ARTÍCULO DE REVISIÓN

Los recursos de red y su monitoreo

Network resources and its monitoring

M.Sc. Gerardo Junco Romero[I]
Dr.C Sonia Rabelo Padua [II]

[I] INSAT/Epidemiología, La Habana, Cuba. E-mail: gerardo@insat.sld.cu
[II] INSAT/Docencia e Investigación, La Habana, Cuba E-mail: sonia@insat.sld.cu

RESUMEN

La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de computadoras son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificar las fallas en la red y de mostrar su comportamiento mediante el análisis y recolección de tráfico. En el presente trabajo se aborda el monitoreo de redes, describiendo los diferentes enfoques y técnicas que se deben tener en consideración para implementar este servicio, los elementos a tomar en cuenta en un esquema de monitoreo, así como un resumen de algunas herramientas para su implementación.

Palabras clave: servicios de red, monitoreo, redes.

ABSTRACT

The timely detection of failures and the monitoring of the elements that make up a computer network are highly relevant activities to provide a good service to users. From this the importance of having a scheme capable of notifying of faults in the network and of showing their behavior through the analysis and collection of traffic is derived. In the present work the monitoring of networks is approached, describing the different approaches and techniques that must be taken into consideration to implement this service, the elements to be taken into accountin a monitoring scheme, as well as a summary of some tools for its implementation.

Key words: network services, monitoring, networks.

INTRODUCCIÓN

La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de computadoras son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificar las fallas en la red y de mostrar su comportamiento mediante el análisis y recolección de tráfico.
Hasta hace poco hablar de sistemas de monitoreo de servicios de red en sistemas operativos de red o desktop resultaba casi imposible, ya que no se contaba con las herramientas necesarias para hacerlo. Bastaba con saber que el servidor estaba operativo; y ¿cómo se hacía?, solo con ejecutar el comando ping y la dirección IP del servidor.
Pero ¿cómo conocer que los servicios tales como, proxy, correo, web y otras computadoras dentro de la intranet están en operación o activos? ¿Cómo conocer que el usuario que usa un Sistema Operativo Windows no está consumiendo un gran ancho de banda?
Hoy día existen diversos mecanismos para poder monitorear los diferentes servicios y servidores. Actualmente se pueden monitorear mediante diferentes herramientas en una página web, donde los elementos más usuales que se monitorean son:
- Apache
- Squid
-MySQL
-Routers
-Servidores / Estaciones de trabajo (CPU, Espacio en disco, etc)
- Swicth (ancho de banda)

OBJETIVO

Diseñar una estrategia de monitoreo que permita la detección oportuna de fallas en los servicios de red, así como el comportamiento de estos a partir de la recolección y análisis del tráfico de red.

DESARROLLO

Se realizó un análisis documental a partir de información recuperada en materiales digitales en Internet bajo los descriptores: servicios de red, monitoreo de servicios, seguridad en redes, entre otros. A partir de la información analizada y la experiencia vivencial de los autores se elaboró una propuesta de una estrategia de monitoreo la cual permite analizar el tráfico de red de la institución así como la detección de fallas en servicios de red, optimizando de esta forma la gestión de redes.
A continuación se muestran los enfoques (activo y pasivo) de monitoreo, sus técnicas, así como la estrategia de monitoreo, incluyendo la definición de métricas y la selección de las herramientas.

Monitoreo activo

Este tipo de monitoreo se realiza introduciendo paquetes de pruebas en la red, o enviando paquetes a determinadas aplicaciones y midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red y es empleado para medir el rendimiento de la misma.

Técnicas de monitoreo activo

Basado en ICMP (Internet Control Message Protocol):
-Diagnosticar problemas en la red.
-Detectar retardo, pérdida de paquetes.

-RTT (Round-Trip delay Time).
-Disponibilidad de host y redes.
Basado en TCP (Transmission Control Protocol):
-Tasa de transferencia.
-Diagnosticar problemas a nivel de aplicación.
Basado en UDP (User Datagram Protocol):
-Pérdida de paquetes en un sentido (one – way)
-RTT (tracerroute)

Monitoreo pasivo

Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Se emplean diversos dispositivos como, programas informáticos que registran la información que envían los periféricos(sniffers), ruteadores, computadoras con software de análisis de tráfico y en general dispositivos con soporte para SNMP (Simple Network Management Protocol),[1] RMON (Remote Network MONitoring) y herramientas de monitorización de ancho banda como el Netflow. Este enfoque no agrega tráfico a la red como lo hace el activo y es utilizado para caracterizar el tráfico en la red y para contabilizar su uso.[2]

Técnicas de monitoreo pasivo

Solicitudes remotas:

Mediante SNMP: Esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para ello se requiere tener acceso a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados *traps* que indican que un evento inusual se ha producido.[3]

Otros métodos de acceso: Se pueden realizar scripts que tengan acceso a dispositivos remotos para obtener información importante a monitorear.

Captura de tráfico:

Se puede llevar a cabo de dos formas:

- Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura.
- Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red.

Análisis del tráfico: Se utiliza para caracterizar el tráfico de red, es decir, para identificar el tipo de aplicaciones que son más utilizadas. Se puede implementar haciendo uso de dispositivos *probe* que envíen información mediante RMON o a través de un dispositivo intermedio con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino, entre otros.

Flujos: También utilizado para identificar el tipo de tráfico utilizado en la red. Un flujo es un conjunto de paquetes con:

- La misma dirección.
-El mismo puerto TCP origen y destino.
-El mismo tipo de aplicación.

Los flujos pueden ser obtenidos de ruteadores o mediante dispositivos que sean capaces de capturar tráfico y transformarlo en flujos. También es usado para tareas de facturación.

Estrategias de monitoreo:

Antes de implementar un esquema de monitoreo se deben tomar en cuenta los elementos que se van a monitorear, así como las herramientas que se utilizarán para esta tarea.

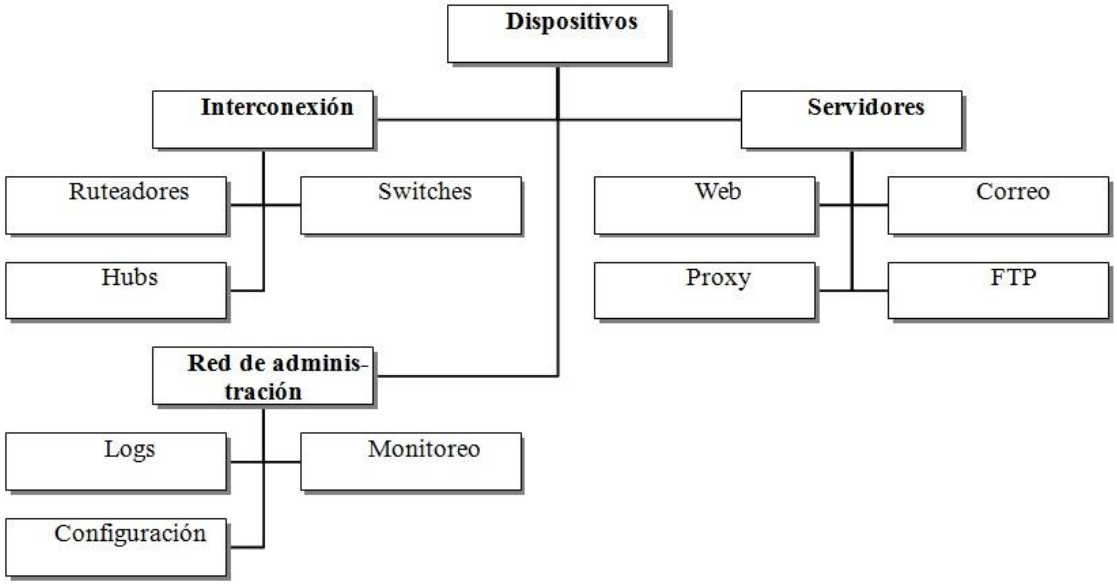
¿Qué monitorear?

Una consideración muy importante es delimitar el espectro sobre el cual se va atrabajar. Existen muchos aspectos que pueden ser monitoreados, los más comunes son los siguientes:

1. Utilización de ancho de banda

2. Consumo de CPU.
3. Consumo de memoria.
4. Estado físico de las conexiones.
5. Tipo de tráfico.
6. Alarmas
7. Servicios (Web, correo, bases de datos, proxy).

Es importante definir el alcance de los dispositivos que van a ser monitoreados, el cual puede ser muy amplio y se puede dividir de la siguiente forma como se especifica en el cuadro 1



Métricas: Las alarmas son consideradas como eventos con comportamiento inusual. Las alarmas más comunes son las que reportan cuando el estado operacional de un dispositivoo servicio cambia. Existen otros tipos de alarmas basado en patrones previamente definidos en nuestras métricas, son valores máximos conocidos como umbrales o *threshold.* Cuando estos patrones son superados se produce una alarma, ya que es considerado como un comportamiento fuera del patrón. Algunos tipos de alarmas son:[4 y 5]

1. Alarmas de procesamiento.
2. Alarmas de conectividad.
3. Alarmas ambientales.
4. Alarmas de utilización.
5. Alarmas de disponibilidad.

Elección de herramientas: Existe un gran número de herramientas para resolver el problema del monitoreo de una red. Las hay tanto comerciales como basadas en software libre. La elección depende de varios factores, tanto humanos, económicos, como de infraestructura:

a) El perfil de los administradores, sus conocimientos en determinados sistemas operativos.

b) Los recursos económicos disponibles.

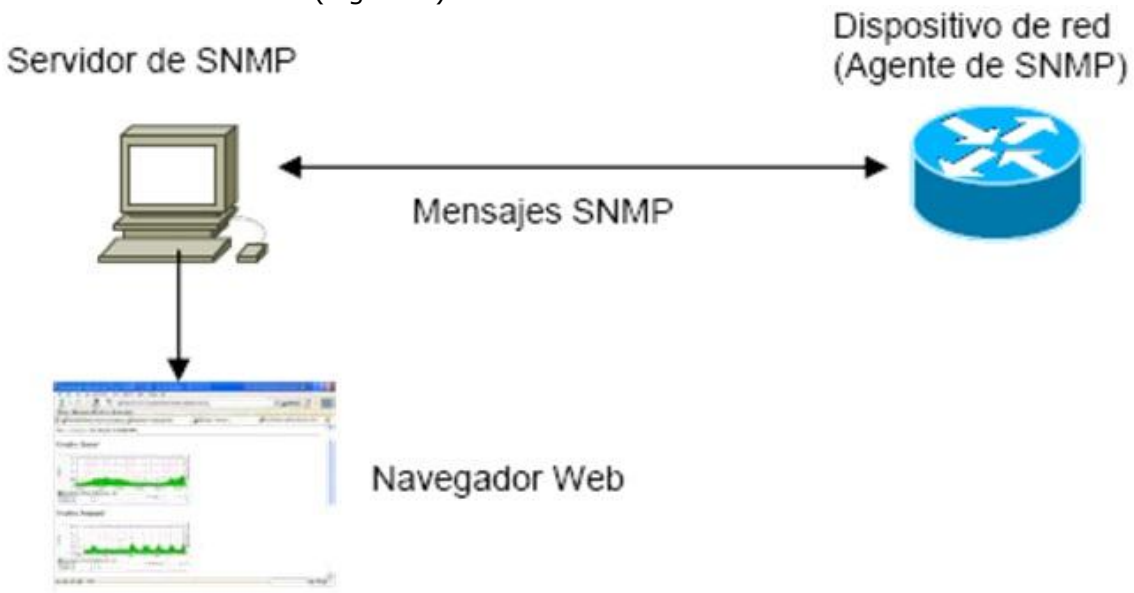
c) El equipo de cómputo disponible.

En este trabajo se hará énfasis en dos herramientas, las cuales han sido implementadas en el Instituto Nacional de Salud de los Trabajadores (INSAT):

Cacti:
Es una completa solución para el monitoreo de redes. Utiliza RRD Tools para almacenar la información de los dispositivos y aprovecha sus funcionalidades de graficación. Proporciona un esquema rápido de obtención de datos remotos, múltiples métodos de obtención de datos (snmp, scripts), un manejo avanzado de plantillas (templates) y características de administración de usuarios. Además ofrece un servicio de alarmas mediante el manejo de umbrales. Todo ello en una sola consola de administración de fácil manejo y configuración. Resulta conveniente para instalaciones del tamaño de una red de área local (LAN), así como también para redes complejas con cientos de dispositivos.[6]

Net-SNMP:
Conjunto de aplicaciones para obtener información vía SNMP de los equipos de interconexión. Soporta la versión 3 del protocolo, la cual ofrece mecanismos de seguridad tanto de confidencialidad como de autenticación. Provee de manejo de *traps* para la notificación de eventos.[7]

Topología del sistema de monitoreo:
El sistema consiste en un servidor que hace las solicitudes mediante el protocolo SNMP a los dispositivos de red, el cual a través de un agente de SNMP envía la información solicitada. (Figura 1)



También puede ser que el dispositivo envíe mensajes *trap* al servidor SNMP anunciando que un evento inusual ha sucedido. (Figura 2-3-4)

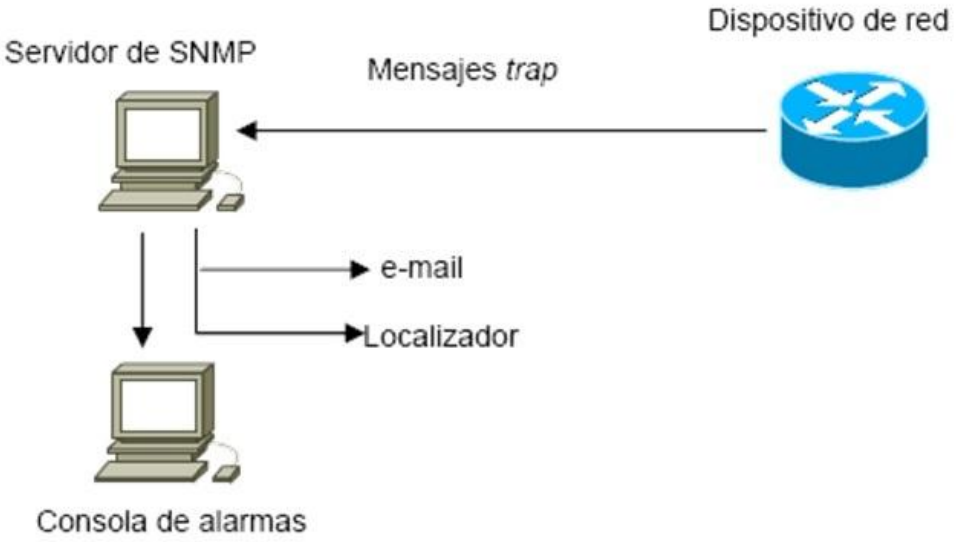


Figura 2: Monitoreo basado en el protocolo snmp con la herramienta cacti

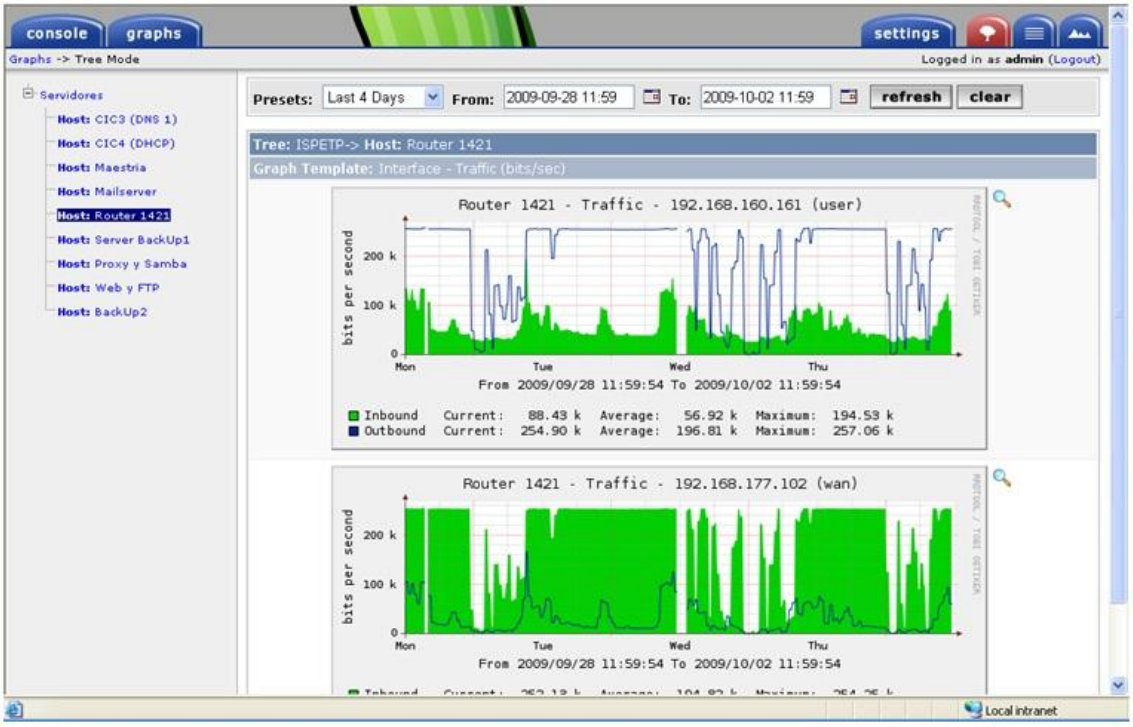


Figura 3: Gráficos en modo árbol (Router INSAT – INFOMED)

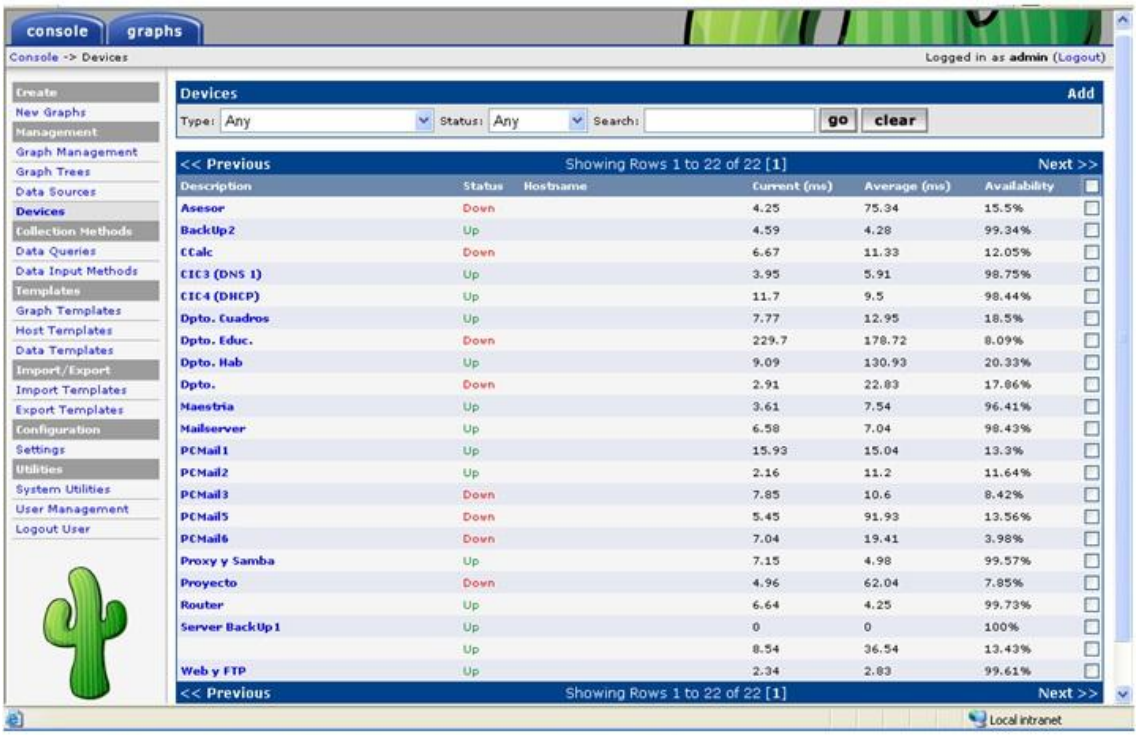


Figura 4: Estado de los dispositivos monitoreados

CONCLUSIONES

La elección del enfoque de monitoreo a emplear debe siempre partir del objetivo que se persigue con el mismo (medir el rendimiento o caracterizar y/o contabilizar el uso de la red), no olvidando que el enfoque activo agrega tráfico a la red y en dependencia del ancho de banda que se dispone, pudiera esto convertirse en una desventaja.

El monitoreo pasivo puede realizarse a través de distintas técnicas, las cuales pueden acompañarse de la definición de métricas o alarmas garantizando así el buen funcionamiento de los dispositivos de red.

Es importante definir el alcance de los dispositivos de monitoreo, así como el espectro a analizar en cada uno de ellos logrando de esta forma una estrategia de monitoreo eficiente.

Es necesario una correcta selección de las herramientas y dispositivos a emplear dentro de la red, en función de optimizar los recursos y la propia infraestructura.

REFERENCIAS BIBLIOGRÁFICAS

1. Wikipedia. Simple Network Management Protocol [en línea]. [citado 20 de septiembre 2016]. Disponible en: http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol

2. RRDTool [en línea]. [citado 20 de septiembre 2016]. Disponible en: http://oss.oetiker.ch/rrdtool/

3.SNMPv3 [en línea]. [citado 20 de septiembre 2016]. Disponible en: http://www.ibr.cs.tu-bs.de/ietf/snmpv3/

4. Linux. Flow-tools [en línea]. [citado 20 de febrero 2018]. Disponible en: https://linux.die.net/man/1/flow-tools

5. Caida org. Flowscan [en línea]. [citado 11 de marzo 2016]. Disponible en: http://www.caida.org/tools/utilities/flowscan/

6.-Cacti [en línea]. [citado 20 de abril 2015] . Disponible en: http://www.cacti.net/

7.-Net-SNMP [en línea]. [citado 20 de marzo 2017]. Disponible en: http://net-snmp.sourceforge.net/

Recibido: 14 de enero de 2018.

Aprobado: 12 de marzo de 2018.