>ethernet_6</td>
           </tr>
           <tr>
               <td>Velocidad Maxima:</td>
               <td>125.0 MBytes/s</td>
           </tr>
        </table>
        </div>


### Interface 11 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S -#2' |
Name: 'ethernet_8' | Ip: '' | Eth: '00-1e-68-57-71-bf' ###

Target[192.168.1.12_11]: 11:SER3@192.168.1.12:
SetEnv[192.168.1.12_11]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S -#2"
Options[192.168.1.12_11]: growright,nopercent
MaxBytes[192.168.1.12_11]: 125000000
Title[192.168.1.12_11]: Análisis de trafico eth8 (ID11) -- SER3
PageTop[192.168.1.12_11]: <h1>Análisis de trafico eth8 (ID11) -- SER3</h1>
     <div id="sysdetails">
          <table>
                <tr>
                    <td>Sistema:</td>
                    <td>SER3</td>
                </tr>
                <tr>
                    <td>Administrador:</td>
                    <td>Elizabeth</td>
                </tr>
                <tr>
                     <td>Descripcion:</td>
                     <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S -#2  </td>
                </tr>
                <tr>
                      <td>Tipo de interfaz:</td>
                      <td>ethernetCsmacd (6)</td>
                </tr>
                <tr>
                      <td>Nombre de interfaz:</td>
                      <td>Ethernet 8</td>
                </tr>
                <tr>
                      <td>Velocidad Maxima:</td>
                      <td>125.0 MBytes/s</td>
                </tr>
          </table>
        </div>

### Interface 12 >> Descr: 'Puente MAC' | Name: 'ethernet_10' | Ip: '192.168.1.12' | Eth: ''
###

Target[192.168.1.12_12]: 12:SER3@192.168.1.12:
SetEnv[192.168.1.12_12]: MRTG_INT_IP="192.168.1.12" MRTG_INT_DESCR="Puente MAC"
Options[192.168.1.12_12]: growright,nopercent
MaxBytes[192.168.1.12_12]: 125000000
Title[192.168.1.12_12]: Análisis de trafico eth10 (ID12) -- SER3
PageTop[192.168.1.12_12]: <h1>Análisis de trafico eth10 (ID12) -- SER3</h1>
        <div id="sysdetails">
             <table>
                   <tr>
                       <td>Sistema:</td>
                       <td>SER3</td>
                   </tr>
                   <tr>
                       <td>Administrador:</td>
                       <td>Elizabeth</td>
                   </tr>
                   <tr>
                       <td>Descripcion:</td>
                       <td>Puente MAC </td>
                   </tr>
                   <tr>
```

```
                    <td>Tipo de interfaz:</td>
                    <td>ethernetCsmacd (6)</td>
                </tr>
                <tr>
                    <td>Nombre de interfaz:</td>
                    <td>Ethernet 10</td>
                </tr>
                <tr>
                    <td>Velocidad maxima:</td>
                    <td>125.0 MBytes/s</td>
                </tr>
                <tr>
                     <td>Ip:</td>
                     <td>192.168.1.12 ()</td>
                </tr>
            </table>
        </div>
```

Anexo 14. Archivo de configuración mrtg4.cfg OpenSuse

```
EnableIPv6: no
WorkDir: /srv/www/htdocs/mrtg
Language: spanish

######################################################################
# System: SER4
# Description: Hardware: Intel64 Family 6 Model 23 Stepping 10 #AT/AT COMPATIBLE - Software:
Windows Version 6.0 (Build 6002 #Multiprocessor Free)
######################################################################

Target[192.168.1.13_cpu]: (
.1.3.6.1.2.1.25.3.3.1.2.2&.1.3.6.1.2.1.25.3.3.1.2.2:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.3&.1.3.6.1.2.1.25.3.3.1.2.3:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.4&.1.3.6.1.2.1.25.3.3.1.2.4:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.5&.1.3.6.1.2.1.25.3.3.1.2.5:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.6&.1.3.6.1.2.1.25.3.3.1.2.6:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.7&.1.3.6.1.2.1.25.3.3.1.2.7:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.8&.1.3.6.1.2.1.25.3.3.1.2.8:SER4@192.168.1.13 +
.1.3.6.1.2.1.25.3.3.1.2.9&.1.3.6.1.2.1.25.3.3.1.2.9:SER4@192.168.1.13) / (8)
MaxBytes[192.168.1.13_cpu]: 100
Title[192.168.1.13_cpu]: Carga CPU--SER4
PageTop[192.168.1.13_cpu]: <H1>Carga Activa CPU %--SER4</H1>
ShortLegend[192.168.1.13_cpu]: %
YLegend[192.168.1.13_cpu]: Carga CPU
Legend1[192.168.1.13_cpu]: CPU activa %
Legend2[192.168.1.13_cpu]:
Legend3[192.168.1.13_cpu]:
Legend4[192.168.1.13_cpu]:
LegendI[192.168.1.13_cpu]: Active
LegendO[192.168.1.13_cpu]:
Options[192.168.1.13_cpu]: growright,nopercent,gauge

######Monitoreo de memoria######
Target[192.168.1.13_mem]:
.1.3.6.1.2.1.25.2.3.1.6.5&.1.3.6.1.2.1.25.2.3.1.5.5:SER4@192.168.1.13 *
.1.3.6.1.2.1.25.2.3.1.4.5&.1.3.6.1.2.1.25.2.3.1.4.5:SER4@192.168.1.13 * 1000 / 1048576
PageTop[192.168.1.13_mem]: <H1>Memoria libre--SER4</H1>
Options[192.168.1.13_mem]: nopercent,gauge,growright
Title[192.168.1.13_mem]: Memoria libre--SER4
MaxBytes[192.168.1.13_mem]: 100000000000000
YLegend[192.168.1.13_mem]: bytes
ShortLegend[192.168.1.13_mem]: bytes

LegendI[192.168.1.13_mem]: Memoria en uso
LegendO[192.168.1.13_mem]: Memoria total
Legend1[192.168.1.13_mem]: Memoria en uso, no incluye swap, en bytes

#####Trafico web de SER4############
Target[192.168.1.13_web]:
1.3.6.1.4.1.311.1.7.3.1.2.0&1.3.6.1.4.1.311.1.7.3.1.4.0:SER4@192.168.1.13
PageTop[192.168.1.13_web]: <H1>Trafico web--SER4</H1>
Options[192.168.1.13_web]: growright,nopercent
Title[192.168.1.13_web]: Trafico web--SER4
MaxBytes[192.168.1.13_web]: 125000000
```

```
###Temperatura procesador 1#######
Target[192.168.1.4_tem-proc-1]:
1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.136&1.3.6.1.4.1.42.2.70.101.1.1.8.1.4.137:SER4@192.168.1.4
PageTop[192.168.1.4_tem-proc-1]: <H1>Temperatura de los procesadores--SER4</H1>
Options[192.168.1.4_tem-proc-1]: gauge,nopercent,growright
Title[192.168.1.4_tem-proc-1]: Temperaturas de procesadores--SER4
MaxBytes[192.168.1.4_tem-proc-1]: 50
YLegend[192.168.1.4_tem-proc-1]: grados
LegendI[192.168.1.4_tem-proc-1]: Temperatura del procesador 1
LegendO[192.168.1.4_tem-proc-1]:Temperatura del procesador 2
ShortLegend[192.168.1.4_tem-proc-1]: Â°


### Interface 11 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S' | Name:
'ethernet 6' | Ip: '' | Eth: '00-26-9e-9b-f6-78' ###

Target[192.168.1.13_11]: 11:SER4@192.168.1.13:
SetEnv[192.168.1.13_11]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S"
Options[192.168.1.13_11]: growright,nopercent
MaxBytes[192.168.1.13_11]: 125000000
Title[192.168.1.13_11]: Analisis de trafico eth6 (ID11) -- SER4
PageTop[192.168.1.13_11]: <h1>Analisis de trafico eth6 (ID11) -- SER4</h1>
               <div id="sysdetails">
                       <table>
                               <tr>
                                       <td>Sistema:</td>
                                       <td>SER4</td>
                               </tr>
                               <tr>
                                       <td>Administrador:</td>
                                       <td>CENAPRED</td>
                               </tr>
                               <tr>
                                       <td>Descripcion:</td>
                                       <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S  </td>
                               </tr>
                               <tr>
                                       <td>Tipo de interfaz:</td>
                                       <td>ethernetCsmacd (6)</td>
                               </tr>
                               <tr>
                                       <td>Nombre de interfaz:</td>
                                       <td>Ethernet 6</td>
                               </tr>
                               <tr>
                                       <td>Velocidad maxima:</td>
                                       <td>125.0 MBytes/s</td>
                               </tr>
                       </table>
               </div>


### Interface 12 >> Descr: ' Intel(R)-PRO/1000-EB-Conexión de red con Aceleración E/S  -#2' |
Name: 'ethernet_8' | Ip: '' | Eth: '00-26-9e-9b-f6-79' ###

Target[192.168.1.13_12]: 12:SER4@192.168.1.13:
SetEnv[192.168.1.13_12]: MRTG_INT_IP="" MRTG_INT_DESCR=" Intel(R)-PRO/1000-EB-Conexión de red
con Aceleración E/S  -#2"
Options[192.168.1.13_12]: growright,nopercent
MaxBytes[192.168.1.13_12]: 125000000
Title[192.168.1.13_12]: Analisis de trafico eth8 (ID12) -- SER4
PageTop[192.168.1.13_12]: <h1>Analisis de trafico eth8 (ID12) -- SER4</h1>
               <div id="sysdetails">
                       <table>
                               <tr>
                                       <td>Sistema:</td>
                                       <td>SER4</td>
                               </tr>
                               <tr>
                                       <td>Administrador:</td>
                                       <td>CENAPRED</td>
                               </tr>
                               <tr>
                                       <td>Descripcion:</td>
```

```
                                        <td> Intel(R)-PRO/1000-EB-Conexión de red con Aceleración
E/S  -#2  </td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>Ethernet 8</td>
                                </tr>
                                <tr>
                                        <td>Velocidad maxima:</td>
                                        <td>125.0 MBytes/s</td>
                                </tr>
                        </table>
                </div>


### Interface 13 >> Descr: 'Puente MAC' | Name: 'ethernet_10' | Ip: '192.168.1.13' | Eth: ''
###

Target[192.168.1.13_13]: 13:SER4@192.168.1.13:
SetEnv[192.168.1.13_13]: MRTG_INT_IP="192.168.1.13" MRTG_INT_DESCR="Puente MAC"
Options[192.168.1.13_13]: growright,nopercent
MaxBytes[192.168.1.13_13]: 125000000
Title[192.168.1.13_13]: Analisis de trafico eth10 (ID13) -- SER4
PageTop[192.168.1.13_13]: <h1>Analisis de trafico eth10 (ID13)-- SER4</h1>
                <div id="sysdetails">
                        <table>
                                <tr>
                                        <td>Sistema:</td>
                                        <td>SER4</td>
                                </tr>
                                <tr>
                                        <td>Administrador:</td>
                                        <td>CENAPRED</td>
                                </tr>
                                <tr>
                                        <td>Descripcion:</td>
                                        <td>Puente MAC</td>
                                </tr>
                                <tr>
                                        <td>Tipo de interfaz:</td>
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>Nombre de interfaz:</td>
                                        <td>Ethernet 10</td>
                                </tr>
                                <tr>
                                        <td>Velocidad maxima:</td>
                                        <td>125.0 MBytes/s</td>
                                </tr>
                                <tr>
                                        <td>Ip:</td>
                                        <td>192.168.1.13 ()</td>
                                </tr>
                        </table>
                </div>
```

Anexo 15. Snmpd.conf de RedHat configurado para OpenSuse

```
#Listas de control de acceso (ACL)
#       nombre          origen          comunidad
com2sec  local   localhost            public

# Asignar el nombre de seguridad a cada grupo
#    Nombre de grupo Modelo de seguridad Nombre de seguridad
group   MyROGroup           v1                 local
group   MyROGroup           v2c                local

#Ramas MIB que se permiten ver
```

```
## nombre   incl/excl subárbol   máscara (opcional)
view    all  included  .1        80

#Establece permisos de lectura y escritura
##group context sec.model sec.level prefix read write  notif
access MyROGroup   any   noauth    exact  all    none  none


#SER3rmación de contacto del sistema
syslocation CENAPRED
syscontact Root <root@localhost>
authtrapenable 1
trapcommunity OPEN
trapsink 192.168.1.160
SER3rmsink 192.168.1.160
trap2sink 192.168.1.160
```