HERRAMIENTAS PARA LA MONITORIZACIÓN DE REDES DE COMPUTADORAS

SOFTWARE FOR COMPUTER NETWORK MONITORING

Dilber Rosabal Montero[1], María Esther Orozco Vaillant[2]

[1]Facultad de Ciencias Informáticas, Universidad de Granma. [2]Facultad de Ciencias Informáticas, Universidad de Granma.
[1]drosabalm@udg.co.cu
[2]mary92@openmailbox.org

RESUMEN

La monitorización de redes de computadoras contribuye a la eficiente gestión y control del comportamiento de los dispositivos de una red, tales como estaciones de trabajo, servidores y equipos de interconexión de redes. Además, permite la evaluación del tráfico de red y la calidad de servicio, así como la detección y notificación de fallas, lo que favorece la detección de intrusiones y la generación de reportes en tiempo real. La monitorización se realiza por medio de técnicas activas, pasivas o un híbrido de ellas, al aprovechar la oportunidad de disminuir el flujo de información de administración y obtener notificaciones y registros de los parámetros de la red en tiempo real. Las aplicaciones para la monitorización de redes emplean los protocolos de gestión de redes. En este artículo se presenta un análisis de diferentes herramientas, basadas en software libre y comercial que facilitan la supervisión de la red, soportan el protocolo simple de administración de redes, versión 2 y ofrecen una interfaz web para visualizar la información de los parámetros de la red de una empresa.

PALABRAS CLAVES: monitorización, redes de computadoras, SNMP

ABSTRACT

Monitoring of computer networks contributes to the efficient management and control of the behavior of network devices such as workstations, servers and networking equipment. It also allows the evaluation of network traffic and quality of service as well as the detection and reporting of failures, which favors the intrusion detection and report generation in real time. To reduce the flow of management information and records of notifications and the network parameters in real time are used active, passive techniques or a hybrid of them. Network management protocols are used by the applications for network monitoring. An analysis of different tools, based on free and commercial software that facilitate the network monitoring, support the simple network management protocol, version 2 and offer a web interface to display the information of the company network is presented in this research.

KEY WORDS: computer networks, monitoring, SNMP

1. INTRODUCCIÓN

El desarrollo de las Tecnologías de la Información y la Comunicación (TIC), han permitido el empleo de los recursos de información para múltiples fines, por lo que hoy en día se hace necesario el uso de las redes de computadoras para llevar a cabo la correcta gestión de los procesos empresariales. Tanenbaum y Wetherall, definen que una red de computadoras es una colección de computadoras autónomas interconectadas a través de una tecnología; expresan además que 2 computadoras están interconectadas si están habilitadas para intercambiar información [1]. El funcionamiento de una red de computadoras debe ser objeto de monitorización, gestión y control por los administradores de redes; permitirá evaluar el funcionamiento de los servicios de red que utilizan los usuarios, detectar fallas en los servidores, en el equipamiento de interconexión como *switch* y *router* y las posibles mejoras que se pueden realizar en la infraestructura de red; además de contribuir a la seguridad de la información que se maneja en una empresa.

2. GESTIÓN Y MONITORIZACIÓN DE REDES DE COMPUTADORAS

La gestión de redes consiste en el desarrollo, integración y coordinación del *hardware*, *software* y recursos humanos para monitorizar, probar, configurar, analizar, evaluar y controlar los elementos de red para conocer el rendimiento operacional en tiempo real y los requerimientos de calidad de servicio a un costo razonable [2].
Saydam y Magedanz [3] hacen referencia a cinco áreas funcionales de la gestión de redes definidas por la ISO (*International Standard Organization*) y también fueron abordadas por Kurose y Ross [2]; ellas son: gestión de rendimiento que tiene el objetivo de cuantificar, medir, reportar, analizar y controlar el rendimiento, como utilización y desempeño de los recursos de red, los enlaces y dispositivos de red y que juega un papel importante la utilización del protocolo simple de administración de redes (*SNMP, Simple Network Management Protocol*); gestión de fallos a través de la cual se realiza el registro, detección y respuesta ante un fallo en la red; gestión de configuración que permite a los administradores de red grabar cuales dispositivos se encuentran en la red administrada y sus configuraciones de hardware y de software; gestión de contabilidad para especificar, registrar y controlar el acceso de usuarios y dispositivos a los recursos de red y gestión de seguridad que servirá para controlar el acceso a los recursos de red de acuerdo a las políticas de seguridad definidas.
La monitorización es un concepto fundamental en la observación de la utilización de las redes y sus componentes. Es la parte de la gestión de redes que se ocupa de la observación y análisis del estado y el comportamiento de los recursos gestionados. Durante el proceso de monitorización o supervisión se deben tener en cuenta las siguientes etapas:

- Definición la información de gestión que se va a monitorizar: existen muchos aspectos que pueden ser monitoreados, los más comunes son la utilización del ancho de banda, el consumo del procesador y su temperatura, consumo de memoria y ciertos servicios, como son el servicio web, el correo electrónico, base de datos.
- Acceso a la información que se va a monitorear: los sistemas de monitoreo utilizan los servicios ofrecidos por un gestor para acceder a la información de tipo administrativa mantenidos por los agentes en su base de datos local. Las comunicaciones entre gestores y agentes tienen lugar gracias al empleo de protocolos de gestión de redes, como SNMP, que utiliza la información que almacenan las variables de la base de información de administración (MIB, *Management Information Base*), mantenidas por cada dispositivo y que se podrán almacenar en bases de datos o en archivos de registros.
- Diseño de las políticas de monitorización: se distinguen dos tipos de comportamiento, el primero es el sondeo, en este caso, el gestor pregunta periódicamente a los agentes por la información que se requiera, los datos pertinentes que se requieran de determinado agente para llevar a cabo el proceso de monitorización. Este método es utilizado para obtener la información de administración de servidores y equipos de interconexión. El segundo tipo de comportamiento se refiere al informe de eventos, que ocurre cuando los agentes, ante cualquier incidente considerado fuera de lo normal, informan a los gestores para que de esta manera se pueda tomar una medida o acción pertinente.
- Procesamiento de la información que se obtiene: es la etapa en la que se almacena en bases de datos o en registros, la información obtenida para su posterior análisis.

Técnicas de monitorización
Las técnicas de monitorización se clasifican en pasivas y activas. Hyun-chul y Lee, exponen que las técnicas pasivas observan el tráfico de la red como mismo pasa a través de los *routers*, *switch* y *hosts* sin generar o insertar tráfico adicional en la red, contrario a las técnicas de medición activas que inyectan paquetes en la red o los retransmiten a otros servidores o *hosts* para probar, diagnosticar o medir parámetros de demora de la red, conectividad y otros. Afirman que el método de medición pasivo es usado con el propósito de medir el volumen de tráfico, para su análisis por las aplicaciones y sistemas autónomos (*AS, Autonomous Systems*) y para el análisis del comportamiento de los usuarios finales [4].

También en *The Practice of System and Network Administration*, Thomas A. Limoncelli y otros autores, abordan 2 tipos primarios de monitorización, en tiempo real cuando se facilita información del estado actual de los servicios y la monitorización histórica cuando provee datos durante un largo tiempo de actividad, uso y desempeño de un sistema [5].
La mayoría de los administradores prefieren la monitorización pasiva o una combinación del pasivo con el reporte de unos cuantos incidentes de alto riesgo, en lugar de la monitorización activa, de ahí que se utiliza la monitorización pasiva para obtener la información de los dispositivos de red y se garantiza que el comportamiento de la red se vea menos afectado por las operaciones de supervisión. Para presentar la información que se extrae de ella, la misma debe transformarse para que sea entendible por los administradores. Una de las vías para lograr dicho propósito, es mediante el diseño de animaciones, gráficos o videos para presentar la información sobre el tráfico de red. Además, el administrador de una red necesita herramientas que lo ayuden a monitorizar, gestionar y controlar la red.
Para el registro de la información de la red existen dos formatos disponibles: captura de paquetes y captura de flujo. En la captura de paquetes se almacena la información que pasa a través de un cable o una interfaz que se monitoriza, se analiza cada paquete individualmente, incluyendo la cabecera y los datos. En la captura de flujo se resume el tráfico y no incluye el contenido. Excluyendo dicho contenido se pierde la capacidad de reconstruir el tráfico de red real, tal como se escuchó. Sin embargo, centrarse en el formato de captura de flujos, permite obtener métricas importantes sobre el rendimiento del tráfico en la red, la calidad de determinado servicio que se brinda o la pérdida de datos. En este formato se trabaja con grandes cantidades de datos [6]. Para la monitorización se utilizan protocolos de administración de redes, que posibilitan la captura y análisis de la información de la red.

PROTOCOLOS DE GESTIÓN DE REDES
Los protocolos de administración de redes permiten la monitorización de los equipos de una red y sus recursos asociados. Ellos guardan la información de administración en variables que son almacenadas en base de datos, las cuales pueden ser consultadas más adelante y también pueden ser configuradas por aplicaciones diseñadas para gestionar una red de computadoras. Además permiten el intercambio de información de gestión entre dispositivos de una misma red. Entre ellos se encuentran SNMP, *netflow* y otros.

Netflow
Es un protocolo desarrollado por la empresa Cisco *Systems* para recopilar información sobre el tráfico de la red, el mismo es implementado en algunos enrutadores y conmutadores que lo soporten (su uso tiene la desventaja de que solo lo implementan los equipos de interconexión antes mencionados, que sean del fabricante y creador de *netflow*), para que generen registros y luego sean enviados a un colector central [7]. Para comprender mejor la esencia de *netflow* es preciso conocer que es un flujo, según Cisco es una secuencia unidireccional de paquetes que comparten [8]: direcciones IP origen y destino, puerto origen y destino UDP o TCP, tipo y código ICMP, protocolo IP, interfaz de ingreso (SNMP *ifIndex*) y tipo de servicio IP.
La recopilación de los registros se puede realizar desde el propio enrutador (se generan en el equipo) o se pueden exportar a un colector pasivo, luego de recopilados mediante el empleo de determinada herramienta, deben ser analizados. Si se usa un colector no será posible obtener todos los flujos de la red (no sucede lo mismo si se realiza desde el enrutador), este solo verá los flujos desde el punto de red donde se encuentra. Esto tiene la ventaja de que libera al enrutador de la tarea de crear y exportar flujos. Se utilizan los colectores cuando solo se requiere observar una sección del tráfico o cuando solo exista un punto de salida de la red [8]. Si la recopilación de la información se realiza desde el enrutador, se logra observar todos los flujos de la red, pero ralentiza el trabajo propio de este dispositivo, tiene más carga. Una alternativa sería designar algunas interfaces para la generación de flujos y dejar otras libres para la ejecución de las funciones propias del dispositivo.

SNMP
El protocolo simple de gestión de red se ubica en la capa aplicación de la arquitectura TCP/IP y permite el intercambio de información de administración entre los dispositivos de una red de computadoras. De esta manera, posibilita a los administradores manejar el desempeño de la red para encontrar y resolver problemas y planificar su crecimiento.
El modelo SNMP de una red administrada consta de cuatro componentes: nodos administrados, estaciones administradoras, información de administración y un protocolo de administración [9], [10], los cuales se muestran en la figura 1.

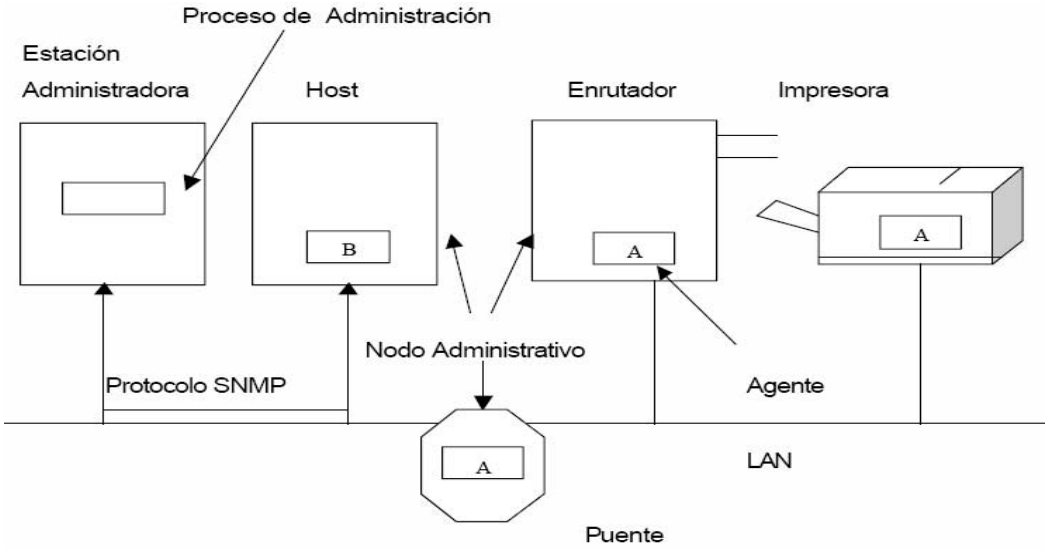

Figura 1: Componentes del modelo de administración SNMP

En el ambiente SNMP existen dos tipos de entidades: estación administradora y agentes. La administración se hace desde la estación administradora, el administrador puede ser un servidor o computadoras de propósito general que ejecutan un software de administración. En el lenguaje SNMP son referidos como estaciones de administración de redes (NMS, *Network Management Stations*). Las estaciones en sentido general, deben ser capaces de generar consultas y de recibir notificaciones de agentes en la red. Por medio de una consulta se obtiene información que puede ser usada más adelante para determinar si ha ocurrido algún evento o se ha presentado un problema en la red.

Por otro lado, una notificación permite al agente dar aviso a la estación que algo ha ocurrido. La estación tiene la capacidad de realizar una acción, basada en la información que recibió del agente. El agente, en cambio, es una aplicación que corre en el nodo administrado, que pueden ser *hosts*, enrutadores, *switch*, impresoras u otros dispositivos. Para ser gestionado directamente por el SNMP, un nodo debe ser capaz de ejecutar un proceso de administración, llamado agente SNMP. Puede venir incorporado en el sistema operativo que controla el equipo o puede ser independiente. Este provee información de tipo administrativa correspondiente a la estación, almacenada en una base de datos local de variables que describen su estado, sin dejar de lado las funciones operacionales propias de cada equipo.

En la práctica el equipamiento de redes es de proveedores distintos. Con el objetivo de permitir que una estación administradora (probablemente de un proveedor distinto a alguno de los equipos que debe administrar) se comunique con estos componentes diversos, la información exacta mantenida por los dispositivos debe especificarse de forma rápida. Por esta razón, el SNMP describe, en detalle, la información de cada tipo de agente o dispositivo que tiene que administrar y el formato con que este tiene que proporcionarle los datos [9].

Cada dispositivo mantiene una o más variables que describen su estado, estas variables en SNMP se denominan objetos. El conjunto de todos los objetos posibles en una red se definen en una estructura llamada MIB o base de información de administración [11].

El modelo contiene una estación administradora que envía solicitudes a los agentes en su red, pidiéndole información, a través de consultas a las variables contenidas en la MIB y otras que son específicas de cada proveedor. La respuesta del agente puede ser la información que le fue solicitada o la confirmación de la actualización de su estado.

SNMP se ha convertido en el estándar de gestión más utilizado desde su surgimiento y a través de la evolución de sus diferentes versiones SNMPv1 [12], SNMPv2 [13] y SNMPv3 [14]. La gran mayoría de los equipos de interconexión de redes ofrecen paquetes de agentes SNMP para ser administrados o gestionados por una entidad administradora; así como ciertas estaciones de trabajo y computadoras personales. Como bien lo indica su nombre, este protocolo se implementa de manera sencilla, no consume mucho tiempo de procesador, ni de recursos de red.

SNMPv1 es una versión de fácil instalación, solo se requiere de una comunidad para comunicarse a través de las distintas consultas que se emitan, algunas de las desventajas que presenta son:

• Posee poca o ninguna seguridad, cualquier persona con acceso a la red, puede ver el texto de la comunidad, que es enviado en texto plano o la fuente o destino de un paquete.

• No puede ver capas inferiores: el SNMP funciona en la capa de aplicación sobre UDP, de tal manera que no puede ver qué está sucediendo en las capas más bajas de la arquitectura.

• Genera mucho tráfico: el mecanismo de petición/respuesta con que trabaja este protocolo genera una gran cantidad de tráfico de red, ya que aunque se envíen reportes no solicitados (*traps*). Al ocurrir eventos inesperados se genera una cantidad enorme de tráfico al solicitar información a los agentes.

• Provee información de una máquina, no de la red: con SNMP se puede ver lo que ocurre en una máquina en específico, pero no lo que sucede en el segmento de red.

SNMPv2, la nueva versión del protocolo simple de administración de redes, tiene entre sus objetivos: reducir el tráfico de red, segmentar redes grandes, soportar múltiples protocolos de transporte, incrementar seguridad y permitir múltiples agentes por dispositivo.

Esta versión incorpora un mecanismo, conocido como recuperación masiva, con el cual los administradores pueden recuperar al mismo tiempo varias tramas de información de la red desde cualquier agente. Se evita así, la necesidad de sucesivas peticiones y respuestas para cada dispositivo administrado en la red. SNMPv2 no solo permite supervisar y administrar dispositivos de forma remota, sino también configurarlos. Quizás el elemento más significativo que incorpore esta versión es la de permitir múltiples agentes por dispositivo, un ejemplo práctico, sobre un servidor distribuido un primer agente podría supervisar la actividad del procesador, un segundo agente monitoriza la actividad de la base de datos y un tercero supervisa la actividad de la red. Finalmente, cada uno de ellos reportará a su propio administrador. La mayoría de los dispositivos hoy en día soportan SNMPv2 y por lo general lo hacen de forma automática.

En el caso de SNMPv3, agrega las características de seguridad dentro del SNMPv2, al incorporar un fuerte dispositivo de seguridad con el cifrado y la autenticación, que pueden ser utilizados juntos o por separado [10].

SNMPv2 constituye la opción más simple para ser utilizada en el desarrollo de aplicaciones para la gestión de redes de computadoras, pues es una versión mejorada de SNMPv1 y ofrece mayores ventajas. Es de fácil implementación, con respecto a SNMPv3, permite configuración remota de los diferentes dispositivos presentes en una red y además, la mayoría de los dispositivos de red hoy en día soportan por defecto la versión 2 de este protocolo. Por otra parte, al considerarse que solo las estaciones administradoras, son las encargadas de enviar solicitudes de actualización de su estado o peticiones de información a los agentes, se logra reducir el tráfico y se libera a los dispositivos de realizar procesos que afecten sus funciones principales, para las que fueron creados. El protocolo SNMPv2 es soportado por múltiples herramientas para la monitorización de las redes de computadoras, por lo que se analizan las características de ellas durante la investigación.

HERRAMIENTAS DE MONITORIZACIÓN DE REDES

Existen diferentes herramientas que permiten la monitorización pasiva o activa de una red de computadoras. A continuación se describen varias herramientas que muestran información del comportamiento de los recursos de red a través de la web, entre ellas PRTG Network Monitor, MRTG, Cacti y Nagios, las cuales se utilizan en el proceso de supervisión y control de los recursos de red.

Monitor de red PRTG

PRTG (*Paessler Router Traffic Grapher*) es un software propietario de monitorización de redes que se puede utilizar tanto para fines comerciales como particulares. Es fácil de instalar y configurar y para su correcta instalación se necesita la ejecución del asistente de instalación y configurar los sensores, que permiten la monitorización de cada una de las unidades [15]. Un sensor monitoriza, por ejemplo, un servicio de red, una dirección web, una conexión de red, algún puerto de un dispositivo de interconexión, como un *switch* o un *router*, la memoria del sistema o el uso del CPU. La versión gratuita o de prueba de PRTG contiene 30 sensores. En la figura 1 se muestra una imagen de la interfaz gráfica de la aplicación.

Figura 1: Monitor de red PRTG [15]

Entre las múltiples acciones que se pueden realizar con el software están [15]: evitar bloqueos del rendimiento y del ancho de banda, maximizar los beneficios, ya que disminuye los tiempos de inactividad ocasionados por errores del sistema que no hayan sido detectados, mejorar la calidad de los servicios para los usuarios, evitar embotellamientos en rendimiento y ancho de banda, lograr identificar aplicaciones o servidores que usan el ancho de banda de la empresa, medir cuánto ancho de banda se utiliza en determinado momento, por qué aplicaciones y los usuarios involucrados y observar tendencias de la utilización de la red.
Además, la aplicación soporta el manejo remoto, incluyendo teléfonos móviles, varios métodos de notificación ante ocurrencia de averías, como son el correo electrónico y los SMS. PRTG es una herramienta útil para la monitorización de disponibilidad, uso y actividad, cubriendo desde la monitorización de sitios web hasta el desempeño de bases de datos. También brinda soporte completo para la adquisición de datos comunes del desempeño de las redes de múltiples formas, ya sea a través de SNMP, *sniffing* de paquetes, *netflow* y otros. Muestra la información de la red en forma de tablas y en diferentes gráficos, aunque su configuración requiere de varias etapas para mostrar la información deseada.

MRTG
La aplicación MRTG (*Multi Router Traffic Grapher*) es una herramienta para monitorizar la carga de tráfico en enlaces de red que genera imágenes PNG contenidas en páginas HTML que brindan una representación visual en vivo del tráfico de la red [16]. Es una herramienta empleada mayormente para la supervisión del tráfico de red, pero también se emplea para monitorizar otras variables que se puedan medir, como temperatura, carga del CPU, es decir, debido a su uso extensivo y las grandes posibilidades que brinda; se utiliza para medir cualquier magnitud durante períodos de tiempo largos. Liberado bajo la Licencia Pública General GNU, está disponible para varios sistemas operativos, entre los que se encuentran GNU/Linux y Windows NT. Para obtener la información de los dispositivos que se deben monitorizar emplea tanto el protocolo SNMP (si los dispositivos pueden ejecutar el recurso de administración: agente SNMP) o scripts desarrollados por los usuarios. En la figura 2 se muestra la interfaz gráfica de la aplicación con la información del tráfico de red por una interfaz.

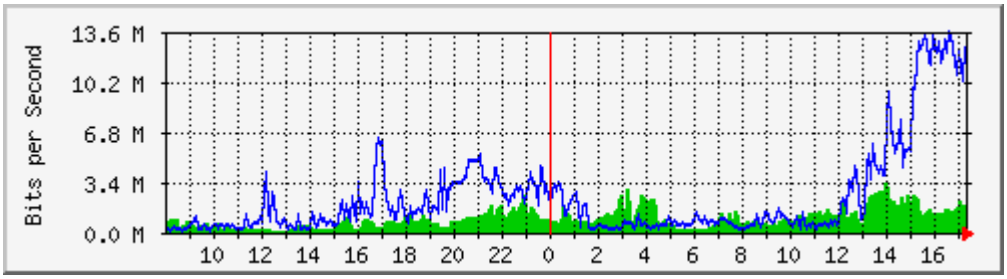

Figura 2: Interfaz web de MRTG [16]

La herramienta contiene un fichero de configuración para saber que variables MIB debe representar en las gráficas. El fichero puede ser construido manualmente y se debe respetar la sintaxis predeterminada por MRTG, aunque debido al gran número de variables, la configuración manual puede llegar a resultar un proceso incómodo. El fichero también puede ser elaborado por medio de una utilidad llamada *cfgmaker*, que facilita el proceso al realizarlo de manera automática. Esta utilidad explora toda la red mediante mensajes SNMP, para averiguar las interfaces que poseen los dispositivos que se desean monitorizar y cuáles se encuentran en funcionamiento. Luego *cfgmaker* genera un fichero de configuración para representar el tráfico a lo largo del tiempo de las interfaces operativas en el momento en que fue ejecutado. Además, incluye información concerniente a las interfaces que no estaban en funcionamiento en ese momento, a modo de comentario, dando opción al usuario de que las incorpore más adelante, si así lo desea, al quitar el comentario de las líneas correspondientes en el fichero de configuración.
Por cada dispositivo nuevo que se quiera agregar, se necesita un archivo de configuración. Esto permite que cada cierto tiempo se pueda ejecutar, en el programador de tareas del sistema, por ejemplo, para los sistemas GNU/Linux, el cron: programador de tareas para su ejecución automática en un espacio de tiempo definido por el usuario, el comando especificando ese archivo de configuración. Primeramente, se debe habilitar en el dispositivo el agente SNMP, con una comunidad y definir los permisos de lectura y escritura o solo lectura. Luego se crea el archivo *.cfg que corresponde al dispositivo que se desea agregar, con un comando, que trae la instalación de la aplicación: /usr/bin/cfgmaker --output=/etc/mrtg/router.cfg public@192.168.10.16
Luego, se ejecuta *cfgmaker*, que automáticamente genera el archivo router.cfg, lo que indica que se autenticará en el dispositivo con dirección IP 192.168.10.16 y con el nombre de la comunidad *public*. Luego en el cron se debe agregar la siguiente entrada: */5 * * * * root /usr/bin/mrtg /etc/mrtg/router.cfg
Con esta entrada se ejecuta cada 5 minutos el comando /usr/bin/mrtg y la configuración realizada en el archivo /etc/mrtg/router.cfg.
Además con la opción: /usr/bin/indexmaker –output=/var/www/mrtg/index.html /etc/mrtg/router.cfg, se pueden mostrar todos los equipos que se monitorizan a través de la web.

Cacti

Es una aplicación web, software libre, un sistema de monitorización que almacena toda la información necesaria para la generación de gráficos en una base de datos MySQL, aunque también utiliza RDDtool (*Round Robin Database*) y soporta SNMP. Fue desarrollado en PHP y aparte de la recogida de los datos y su almacenamiento, también los mantiene y proporciona la información que se observa en tiempo real. En cuanto a la gestión de usuarios, debido a la cantidad de funcionalidades que ofrece y al ser una herramienta de gestión; permite la creación de usuarios y otorgarle permisos de acceso. De esta manera unos usuarios podrán cambiar parámetros de los gráficos, mientras que otros solo podrán visualizarlos y cada usuario puede definir su propia configuración para la visualización. Además, la generación de gráficos es totalmente personalizable [17].

Cacti permite la creación de plantillas, es decir, escala un gran número de fuentes de datos y gráficos, lo que permite que cuando se adicione un nuevo host a la red con características similares a otro ya existente, se cree una plantilla de gráfico basado en la información obtenida del host antes monitoreado. La aplicación no genera alertas en función de los valores de los parámetros medidos, es decir, no emite una notificación, ya sea mediante el envío de un email, un SMS o por cualquier otra vía; cuando la lectura de algún valor no es considerado como normal [17]. En la figura 3 se muestra la interfaz gráfica de esta aplicación.

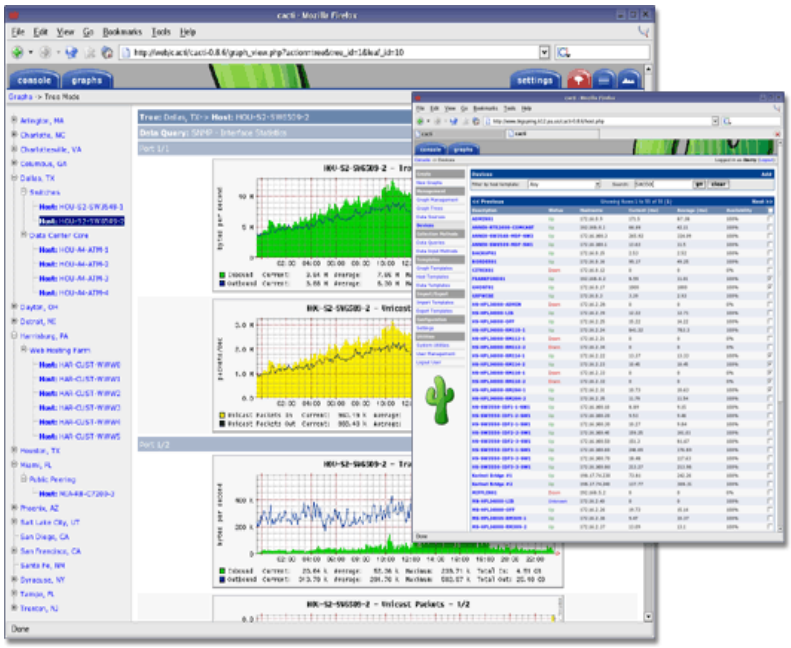

Figura 3: Interfaz web de Cacti [17]

Para lograr la visualización correcta de la información de gestión deseada, se deben realizar varias configuraciones durante el proceso de añadir un dispositivo que tenga habilitado un agente SNMP para ser gestionado y la generación de los gráficos que se van a visualizar, pues hay que acceder a diferentes vistas, dentro de las pestañas *console* y *graphs*, que se muestran en la figura anterior. La aplicación tiene plantillas predefinidas para dispositivos de interconexión como Cisco, por lo que se puede dificultar la visualización del tráfico de red de equipos de otros proveedores, que pueden ofrecer la información de administración basada en diferentes variables MIB.

Nagios

Es una herramienta que permite la monitorización de servidores, dispositivos de interconexión, aplicaciones y servicios de red [18]. Es un sistema de monitorización convertido en el estándar líder en soluciones de monitorización de clase empresarial, aunque con lo rápido que se ha difundido, es utilizado para la monitorización de infraestructuras de propósito general. Es una herramienta de código abierto, liberada bajo la Licencia Pública General GNU, fue desarrollada en el lenguaje de programación C. La aplicación supervisa constantemente *hosts*, servicios u otro parámetro a gestionar previamente definido y envía una alerta cuando aparece algún problema o cuando estos se solucionan. En la figura 4 se muestra una imagen que ilustra la interfaz gráfica de la aplicación. Entre sus principales características están: permite la monitorización de servicios de red, tales como: SMTP, POP3, HTTP, SSH, DNS, permite la monitorización de la carga del procesador, espacio libre en archivos del sistema y el uso de la memoria, es altamente flexible, permitiendo que los usuarios puedan crear sus propios comandos, posee un entorno web para visualizar el estado actual de los servicios, la generación de las estadísticas y soporta base de datos para el almacenamiento de la información de gestión.

La aplicación muestra, por defecto, la información básica sobre el uso del espacio en el disco duro, sobre los usuarios del sistema, el estado de algún servicio de red instalado, entre otros. La principal desventaja está dada para la configuración de la información que se desea visualizar con el sistema, la cual se debe realizar a través de la edición de ficheros de texto en la consola y solo se ejecuta sobre sistemas GNU/Linux.

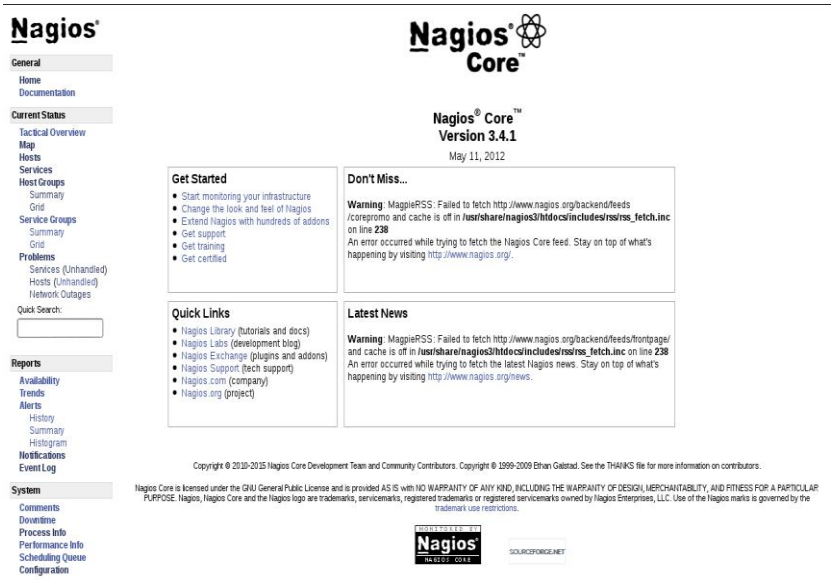

Figura 4: Interfaz web de Nagios.

De las diferentes herramientas de monitorización analizadas se obtuvo que se debe pagar una licencia comercial para la utilización de PRTG, no siendo así si se emplean MRTG, Cacti o Nagios, pues utilizan la licencia pública general, GNU/GPL. PRTG y Cacti permiten la gestión de la información de gestión mediante la web, sin embargo al utilizar MRTG y Cacti, se debe hacer la configuración mediante la edición de ficheros y solo se visualiza la información de la red en la web. Las herramientas Nagios y MRTG han alcanzado un gran auge en la gestión de redes de computadoras, por lo que se recomienda su uso en un ambiente empresarial en el que tienen definidas políticas de empleo de software libre. De igual forma, PRTG es considerada una potente herramienta privativa para la monitorización, control y administración de una red de computadoras, que además de SNMP, soporta *netflow*.

3. CONCLUSIONES

Las herramientas analizadas usan tablas y gráficos para presentar la información de la red. La mayoría son software libre, excepto PRTG. Uno de los métodos que emplean para almacenar la información, es mediante el empleo del sistema gestor de base de datos MySQL.

Todas las aplicaciones ofrecen una interfaz web para mostrar la información de gestión de la red. PRTG y Cacti permiten la gestión de las opciones de configuración por esta vía, la primera es una herramienta privativa y en la segunda para la generación de gráficos, hay que realizar una serie de configuraciones para mostrar la información de gestión que se desea visualizar. En ambos casos, se debe tener bien definido los parámetros de red que se desean visualizar y un buen dominio de los conceptos asociados a la gestión y monitorización de redes.

Nagios y MRTG, solo utilizan la interfaz web para mostrar la información que se obtiene en el proceso de monitorización de la red. En ellas es necesaria la configuración de ficheros de texto a través de la consola para establecer los parámetros que se quieren gestionar, lo que dificulta el proceso de configuración para visualizar la información de la red.

Durante la investigación se evidenció que existen otras herramientas libres y privativas, unas con entorno web y otras no, para la monitorización de las redes de computadoras, las que se caracterizan por emplear gráficos para presentar la información acerca del comportamiento de la red y de la supervisión de los dispositivos activos. Además permiten la recopilación de los datos de administración de los dispositivos gestionables de la red y se visualizan a partir de la información que almacenan las variables MIB de cada equipo de red. La mayoría de las aplicaciones, ya tienen dispositivos de interconexión predefinidos para ser administrados y muestran los datos de la red a partir de la información de las variables prefijadas que ofrecen los datos de la red a través de SNMP.

4. REFERENCIAS

[1] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed. 2011, p. 2.

[2] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 6th ed. 2013, pp. 734-735.

[3] T. Saydam and T. Magedanz, "From Networks and Network Management into Service and Service Management," *Journal of Networks and System Management*, vol. 4, no. 4, pp. 345-348, 1996.

[4] H.-chul Kim and J. Lee, "Design and Implementation of an Interactive DBMS-supported Network Traffic Analysis and Visualization System," *International Journal of Digital Content Technology and its Applications (JDCTA)*, vol. 7, no. 13, pp. 166-175, 2013.

[5] T. A. Limoncelli, C. J. Hogan, and S. R. Chalup, *The Practice of System and Network Administration*, 2nd ed. Addison-Wesley, 2007, p. 42.

[6] K. Buell, M. G. Baydogan, B. Senturk, and J. P. Kerr, "Compressing Test and Evaluation by using flow data for scalable network traffic analysis," 2014.

[7] B. Claise, "RFC3954. Cisco Systems NetFlow Services Export Version 9," 2004. [Online]. Available: https://www.ietf.org/rfc/rfc3954.txt. [Accessed: 25-Feb-2015].

[8] C. Systems, "Cisco Netflow Collector User Guide." [Online]. Available: http://www.cisco.com/c/en/us/td/docs/net_mgmt/netflow_collection_engine/6-0/tier_one/user/guide/user.html. [Accessed: 30-May-2015].

[9] A. Tanenbaum, *Redes de computadoras*, 3rd ed. 1997.

[10] J. Case, R. Mundy, D. Partain, and B. Stewart, "RFC3410. Introduction and Applicability Statements for Internet Standard Management Framework," 2002. [Online]. Available: https://tools.ietf.org/rfc/rfc3410.txt. [Accessed: 20-Feb-2015].

[11] K. McCloghrie and M. Rose, "RFC1213. Management Information Base for Network Management of TCP/IP-based internets: MIB-II," 1991. [Online]. Available: https://www.ietf.org/rfc/rfc1213.txt. [Accessed: 20-Feb-2015].

[12] J. Case, M. Fedor, M. Schoffstall, and J. Davin, "RFC1157. A Simple Network Management Protocol (SNMP)," 1990. [Online]. Available: https://tools.ietf.org/rfc/rfc1157.txt. [Accessed: 20-Feb-2015].

[13] R. Presuhn, J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "RFC3416. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)," 2002. [Online]. Available: https://tools.ietf.org/html/rfc3416.txt. [Accessed: 20-Feb-2015].

[14] D. Harrington, R. Presuhn, and B. Wijnen, "RFC3411. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," 2002. [Online]. Available: https://tools.ietf.org/rfc/rfc3411.txt. [Accessed: 20-Feb-2015].

[15] A. Paessler, "Paessler the network monitoring company." [Online]. Available: http://www.es.paessler.com/. [Accessed: 12-Apr-2015].

[16] T. Oetiker, "MRTG. The Multi Router Traffic Grapher." [Online]. Available: http://oss.oetiker.ch/mrtg/. [Accessed: 20-Apr-2015].

[17] Inc. The Cacti Group, "Cacti. The complete rrdtool-based graphing solution." [Online]. Available: http://www.cacti.net/. [Accessed: 10-Mar-2015].

[18] E. Galstad, "Nagios. The Industry Standard in IT Infrastructure Monitoring," *LLC., Nagios Enterprises*. [Online]. Available: https://www.nagios.org/. [Accessed: 19-Apr-2015].

SOBRE LOS AUTORES

Ing. Dilber Rosabal Montero, graduado de Ingeniería en Telecomunicaciones y Electrónica, profesor asistente que imparte las asignaturas Redes y Seguridad Informática, Redes de Computadoras y Protocolos TCP/IP y sus aplicaciones en la Facultad de Ciencias Informáticas de la Universidad de Granma.
Ing. María Esther Orozco Vaillant, graduada de Ingeniería en Ciencias Informáticas de la Universidad de Granma.