Tercera Conferencia de Directores de Tecnologías de Información y Comunicación de Instituciones de Educación Superior, Gestión de las TICs para la Investigación y la Colaboración, Cartagena de Indias, 8 y 9 de Julio de 2013

Experiencia de la UIS en la instalación e implementación del centro de control de Red de datos (COR-UIS).

Jaime Enrique Sarmiento[a], Benjamín Pico Merchán[a], Antonio José Lobo[a]

[a] Universidad Industrial de Santander – UIS
Bucaramanga - Colombia. Carrera 27 calle 9
jaimesar@uis.edu.co, bpico@uis.edu.co, ajlobofi@uis.edu.co

Resumen. A medida que las organizaciones crecen, también crece la red de datos y por consiguiente se incrementan los problemas en esta. Por tal motivo se hace necesario la instalación e implementación de herramientas que permitan monitorizar y generar alarmas para minimizar el impacto en el rendimiento de las redes y en el servicio a los usuarios finales. El siguiente trabajo describe la implementación de un centro de operaciones de red (COR) utilizando herramientas de software libre y la implementación del centro de atención al usuario para la gestión de incidentes y requerimientos sobre la red de datos institucional de la Universidad Industrial de Santander UIS.

Palabras Clave: Redes, Software libre, Gestión.

1 Introducción

El uso de la red de datos se ha incrementado en los últimos años de forma exponencial. Según datos del Internet World Stats[1] entre 2000 y 2012, el número de usuarios en internet ha crecido un 566.4%. Por tal motivo la disponibilidad y continuidad de los servicios de la red de datos se hace extremadamente importante para el normal funcionamiento de las instituciones, cualquier factor que ponga en riesgo o afecte su normal funcionamiento debe ser detectado y corregido lo más rápido posible evitando así que se comprometa la integridad y disponibilidad de la información.

El problema que se presenta frecuentemente en las unidades encargadas de la administración de la red de datos es la falta de personal profesional para atender y satisfacer oportunamente los requerimientos de los usuarios referidos a problemas con la red de datos.

[1] http://www.internetworldstats.com/stats.htm

2 Centro de control de Red de datos (COR-UIS)

La Universidad Industrial de Santander (UIS), institución de educación superior pública colombiana, decidió a través de su División de Servicios de Información la creación e implementación de un centro de operaciones de red de datos (COR-UIS) utilizando software libre que permita gestionar los recursos humanos y técnicos necesarios para la corrección de fallas, evitando interrupciones en el servicio o reduciéndolas al mínimo, salvaguardando el normal funcionamiento de los servicios prestados a través de la red de datos. Se busca ser proactivos, evitando en lo posible que los usuarios de la red detecten los problemas antes que los administradores. Este trabajo pretende ser una guía para otras instituciones en los pasos que deben seguir para implementar un sistema de gestión de red de datos a bajo costo.

2.1 ¿Por dónde se debe comenzar?

Lo primero fue identificar los puntos donde se consideraba existía un problema o una carencia en la administración o gestión de la red de datos:

2.1.1 Atención al usuario

Uno de los problemas que se presentaban con la gestión de red era la constante queja por parte de los usuarios en los tiempos de atención a sus requerimientos. Esto se debía principalmente a que los usuarios contactaban directamente al técnico para reportar su problema y muchas de estas llamadas no eran atendidas ya que el técnico estaba resolviendo las solicitudes recibidas personalmente, situación que retrasaba el proceso de atención a los demás usuarios y creaba un malestar en los mismos por no sentirse atendidos oportunamente. Para lograr una mejora en este aspecto se implementó un centro de atención al usuario, que consiste en un sitio único para la atención y el seguimiento de consultas y peticiones de los usuarios en lo que respecta a la red de datos. Los usuarios pueden tramitar a través de este centro, solicitudes como reporte de problemas con cuentas de correo, con conexión a Internet, fallas relacionadas con el funcionamiento de la red, entre otros. Esto garantiza una mejora en la interacción y en los tiempos de respuesta. Más adelante en este documento se comenta sobre las herramientas de apoyo para la gestión de incidentes.

2.1.2 Documentación

Otro de los problemas era el referente a la documentación de la red de datos y sus componentes (router, switches y servidores), así como lo referente a los archivos de configuración y el control de cambios de estos componentes. Es común que con la salida de un integrante del equipo de redes se pierda valiosa información sobre la red de datos, teniendo en cuenta que dicha información generalmente sólo la posee esta persona. También es común encontrarse con frases como “Pregúntale a Pedro sobre la configuración de ese equipo” o “Ramón es quien conoce sobre ese equipo o servidor”. Por tal motivo otro de los propósitos fue centralizar la documentación con la

implementación de un servidor que permita obtener, organizar y mantener la documentación de la red, así como un servidor que nos permita guardar y/o controlar los cambios en la configuración de los routers, switches y servidores.

2.1.3 Métricas y comportamiento de la red

Finalmente otro de los problemas era referente a la ausencia de los indicadores o estadísticas de uso de los elementos de la red. Si no se monitorea no se puede ser proactivo, se permanece a la expectativa de que algo suceda con los elementos activos de la red, esperando ser notificados por alguno de los usuarios. Además tampoco se disponía de estadísticas confiables sobre la utilización de los anchos de banda o enlaces. Se carecía de métodos fiables para saber si existía latencia o lentitud en la red, producida por problemas a nivel de LAN o por problemas con los enlaces a internet. Para este punto se implementaron varios servidores para ayudar a monitorear los elementos activos de la red de datos.

Éstas son algunas de las métricas que se monitorean:

- Carga típica de los enlaces
- Nivel de variabilidad (jitter) entre dos puntos
- Utilización típica de recursos

La idea fue consolidar en un centro, la información y documentación de la red de datos, así como coordinar desde allí las tareas de monitoreo del estado de la red y de sus servicios. Además, recibir los reportes sobre incidentes, quejas y reclamos por parte de los usuarios a través del sistema de gestión de incidentes. En este lugar se encuentran los servidores con todas las herramientas de gestión necesarias para estas actividades. Ver Fotografía 1.

Fotografía 1. Centro de Operaciones de Red – Universidad Industrial de Santander

A continuación se presenta un esquema del centro de operaciones de red (ver Figura 1.)

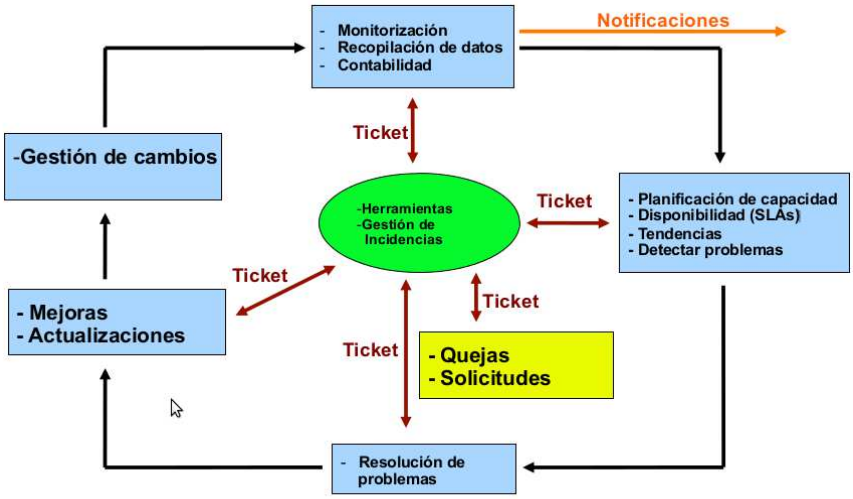

Figura 1. Esquema del Centro de operaciones de Red (COR)

2.2 ¿Qué herramientas se pueden utilizar para la gestión de la red?

A lo largo de los años la comunidad Open Source ha evolucionado y mejorado significativamente tecnologías estándares en el mundo, buscando que sean redistribuidas de forma gratuita. Hoy, el uso estandarizado de las aplicaciones Open Source (también llamado "software libre") es claramente visible en compañías y empresas de todo tipo y tamaño en prácticamente todos los países del mundo. Por lo tanto, para la gestión de redes es una buena alternativa el uso de las aplicaciones Open Source actualmente disponibles.

El concepto de Open Source se basa en una gestión y desarrollo comunitarios, que toma un producto y lo mejora constantemente, aumentando su funcionalidad, adaptabilidad y potencial de producción con el menor mantenimiento posible. La ventaja comparativa entre los sistemas propietarios y los sistemas Open Source es específicamente el bajo costo de mantenimiento y la estabilidad operativa de estos sistemas, que por su naturaleza de código abierto permiten integrar estas soluciones, cambiarlas y utilizarlas en diferentes tipos de sistemas que comprenden toda la gama de productos actualmente disponibles.

Por estas razones, la UIS decidió utilizar herramientas Open Source, teniendo en cuenta adicionalmente la reticencia de sus directivas a invertir recursos financieros en la implementación de centros de operaciones de red.

2.2.1 Algunas herramientas software libre utilizadas para la gestión de red.

a. Rendimiento: Cricket, IFPFM, flowc, mrtg*, NetFlow*, NfSen*, ntop*, perfSONAR, pmacct, RRDtool*, SmokePing*
b. Manejo de Incidencias: RT*, Trac, Redmine
c. Gestión de Cambios: Mercurial, Rancid* (routers), CVS, Subversion*, git
d. Seguridad/ (SDI): Nessus, OSSEC, Prelude, Samhain, SNORT *, Untangle
e. Registro de Eventos: swatch, syslog-ng/rsyslog*, tenshi.
f. Gestión de Redes: Big Brother, Cacti*, Hyperic, Munin*, Nagios*, OpenNMS, Observium, Sysmon, Zabbix.
g. Documentación: Ipplan, Netdisco, Netdot*, Rack Table
h. Protocolos/Utilidades: SNMP*, Perl, ping, tcpdump*, wireshark*

* Herramientas instaladas en el COR-UIS.

2.3 Preparación de los equipos activos y servidores

En esta fase se explica la selección de hardware de los servidores de monitoreo, la instalación del sistema operativo y la implementación de las herramientas seleccionadas.

2.3.1 Selección del hardware e instalación de las herramientas del COR-UIS

Una de las ventajas de utilizar software libre es el hecho de que se puede instalar prácticamente en cualquier plataforma. En el caso de la Universidad Industrial de Santander se decidió utilizar los computadores que estaban a punto de salir de actividad por desactualización tecnológica. Los computadores seleccionados para el funcionamiento del COR son de arquitectura 32bits, 512M de memoria y 350G de disco duro; el sistema operativo seleccionado es la distribución Debian. Ver en la Fotografía 2. los equipos servidores del COR-UIS.

Fotografía 2. Servidores del COR-UIS

2.3.2 Puesta a punto de las herramientas del COR-UIS

Fue una de las fases más delicadas y de más trabajo para los responsables del COR-UIS. Antes de instalar las herramientas de gestión fue necesario revisar y ajustar la configuración en cada uno de los elementos de la red (router, switches y servidores), el protocolo SNMP (comunidad, versión, sysname y contacto) y registro en el servidor DNS, variables requeridas por las herramientas de gestión. A la fecha están configuradas y debidamente instaladas las herramientas Cacti, Nagios, SmokePing, Munin y Wireshark que conforman el núcleo de la gestión de la red UIS. Uno de los logros del equipo del COR-UIS fue implementar un script que permite a través de un modem y una línea telefónica realizar llamadas de alerta cuando algunos de los equipos activos o servicios fallen, permitiendo enterarse del problema sin importar la ubicación física del personal del COR-UIS.

A continuación se muestran algunas imágenes de las herramientas ya configuradas e implementadas por el COR-UIS.

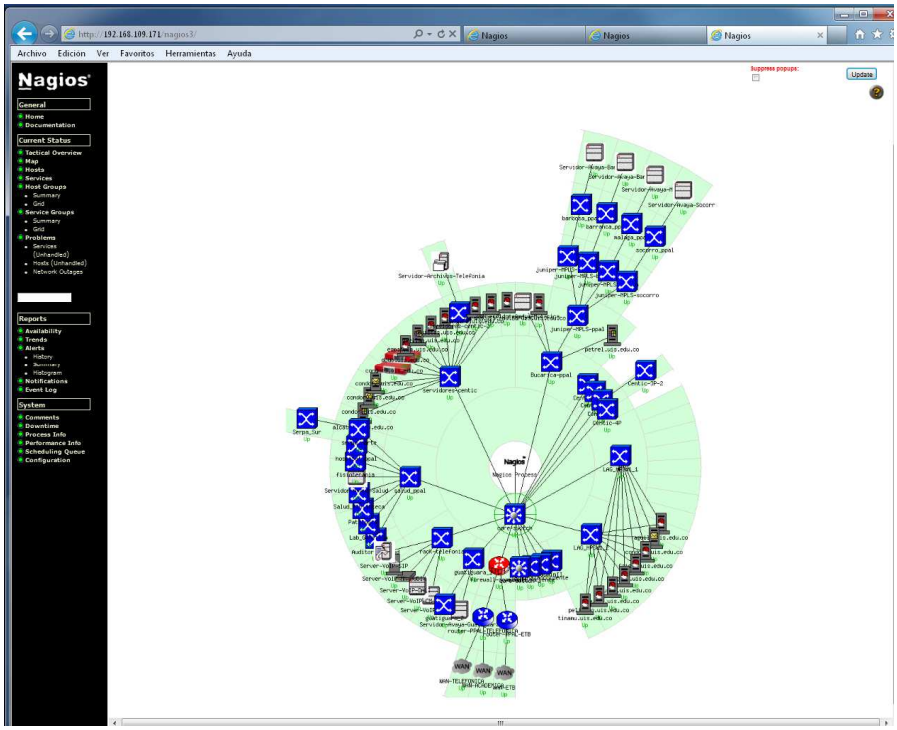

Figura 2. Herramienta de monitoreo (Nagios) de Disponibilidad de la red de datos

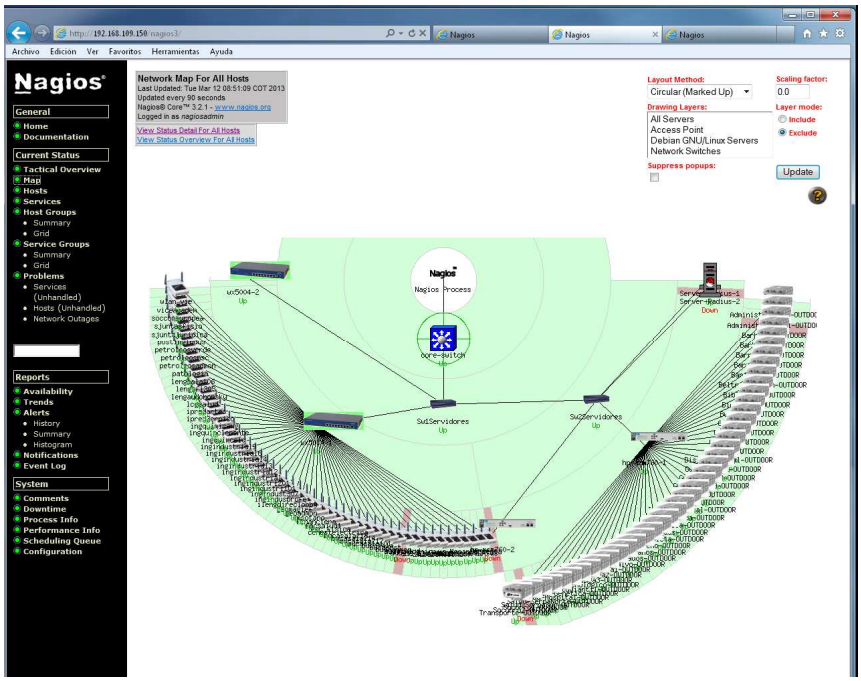

Figura 3. Herramienta de monitoreo (Nagios) de Disponibilidad de la red de inalámbrica

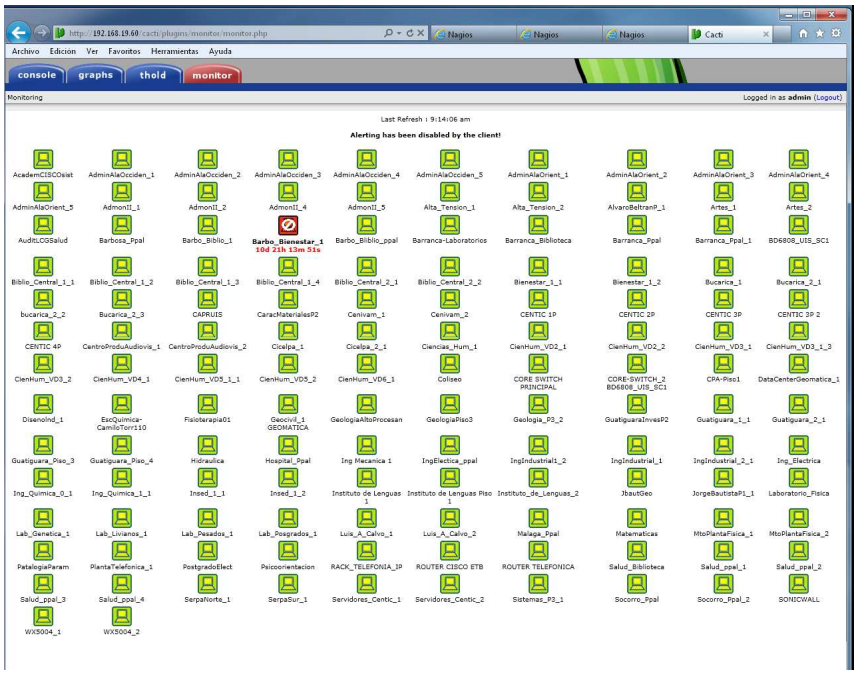

Figura 4. Herramienta de monitoreo (Cacti) para la Disponibilidad de la red de datos

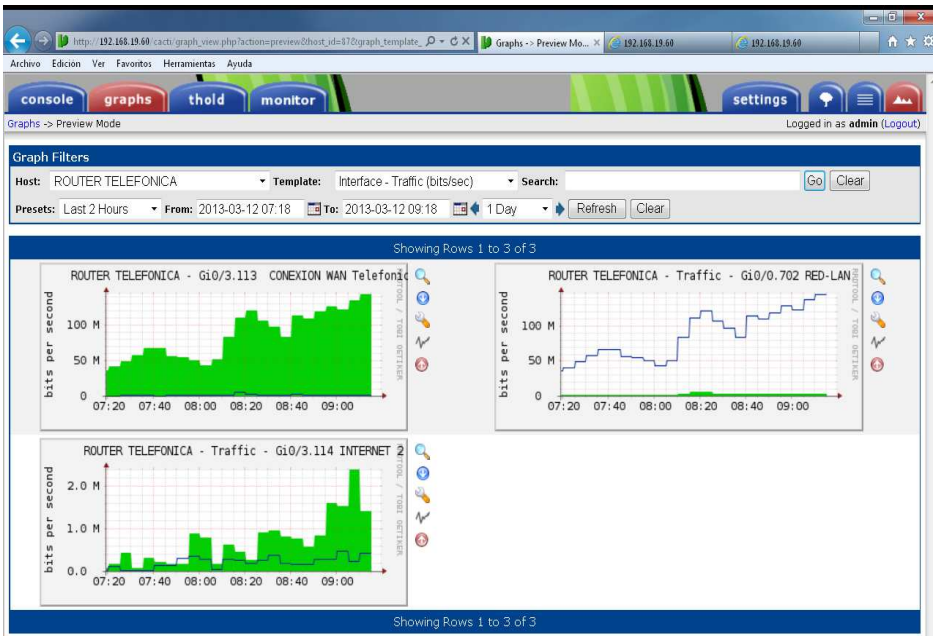

Figura 5. Herramienta de monitoreo (Cacti) de la utilización del canal de internet

3 Conclusión

El COR-UIS comenzó su implementación a mediados del 2011, en ese momento el monitoreo de la red de datos se realizaba en forma no integrada, con la herramienta de software libre MRTG aplicada individualmente a cada segmento de la red para medir la carga de tráfico en los enlaces individuales de la red. La administración de incidentes operaba de manera reactiva. Además, no se contaba con métricas confiables para determinar por ejemplo la cantidad de personal técnico para la atención de usuarios, el número de incidentes que se presentaban mensualmente en la red, y la documentación de la red de datos era parcial y desactualizada. A casi 2 años de su implementación, el COR-UIS monitorea más de 200 equipos activos de red (switches y routers), aproximadamente 70 servidores, 110 access points (indoor y outdoor), y se apoya en la plataforma de gestión de incidentes para atender más de ocho mil usuarios repartidos en 4 sedes metropolitanas y 4 sedes regionales. Actualmente se encuentra en construcción el portal web del NOC-UIS en donde se podrá ofrecer más información y noticias a la comunidad universitaria y usuarios de la red de datos institucional.

Finalmente comentamos que en la actualidad la administración de la red de datos institucional de la Universidad Industrial de Santander es totalmente proactiva y que se planifica en base a la información extraída de las herramientas de gestión.

Agradecimientos

Los autores de este trabajo desean expresar su agradecimiento al grupo de administradores de la red de datos de la Universidad de los Andes[2], Venezuela, a la Fundación Escuela Latinoamericana de Redes[3], y al ingeniero José Domínguez, Director for Network Engineering perteneciente al NOC de la Universidad de Oregón, EE UU., por toda la información y recomendaciones que hicieron posible la implementación del COR-UIS.

Glosario de términos

A continuación se explican algunos conceptos importantes para la gestión de red y que son necesarios para la implementación del centro de operaciones de red.

Monitoreo de la red de datos. Es fundamental para asegurar el buen funcionamiento de los sistemas informáticos al permitir detectar fallos en la red. La monitorización de redes también ayuda a optimizar su funcionamiento, al facilitar información detallada sobre el uso efectivo del ancho de banda y otros recursos de la red.

Normalmente, se debe monitorizar lo siguiente:

- Sistemas y servicios, buscando que cada uno de ellos esté disponible y alcanzable.
- Recursos, lo que permite planificar su expansión y mantener su disponibilidad.
- Rendimiento, mide el tiempo de ida y vuelta, y la tasa máxima de transmisión.
- Cambios y configuraciones, para disponer de documentación, control de versiones, bitácoras (logs).

Gestión de red. Se define como una serie de tareas y actividades establecidas para controlar, vigilar y evaluar los recursos que posee la empresa u organización en cuanto a telecomunicaciones se refiere. Su principal objetivo es garantizar los Acuerdos de Nivel de Servicio proyectados (ANS).

Acuerdos de Niveles de Servicio (ANS). Es un contrato suscrito entre dos partes con objeto de fijar el nivel acordado para la calidad de un servicio en particular. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.

[2] http://www.ula.ve

[3] http://www.eslared.org.ve

Básicamente el ANS establece la relación entre las partes. Un ANS identifica y define las necesidades del cliente a la vez que controla sus expectativas de servicio en relación a la capacidad del prestador o responsable del servicio, proporciona un marco de entendimiento, simplifica asuntos complicados, reduce las áreas de conflicto y favorece el diálogo ante la disputa.

Disponibilidad. Significa que los sistemas informáticos se mantienen trabajando sin sufrir ninguna degradación en cuanto a accesos y proveen los recursos que requieran los usuarios autorizados cuando éstos los necesiten.

Fiabilidad. Probabilidad de que un componente funcione correctamente bajo unas condiciones específicas.

Rendimiento. Es una medida concreta y de fácil cálculo, que permite saber si una red está funcionando en forma óptima; el tiempo de respuesta es uno de sus factores determinantes. La velocidad en la transferencia de datos puede ser alta, pero puede ser lenta la velocidad que tarda en contactarse un nodo con otro. En algunas redes, el tiempo de respuesta es crítico.

Contabilidad. Sirve para medir el uso de los recursos y llevar estadísticas de utilización por usuarios, sectores o de forma general.

Tendencias. Toda la información recopilada sirve para ver las tendencias en el funcionamiento de la red. Esto a su vez sirve para el establecimiento de puntos de referencia, planificación de la capacidad, etc. Se pueden conocer parámetros de funcionamiento de la red, tales como carga típica de los enlaces, nivel de variabilidad (jitter) entre dos puntos, utilización típica de recursos y niveles de “ruido” típicos (escaneos de red, datos descartados, errores reportados y fallos).

Protocolo SNMP (Simple Network Management Protocol). Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red (switch, routers, access point, servidores, etc.).

El sistema de administración de red se basa en dos elementos principales: un supervisor y agentes. El supervisor es el terminal que le permite al administrador de red realizar solicitudes de administración. Los agentes son entidades que se encuentran al nivel de cada interfaz. Ellos conectan a la red los dispositivos administrados y permiten recopilar información sobre los diferentes objetos.

Los conmutadores, concentradores (hubs), routers y servidores son ejemplos de hardware que contienen objetos administrados. Estos objetos administrados pueden ser información de hardware, parámetros de configuración, estadísticas de rendimiento y demás elementos que estén directamente relacionados con el comportamiento en progreso del hardware en cuestión. Estos elementos se encuentran clasificados en algo similar a una base de datos denominada MIB ("Base de datos de información de administración"). SNMP permite el diálogo entre el supervisor y los

agentes para recolectar los objetos requeridos en la MIB.

La arquitectura de administración de la red propuesta por el protocolo SNMP se basa en tres elementos principales:

- Los dispositivos administrados, elementos de red (puentes, concentradores, routers o servidores) que contienen "objetos administrados" que pueden ser información de hardware, elementos de configuración o información estadística;
- Los agentes, es decir, una aplicación de administración de red que se encuentra en un periférico y que es responsable de la transmisión de datos de administración local desde el periférico en formato SNMP;
- El sistema de administración de red (NMS), esto es, un terminal a través del cual los administradores pueden llevar a cabo tareas de administración.

A continuación observamos en la Figura 6. el funcionamiento del protocolo SNMP.

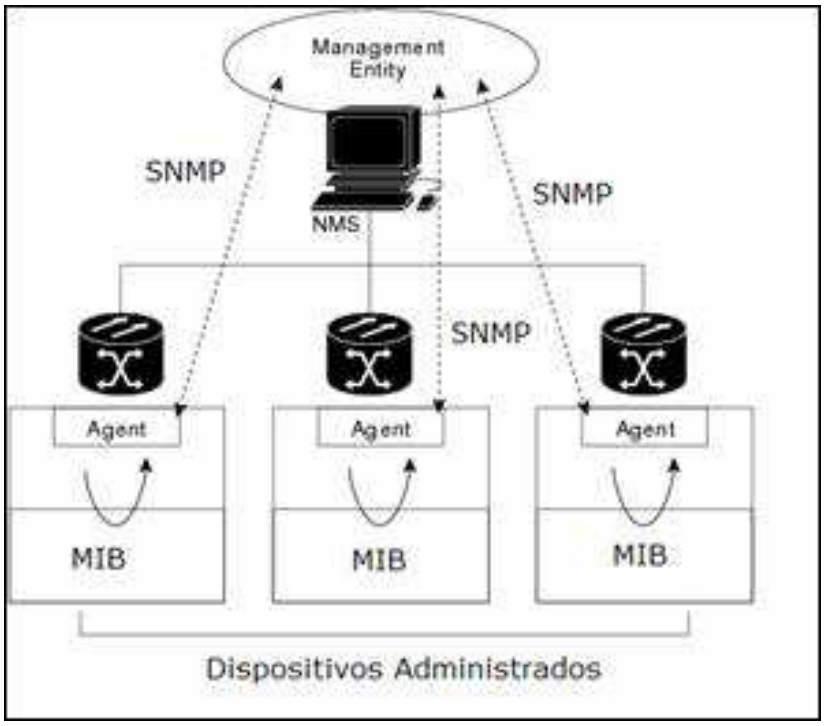

Figura 6. Funcionamiento del Protocolo SNMP

Para complementar la información sobre SNMP se puede consultar su rfc de manera online en la siguiente dirección http://www.ietf.org/rfc/rfc1157.txt

Referencias

1. RFC protocolo SNMP, http://www.ietf.org/rfc/rfc1157.txt
2. Mauro, D., Schmidt, K.: Essential SNMP. O'REILLY 2005. 2nd Edition.
3. CACTI, http://www.cacti.net
4. NAGIOS, http://www.nagios.org
5. Barth, W.: NAGIOS: System and Network Monitoring. Open Source Press GmbH 2008. 2nd Edition.
6. Smokeping, http://oss.oetiker.ch/smokeping
7. Munin, http://munin-monitoring.org
8. Escuela Latinoamericana de Redes, material sobre gestión de redes WALC 2012, https://nsrc.org/workshops/2012/walc-gestion
9. Kaufmann, M.: Network Management Know It All. Morgan Kaufmann Publishers 2008.
10. Clenm, A.: Network Management Fundamentals. Cisco Press 2006.
11. Recurso electrónico:https://nsrc.org/workshops/2004/CEDIA2/material/NOC.pdf
12. Frisch, A.: Essential System Administrator. O'REILLY 2002.