

Monitorización del Sistema

Tabla de Contenidos

9. Monitorización del Sistema.....	2
Monitorización de la actividad de Red.....	2
Planificación de progresos.....	2
Protección contra virus.....	3
Soporte de Impresoras.....	3
Gestión del espacio de almacenamiento.....	4
9.1 Monitorización gráfica del tráfico de red.....	4
9.2 Simple Network Management Protocol.....	7
Management Information Base.....	7
SNMP en Linux.....	7
Multi Router Traffic Grapher.....	9
SNMP en Microsoft Windows	11
Conclusión.....	12
Referencias:.....	13



9. Monitorización del Sistema.

Monitorización de la actividad de Red.

Las funciones de la monitorización de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad de red, la detección de eventos y la comunicación de alertas al personal responsable del buen funcionamiento de la red.

Los eventos típicos que son monitorizados suelen ser:

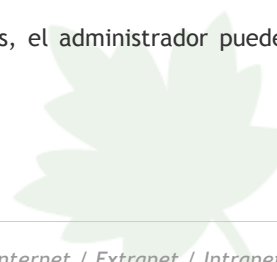
- Ejecución de tareas como pueden ser realización de copias de seguridad o búsqueda de virus.
- Registro del estado de finalización de los procesos que se ejecutan en la red.
- Registro de los cambios que se producen en el inventario de hardware.
- Registro de las entradas y salidas de los usuarios en la red.
- Registro del arranque de determinadas aplicaciones.
- Errores en el arranque de las aplicaciones.
- etc.

En función de la prioridad que tengan asignados los eventos y de la necesidad de intervención se pueden utilizar diferentes métodos de notificación como son:

- Mensajes en la consola: se suelen codificar con colores en función de su importancia.
- Mensajes por correo electrónico: conteniendo el nivel de prioridad y el nombre e información del evento.
- Mensajes a móviles: cuando el evento necesita intervención inmediata se suele comunicar a los técnicos de guardia a través de este método.
- Además de los eventos, otra característica importante es la monitorización del tráfico de red:
- Se toman nuevas medidas sobre aspectos de los protocolos, colisiones, fallos, paquetes, etc.
- Se almacenan en BBDD para su posterior análisis.
- Del análisis se obtienen conclusiones, bien para resolver problemas concretos o bien para optimizar la utilización de la red.

Planificación de progresos

En vez de tener que recordar y realizar trabajos periódicos o en horas no laborables, el administrador puede programar un agente que realiza las tareas programadas en los momentos previstos.



Además, estos agentes recogen información sobre el estado de finalización de los procesos para un posterior análisis por el administrador.

Los procesos típicos que se suelen planificar son: copias de seguridad, búsqueda de virus, distribución de software, impresiones masivas, etc.

La planificación de procesos permite también aprovechar los períodos en que la red está más libre como las noches y los fines de semana.

Los planificadores como AT de Windows NT y CRON de Unix permiten procesos especificando un momento determinado y una frecuencia.

Normalmente también se suelen usar scripts para programar a los agentes planificadores.

Protección contra virus

La protección contra la entrada de virus en la red se suele hacer mediante la utilización de paquetes especiales basados en una parte servidora y un conjunto de agentes distribuidos en los puestos de trabajo.

La parte servidora realiza las tareas de actualización contra nuevos virus, realiza tareas de registro de virus, comunicación de alarmas al administrador, comunicación con otros servidores distribuidos en la red con software antivirus, protección de los discos y ficheros de los propios servidores, etc.

Los agentes por su parte evitan la entrada de virus en los propios puestos de trabajo comunicando al servidor la detección de los virus y eliminándolos automáticamente siempre que sea posible.

Soporte de Impresoras

La gestión centralizada de impresoras en la red permite reducir el tiempo y el esfuerzo que necesitan los usuarios para configurar la impresión desde unos puertos de trabajo y también permiten al administrador realizar una gestión unificada de todas las impresoras de la red.

Las actividades relacionadas con el soporte de impresoras son dos:

1. Las relacionadas con el manejo de las impresoras por parte del administrador.
2. Las relacionadas con la selección de impresoras e impresión por parte de los usuarios.

El modo de operar suele ser el siguiente:

1. El administrador da de alta las impresoras en la red seleccionando los servidores que actuarán de spoolers, identificándolos con un nombre y asociando el driver correspondiente para su utilización.

2. Posteriormente el administrador, establece las condiciones de acceso como permisos a los usuarios, horario de acceso a las impresoras, etc.
3. El usuario después selecciona las impresoras de las que tiene acceso permitido y las instala en un puerto de trabajo de forma remota y transparente.
4. Cuando el usuario imprime también tiene acceso a las colas de impresión de forma que puede añadir o eliminar trabajos de su propiedad.
5. El administrador a través de la consola y los agentes de impresión monitoriza la actividad de las impresoras y soluciona problemas que puedan surgir.

Gestión del espacio de almacenamiento

La utilización masiva de servidores de ficheros y BBDD en las redes actuales han hecho del espacio de almacenamiento un recurso común a los usuarios y un elemento escaso que hay que optimizar.

El administrador utiliza agentes que recolectan información sobre el grado de ocupación de los discos con objeto de tomar decisiones al respecto de la redistribución de ficheros y de la adquisición de nuevos discos.

La extracción de información que realiza el agente suele ser a nivel de:

- Partición: utilización del espacio de la partición (poco nivel de detalle)
- Directorios: grado de utilización del espacio para los directorios.
- Ficheros: tamaño que ocupan los ficheros.

Al igual que con otras actividades de administración se suelen programar una serie de eventos consistente en ciertos límites que cuando son sobrepasados elevan una alarma que es comunicada al administrador a través de un mensaje en la consola, un correo electrónico o un mensaje a un móvil por ejemplo.

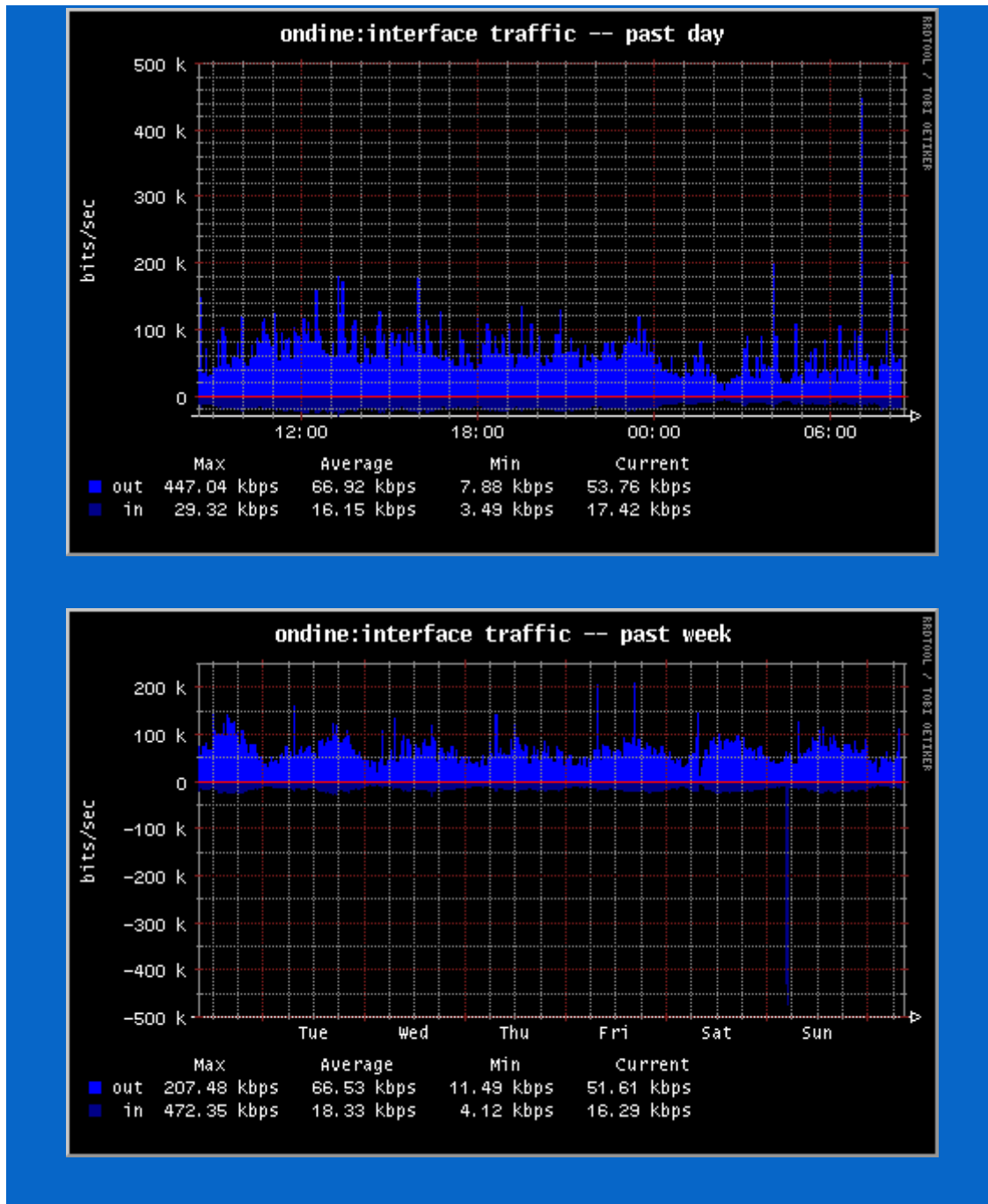
La tarea de recogida de información normalmente se puede hacer en background sin afectar a los procesos en ejecución aunque también pueden ser planificados para su posterior ejecución.

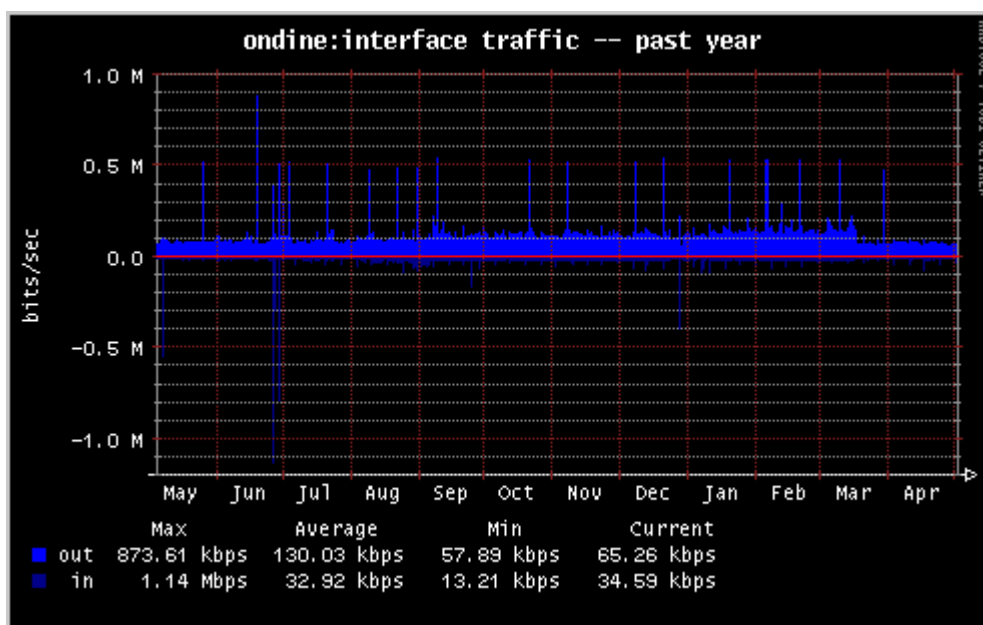
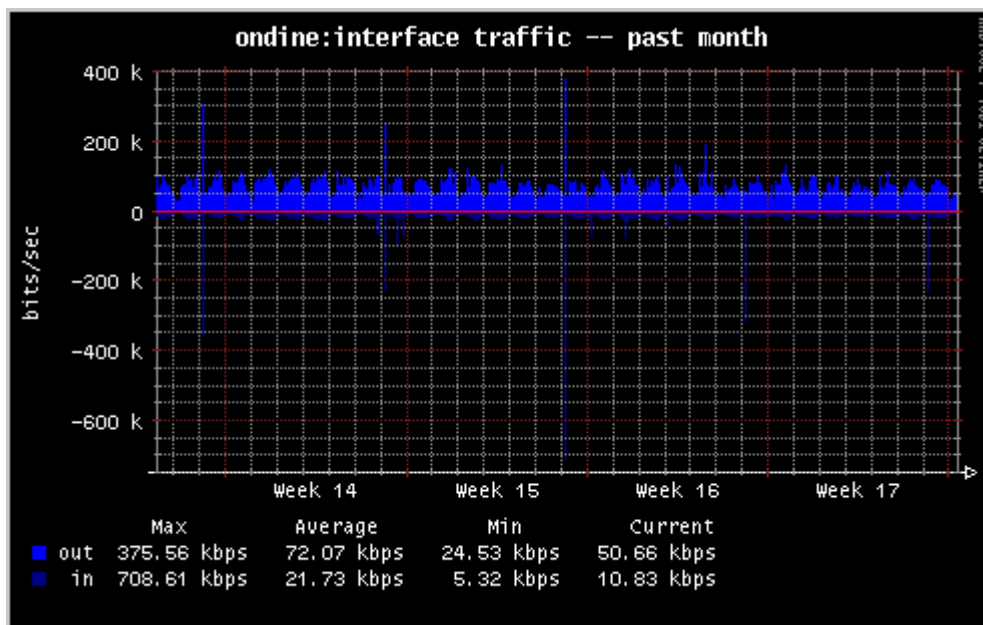
9.1 Monitorización Gráfica Del Tráfico De Red

Una de las muchas tareas importantes que corresponden a un administrador de redes 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.

Podemos ver una configuración real en <http://spackle.xidus.net/>





0.115 sec to top of layout loop

Generated 24 images, 0 from cache, in 2.679 sec, 2.459 sec in rrd_graph

2.680 sec to footer

9.2 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

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`



- ucd-snmp-util

<http://ucd-snmp.ucdavis.edu/>

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

Instalado el software el fichero de configuración del agente `snmpd` está en:

`/etc/snmp/snmpd.conf`

Aquí se definen las *comunidades*, 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.

Aquí podemos ver 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 192.168.0.1
# 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 RedLocal
syscontact hann <jmmolinafuentes@wanadoo.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:

: 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
```

```
# 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 Mandrake 10.0 #1 Tue Mar 7 20:53:41 EST 2000 i586
```

: puede leer una rama completa,

```
snmpwalk
```

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 para facilitarnos la creación de dicho fichero se puede utilizar el programa éste detecta los dispositivos SNMP que tiene nuestro ordenador y genera el fichero de configuración adecuado para su monitorización:

```
mrtg.cfg;
cfgmaker,
# /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 y añadimos la variable:

```
mrtg.cfg
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:

y debe aparecer la página index.html que antes has

<http://localhost/mrtg>

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 desearemos 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. Para un estudio más detallado sobre su configuración visita la web de MRTG.***mrtg.cfg***

Algunos scripts a los que hago referencia en mrtg.cfg los puedes encontrar en <http://mrtg.xidus.net/info.shtml> y algunos los expondremos a continuación:

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 por ejemplo, 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 a 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:

: software SNMP para GNU/Linux

<http://ucd-snmp.ucdavis.edu/>

: web de MRTG.

<http://www.mrtg.org>

: ejemplos sobre MRTG/SNMP

<http://mrtg.xidus.net/info.shtml>

El artículo "Administración y Mantenimiento de Redes con Linux" aparecido en enero de 1998 en LinuxFocus.

SNMP4tPC; SNMP para Microsoft Windows

<http://www.wtcs.org/snmp4tpc/>

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

