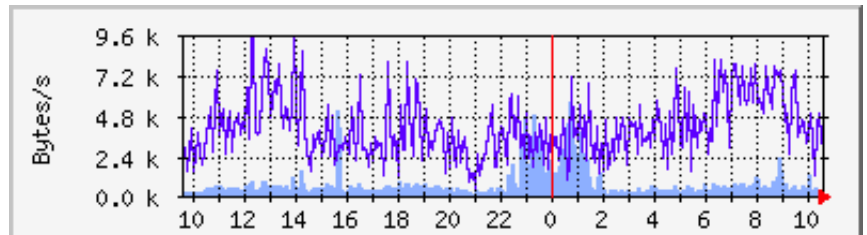


Monitorización gráfica del tráfico de red y otros parámetros del sistema

Joaquín Garzón Alcalde

En este artículo se explica como monitorizar de forma gráfica determinados parámetros del sistema como el tráfico en interfaces de red, carga de CPU, memoria libre, swap, uso de servicios, y casi todo aquello que se nos ocurra, tanto en servidores Linux como en puestos de trabajo con Microsoft Windows.

Una de las muchas tareas importantes que corresponden a un administrador de red es la monitorización del sistema, es imprescindible conocer en todo momento qué está ocurriendo en nuestra red y atajar así cualquier problema que pueda surgir, esto es posible mediante el Simple Network Management Protocol y otras herramientas como Multi Router Traffic Grapher que permiten obtener información en tiempo real de numerosos parámetros del sistema.



Visita <http://mrtg.xidus.net/> para ver una configuración real de MRTG.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) es un protocolo de gestión de red muy utilizado, que permite obtener información de dispositivos de red, memoria libre, uso de la CPU, detección de errores, establecer alarmas, estado de funcionamiento, etc. Por ejemplo, en la gestión de un hub, SNMP podría desconectar automáticamente los nodos que estén corrompiendo la red, o se podrían establecer alarmas para alertar al administrador de la red cuando en un dispositivo el tráfico de datos supere el umbral establecido, o se podrían buscar IPs duplicadas, etc.

La mayoría de los fabricantes de dispositivos de red soportan SNMP, para ello unos agentes localizados en el dispositivo recogen la información y la registran en una base de datos en forma de árbol, llamada MIB (Management Information Base). Los MIB tienen un formato estándar, de forma que aún siendo de fabricantes distintos, las herramientas SNMP puedan obtener información del dispositivo.

El protocolo SNMP está formado por un agente que se instala en los nodos que se desean monitorizar y un gestor que se instala en el ordenador encargado de monitorizar la red. El gestor es el que obtiene la información de los agentes. El gestor solicita a los agentes información sobre los dispositivos gestionados, y los agentes responden a dicha solicitud. Esto último tiene una excepción, mediante el comando SNMP trap, los agentes pueden enviar datos no solicitados al gestor, p.e. cuando hay un fallo eléctrico.

SNMP funciona bajo TCP/IP, lo cual significa que desde un sistema central se puede gestionar cualquier ordenador de la LAN, WAN o internet.

Management Information Base

Como puede verse en la figura 1, las bases de datos MIB tienen una estructura arborescente, algunas de las ramas más usadas para obtener información son: rmon, host, system, interfaces, ip, udp, tcp, private, etc.

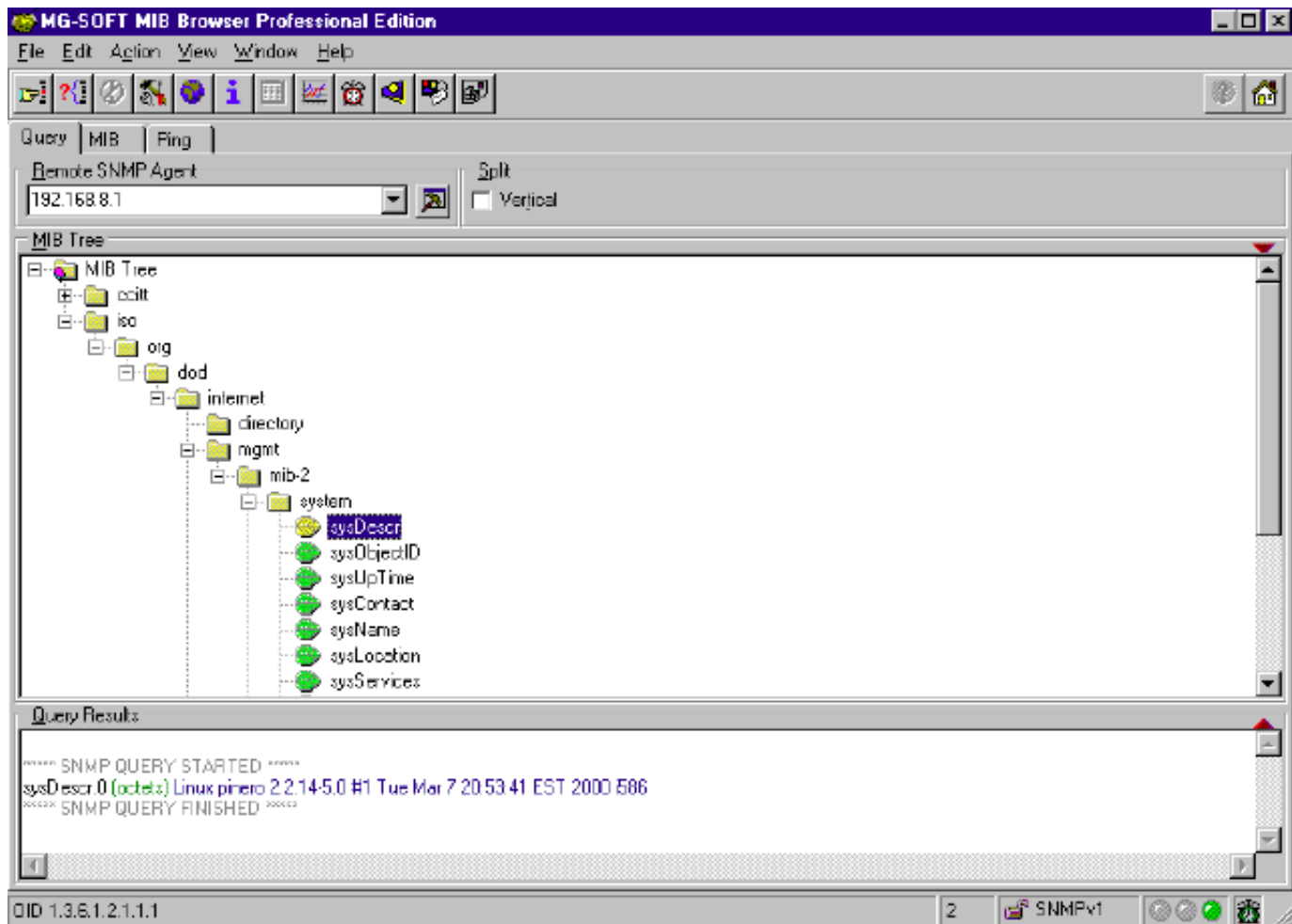


Figura 1

Para referenciar un elemento de la base de datos MIB podemos hacerlo por su nombre, por ejemplo:

.iso.org.dod.internet.mgmt.mib-2.system.sysDescr

o por su representación numérica llamada OID:

.1.3.6.1.2.1.1.1.

A las hojas del árbol MIB se les llama objetos.

Para navegar por el árbol MIB se utilizan browser, UCD-SNMP incluye el browser MIB *tkmib*.

SNMP en Linux

En Linux el protocolo SNMP está implementado con el software UCD-SNMP, todas las distribuciones incluyen este software, que suelen ser tres paquetes; *ucd-snmp*, *ucd-snmp-devel* y *ucd-snmp-util*. No obstante si prefieres bajarte el paquete con el código fuente del programa y compilarlo a tu gusto, la Home Page de UCD-SNMP está en <http://ucd-snmp.ucdavis.edu/>

UCD-SNMP incluye el agente *snmpd* y las herramientas de gestión *snmpget*, *snmpgetnext*, *snmpset*, *snmpwalk*, *snmpnetstat*, *snmptrapd* y *snmpstat*.

Instalado el software el fichero de configuración del agente *snmpd* está en */etc/snmp/snmpd.conf*, aquí se definen las *communities*, que son un par de claves que se utilizan para acceder al agente SNMP, normalmente

está configurado con *public* para lectura y *private* para escritura, por razones de seguridad obvias es conveniente cambiarlas.

Adjunto un ejemplo de configuración del agente:

```
file:/etc/snmp/snmpd.conf
```

```
-----
```

```
# Reglas de control de acceso al agente, establece quién puede
# conectarse, permisos
# de lectura, escritura, que ramas puedes ver, etc.
```

```
# Sólo será posible acceder al agente SNMP desde el host 192.168.8.1
# sec.name source community
com2sec local localhost secreto
com2sec mynetwork 192.168.8.1 secreto
```

```
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local
group MyROGroup v1 mynetwork
group MyROGroup v2c mynetwork
group MyROGroup usm mynetwork
```

```
# Ramas MIB que se permiten ver
# incl/excl subtree mask
view all included .1 80
```

```
#Establece permisos de lectura y escritura
# context sec.model sec.level match read write notif
access MyROGroup "" any noauth exact all none none
access MyRWGroup "" any noauth exact all all none
```

```
# System contact information
syslocation MiCasa
syscontact GarZa <garza@micasa.es>
```

Iniciar el agente con: `/etc/rc.d/initd./snmp start`

Las herramientas de gestión más usadas son `snmpget` y `snmpwalk` que a continuación comento, y que vamos a utilizar para comprobar si SNMP está funcionando correctamente:

`snmpget`: lee el valor de un objeto SNMP (hoja del árbol MIB), siguiendo con el ejemplo de la figura 1, vamos a obtener información sobre el sistema:

```
# snmpget localhost <community> system.sysDescr.0 ó snmpget localhost <community>
.1.3.6.1.2.1.1.1.0
```

y devuelve

```
system.sysDescr.0 = Linux pinero 2.2.14-5.0 #1 Tue Mar 7 20:53:41 EST 2000 i586
```

`snmpwalk`: puede leer una rama completa,

```
# snmpwalk localhost <community> system
```

y devuelve información sobre el sistema operativo, nombre del hosts, persona de contacto, localización, etc. Si no obtienes la información comentada es que SNMP tiene algún problema bien en la instalación o configuración.

Aunque en la distribución ucd-snmp se incluyen mibs de numerosos fabricantes, puede ser que necesites bajarte de la web del fabricante las mibs propietarias del dispositivo. Si necesitas monitorizar un router cisco, en la web del fabricante, podrás encontrar las mibs de todos sus modelos de router así como faq para su instalación.

Multi Router Traffic Grapher

Multi Router Traffic Grapher (MRTG) es una herramienta para monitorizar el tráfico en los interfaces de red y representar gráficamente en páginas html con gráficos GIF los datos que obtiene de agentes SNMP o scripts. Antes de comenzar la instalación debemos asegurarnos que tenemos instalado Perl, gd, libpng y zlib de lo contrario no se podrá realizar correctamente la compilación del programa. Una vez verificados estos requisitos, podemos descargar el paquete con el código fuente del programa desde la red, visitando la página <http://www.mrtg.org>

A continuación resumo los pasos a seguir en la instalación y configuración:

- 1.- Desempaquetar MRTG y proceder a compilar e instalar;

```
tar xvfz mrtg-2.9.10.tar.gz
cd mrtg-2.9.10
./configure
./make
./make install
```

Salvo que modifiques el path, se instala en /usr/local/mrtg-2.

2.- La configuración se realiza mediante un único fichero, normalmente denominado *mrtg.cfg*; para facilitarnos la creación de dicho fichero se puede utilizar el programa *cfgmaker*, éste detecta los dispositivos SNMP que tiene nuestro ordenador y genera el fichero de configuración adecuado para su monitorización:

```
# /usr/local/mrtg-2/cfgmaker <community>@localhost > /home/httpd/html/mrtg/mrtg.cfg
```

Lo normal es colocar los ficheros necesarios en el directorio mrtg en la estructura de directorios de nuestro servidor web.

- 3.- Editamos *mrtg.cfg* y añadimos la variable: *WorkDir: /home/httpd/html/mrtg*

- 4.- Ejecutar: */usr/local/mrtg-2/mrtg /home/httpd/html/mrtg/mrtg.cfg*

- 5.- Comprobar que se han generado correctamente las páginas html, ficheros log y los gráficos .gif.

- 6.- Para crear la página índice ejecutar:

```
/usr/local/mrtg-2/indexmaker /home/httpd/html/mrtg/mrtg.cfg > /home/httpd/html/mrtg/index.html
```

7.- Y ahora queda comprobar que todo ha funcionado como se esperaba, para ello en la barra de dirección de tu navegador escribe: *http://localhost/mrtg* y debe aparecer la página index.html que antes has

generado con indexmaker, con un gráfico por cada interfaz detectado, haciendo click en uno de los gráficos, se ofrece más información sobre el interfaz en cuestión, con datos diarios, semanales, mensuales y anuales. En la figura 2 puedes ver algunos gráficos de mi ordenador de casa:

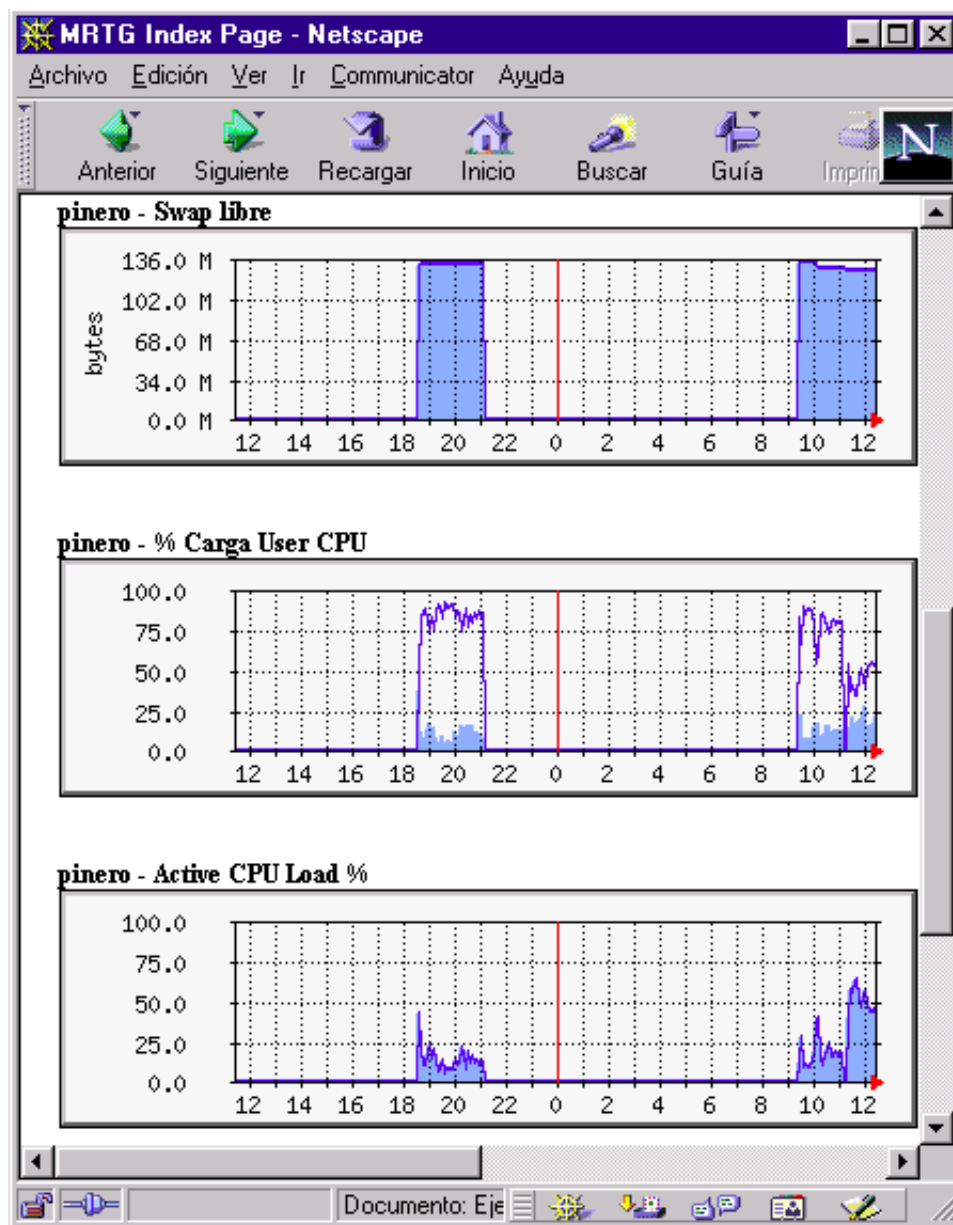


Figura 2

8.- Modificar el cron para que mrtg se ejecute cada 5 minutos; edita el fichero /etc/crontab y añade

```
*/5 * * * * root /usr/local/mrtg-2/bin/mrtg /home/httpd/html/mrtg/mrtg.cfg 2> /dev/null
```

En muchas ocasiones el fichero de configuración generado por cfgmaker será insuficiente, ya que desearíamos monitorizar otras variables del sistema, en estos casos habrá que editar el fichero mrtg.cfg y añadir a mano las opciones necesarias.

Aquí tienes un ejemplo con comentarios del fichero de configuración [mrtg.cfg](#). Para un estudio más detallado sobre su configuración visita la web de MRTG.

Algunos scripts a los que hago referencia en mrtg.cfg los puedes encontrar en <http://mrtg.xidus.net/info.shtml>, y los expuestos a continuación han sido realizados por el autor de este artículo:

- trafstat2.sh: proporciona datos de entrada y salida de servicios, haciendo uso de los contadores de ipchains.

- freemem.sh: memoria libre.

- loadcpu.sh: proporciona la carga del sistema de PC's con Microsoft Windows + SNMP4tPC.

- freemem2.sh: memoria libre en PCs con Microsoft Windows + SNMP4tPC.

Con esta configuración se puede obtener información sobre la carga de la CPU, memoria libre, número de procesos en ejecución, servidor web e información sobre otros ordenadores, en este caso con Microsoft Windows. Para ello se hacen llamadas a script o a objetos MIB que obtienen la información que se desea monitorizar.

Como se desprende de estos ejemplos, MRTG puede obtener información de scripts siempre y cuando ésta se devuelva en el formato que MRTG espera.

SNMP en Microsoft Windows

En la web de SNMP4tPC (<http://www.wtcs.org/snmp4tpc/>) se ofrece soporte SNMP para Microsoft Windows 9x/NT/2000, NetWare y MRTG. Para monitorizar ordenadores con Windows NT 4:

- instalar el servicio SNMP, para ello en Panel de Control/Red, seleccionar Servicio y añadir el Servicio SNMP.

- Configurar SNMP: email de contacto, ubicación del PC, nombre de la comunidad, seguridad, etc.

- Instalar el service pack, esto es obligatorio de lo contrario SNMP no funcionará correctamente.

- Descargar e instalar SNMP4NT-STD.EXE que proporciona numerosos contadores para estadísticas.

Hecho esto desde MRTG en nuestro Linux podremos monitorizar los ordenadores de nuestra red local, y saber en que estado se encuentran y cual es el uso que se está haciendo de ellos, lo cual servirá para tomar decisiones como p.e. la asignación de nuevos recursos.

En la web antes citada podrás encontrar algunas utilidades para Microsoft Windows como getif, snmputil, Mibs.zip, etc.

Conclusión

Simple Network Management Protocol y Multi Router Traffic Grapher, junto al ingenio de un buen administrador de red para crear script, constituyen una herramienta muy potente para monitorizar toda la red, que además de utilizarlos para saber en tiempo real que ocurre y poder detectar cualquier anomalía, también nos será útil para saber el uso que se hace de los recursos informáticos.

Referencias:

- <http://ucd-snmp.ucdavis.edu/>: software SNMP para GNU/Linux
- <http://www.mrtg.org>: web de MRTG.
- <http://mrtg.xidus.net/info.shtml>: ejemplos sobre MRTG/SNMP
- El artículo "Administración y Mantenimiento de Redes con Linux" aparecido en enero de 1998 en LinuxFocus.
- <http://www.wtcs.org/snmp4tpc/> SNMP4tPC; SNMP para Microsoft Windows
- scotty (<http://wwwhome.cs.utwente.nl/~schoenw/scotty/>): gestor de red para Linux (tkined).
- Otros monitores de red: Big Brother (<http://bb4.com/>) y ntop (<http://www.ntop.org/>).

Software utilizado: RedHat 6.2, kernel 2.2.14-5, ucd-snmp-4.2-1 y mrtg-2.9.10

Posibles mejoras:

- Explicar más a fondo las opciones de configuración de mrtg.
 - El browser tkmb no funciona, aparece un error sobre Perl, por eso he utilizado una imagen de un browser para Microsoft Windows. :((
-

garza@thelinuxmaster.org