

UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA



CARRERA:
LIC. CIENCIAS DE LA COMPUTACIÓN

CÁTEDRA:
REDES I

CATEDRÁTICO:
ING. MANUEL FLORES VILLATORO

PROYECTO:
"MONITOREO DE EQUIPOS CON SNMP"

ALUMNOS:

N	Apellido	Nombre	Carne	Participación
01	Miranda Ortiz	Miguel Angel	MO02110308	100%
02	Palacios Lemus	Rene Jose Angel	PL01121606	100%
03	Rodriguez Alvarado	Fabio Eduardo	RA02110575	100%
04	Orante Sosa	Jorge Alberto	OS01132914	100%

FECHA:

SAN SALVADOR, 31 DE MAYO DE 2014

Índice de contenido

INTRODUCCIÓN.....	1
OBJETIVOS.....	2
OBJETIVO GENERAL.....	2
OBJETIVOS ESPECÍFICOS.....	2
MARCO TEÓRICO.....	2
¿Qué es SNMP?	3
Ventajas del SNMP.....	3
Desventajas del SNMP.....	3
Diagrama de red.....	4
QUÉ PERMITE CONTROLAR Y MONITOREAR EL PROCOTOLO SNMP.....	5
El proceso de envío de un mensaje SNMP es el siguiente:.....	6
Diagrama de funcionamiento de envío de mensajes en snmp.....	8
Los cinco tipos de mensajes SNMP intercambiados entre los agentes y los administradores, son:.....	9
Las MIBs se dividen en 8 niveles que corresponde a los 8 diferentes tipos de objetos que pueden ser descriptos en la MIB.....	10
Listado de actividades.....	12
ORGANIGRAMA DE ACTIVIDADES.....	13
Factibilidad del proyecto.....	14
Factibilidad técnica.....	14
Factibilidad económica.	14
Factibilidad operativa.....	14
Factibilidad legal.....	14
Presupuesto del proyecto.....	15
ANEXOS.....	16
Conclusiones.....	28
FUENTES BIBLIOGRÁFICAS.....	29

INTRODUCCIÓN

Simple Network Management Protocol (SNMP), o Protocolo Simple de Red. Es un protocolo que facilita el intercambio de información de administración entre dispositivos de red. Permite supervisar el funcionamiento de la red, buscar y resolver sus problemas y planear su crecimiento, también podemos mencionar que la SNMP es un administrador de redes ya que facilita en un gran número la conexión de las redes computacionales.

En Agosto de 1988, la especificación de SNMP aparece y rápidamente es adoptada por el creciente mundo de las redes. SNMP tenía que ser lo bastante simple para que lo pudiera implementar en cualquier dispositivo que se imaginaran, y lo bastante potente como para permitir la gestión remota de los equipos. Los complejos sistemas de gestión (como HP Openview) se podían desarrollar utilizando sólo SNMP como sistema de comunicación. El propósito inicial del SNMP era integrar la gestión de diferentes tipos de redes en un diseño simple que sobrecargara poco la gestión de red.

Soportar SNMP era una necesidad para cualquier PC que se pudiera conectar a Internet entonces, ¿qué se puede hacer con SNMP? Con SNMP se puede monitorizar el estado de un enlace punto a punto para detectar cuándo está congestionado y tomar así las medidas oportunas; se puede hacer que una impresora alerte al administrador cuando se ha quedado sin papel, o que un servidor envíe una alerta cuando la carga de su sistema se incrementa significativamente. SNMP también permite la modificación remota de la configuración de dispositivos, de forma que se podría modificar las direcciones IP de un ordenador a través de su agente SNMP, u obligar a la ejecución de comandos (si el agente ofrece las funcionalidades necesarias).

OBJETIVOS

OBJETIVO GENERAL

- Analizar de manera breve el uso del monitoreo mediante SNMP, mostrando su instalación y configuración mediante el desarrollo de esta actividad.

OBJETIVOS ESPECÍFICOS

- Reconocer los beneficios de uso que se obtienen mediante la implementación de un sistema de monitoreo de red como lo es el protocolo SNMP.
- Identificar las características principales del SNMP, así como el uso de este con bajos costes.
- Conocer el funcionamiento de protocolo SNMP de una forma rápida y sencilla.

MARCO TEÓRICO

¿Qué es SNMP?

El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

Las versiones de SNMP más utilizadas son dos: SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Ambas versiones tienen un número de características en común, pero SNMPv2 ofrece mejoras, como por ejemplo, operaciones adicionales.

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

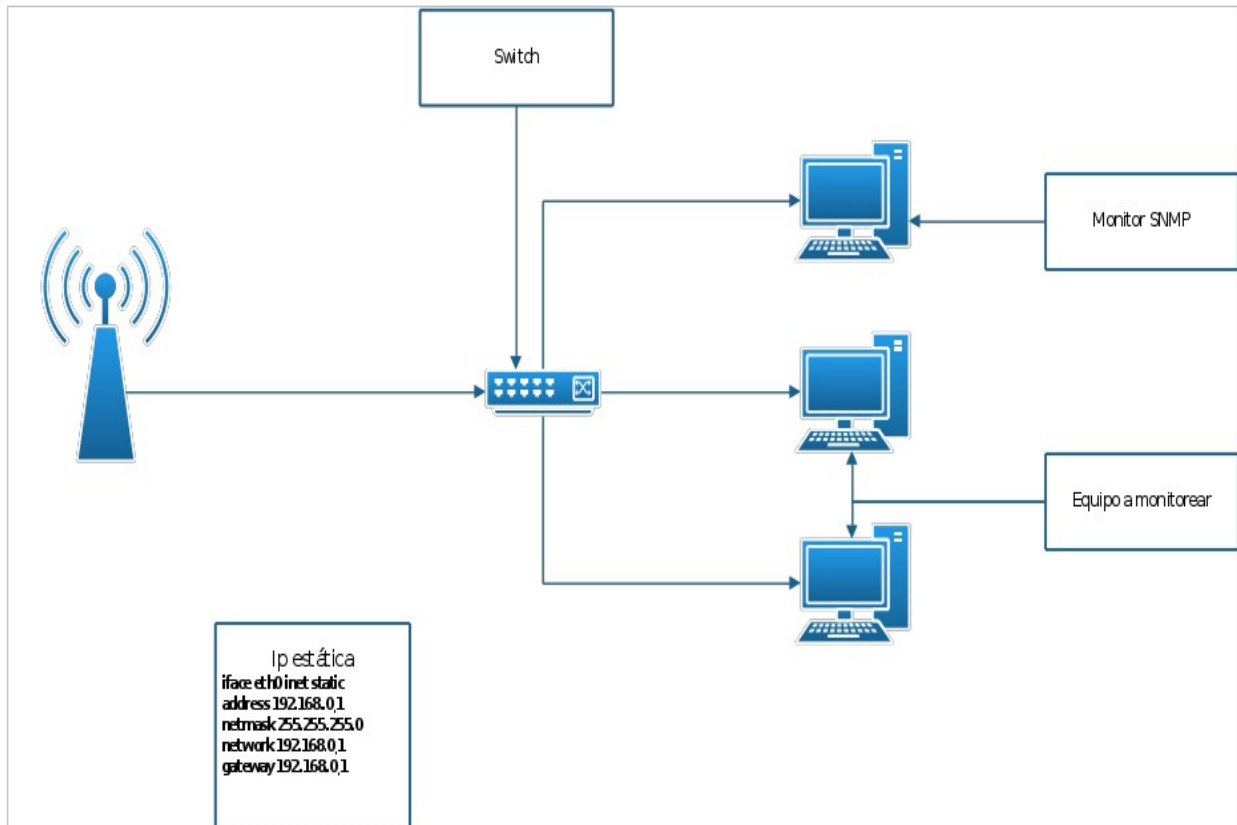
Ventajas del SNMP

- Simplicidad
- Requiere menor procesamiento que el CMPI
- Ampliamente usado y probado
- Está integrad en muchos productos actuales

Desventajas del SNMP

- Aspectos de seguridad
- Funcionalidad reducida (No facilita la innovación de operaciones, creación de objetos)
- Genera mucho tráfico por la red
- No facilita el diseño de las MIBs
- Es poco adaptable para gestión jerárquica

Diagrama de red.



QUÉ PERMITE CONTROLAR Y MONITOREAR EL PROCOTOLO SNMP

Las redes tienen una gran importancia ya que mientras más grandes son, tienden a tener sistemas complejos soportando más aplicaciones y usuarios.

A medida que estas redes crecen en escala, dos factores comienzan a evidenciarse:

- La red, sus recursos asociados y las aplicaciones distribuidas comienzan a hacerse indispensables.
- Muchos dispositivos pueden fallar, inutilizando la red o una porción de ella, o la carga sobre la red, puede ir degradando el desempeño hasta niveles inaceptables.

Para dar respuesta a estas necesidades han surgido aplicaciones estándar que permiten administrar las redes, cubriendo servicios, protocolos y bases de información de gestión, tal es el caso de un sistema de gestión de red:

“Es una colección de herramientas para el monitoreo y control de redes el cual es integrado en el siguiente sentido:

- Una sencilla interfaz para el operador con un poderoso y amigable colección de comandos que permita ejecutar la mayoría o todas las tareas de gestión de red.
- Proveer una visión de la red en su totalidad como una arquitectura unificada.” William Stallings. SNMP v2. 1999

“A grandes rasgos una gestión de red lo que hace es planificar, organizar, supervisar y controlar los elementos de comunicaciones para garantizar un nivel de servicio.”

Un sistema de gestión de red está compuesto por:

- Estación de gestión
- Agente
- Base de datos de información de gestión
- Protocolo de gestión de red

La administración de una red puede ser difícil por dos razones:

- Primera, la mayor parte de las redes son heterogéneas, es decir, la red consta de componentes de hardware y software fabricado por varias compañías. Los pequeños errores de un proveedor pueden hacer incompatibles los componentes.

- Segunda, las redes en su mayor parte son grandes. La detección de las causas de un problema de comunicación puede ser muy difícil si el problema sucede entre computadoras de sitios diferentes.

Aunque el hardware de red y el software de protocolo deben tener mecanismos para detectar automáticamente fallas y retransmitir paquetes, los administradores tienen la tarea de detectar y corregir los problemas subyacentes porque las retransmisiones reducen el desempeño de todas las computadoras que comparten la red.

Sin embargo es el software como administración de red que permitirá al administrador supervisar y controlar los componentes; por ejemplo, investigar y determinar el funcionamiento de dispositivos como hosts, enrutadores, conmutadores, hub, Switches y Routers determinando su estado y obtener estadísticas sobre las redes a las que se conectan, también controlar tales dispositivos cambiando las rutas y configurando interfaces.

Hoy día existen diferentes aplicaciones y herramientas para la administración y monitoreo de red utilizando el protocolo SNMP, además de evaluar y estudiar el funcionamiento de la red también se permite para equipos de conexión como el Hub, Switches y Router.

El proceso de envío de un mensaje SNMP es el siguiente:

Transmisión:

- Se construye UDP
- Se invoca al servicio de autenticación con la dirección de transporte,
- Se construye el mensaje SNMP
- Se codifica

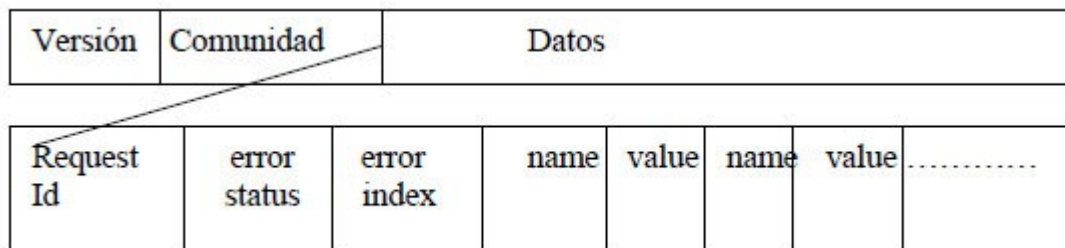
Recepción:

- Comprobación sintáctica
- Verificación de la versión utilizada
- Autenticación, (verifica si falla)
- Proceso de petición

Mensajes SNMP

Mensaje SNMP ← → Datagrama UDP

Disminuye procesado de mensajes y complejidad del agente



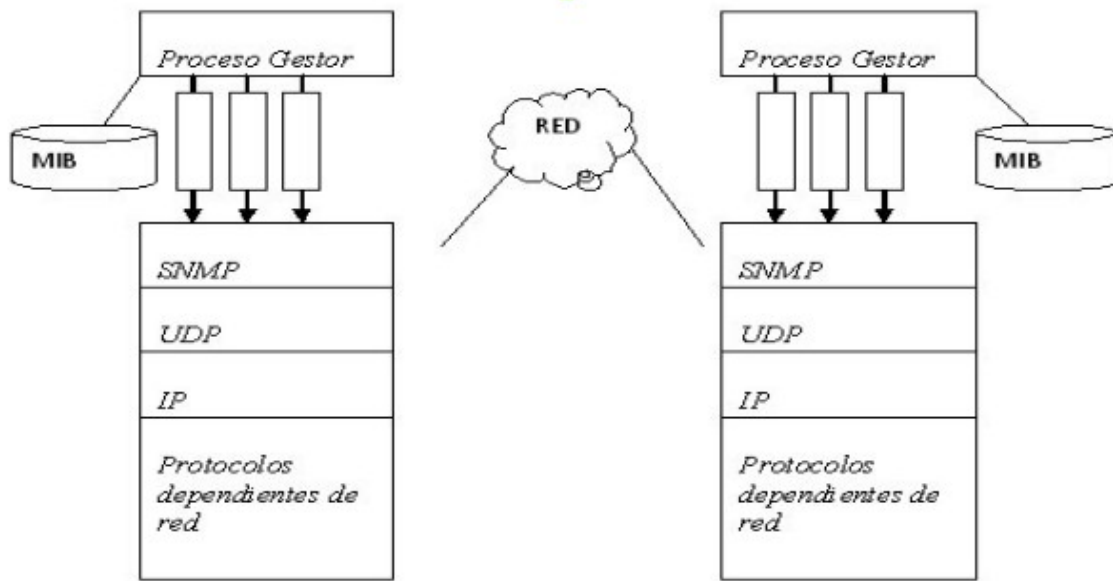
Los mensajes SNMP son recibidos en el puerto UDP 161

Traps: puerto 162

Operaciones que se realizan en el SNMP

- GetRequest: Petición de valores específicos de la MIB
- GETNextRequest: Proporciona un medio para moverse por la MIB. Petición del objeto siguiente a uno dado de la MIB
- GetResponse: Devuelve los valores solicitados por las operaciones anteriores
- SetRequest: Permite asignar un valor a una variable
- Traps: Permite a los agentes informar de sucesos inusuales

Diagrama de funcionamiento de envío de mensajes en snmp



Componentes Básicos.

Una red administrada a través de SNMP consiste de tres componentes claves:

- Dispositivos administrados.
- Agentes.
- Sistemas administradores de red (NMS's).

Un dispositivo administrado es un nodo de red que contiene un agente SNMP y reside en una Red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras.

Un agente es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

Un NMS ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's deben existir en cualquier red administrada.

Los cinco tipos de mensajes SNMP intercambiados entre los agentes y los administradores, son:

- Get Request: Una petición del Administrador al agente para que envíe los valores contenidos en el MIB (base de datos).
- Get Next Request: Una petición del Administrador al Agente para que envíe los valores contenidos en el MIB referente al objeto siguiente al especificado anteriormente.
- Get Response: La respuesta del Agente a la petición de información lanzada por el Administrador.

- Set Request: Una petición del Administrador al Agente para que cambie el valor contenido en el MIB referente a un determinado objeto.

- Trap: Un mensaje espontáneo enviado por el Agente al Administrador, al detectar una condición predeterminada, como es la conexión/desconexión de una estación o una alarma.

MIB: (Management Information Base – base de manejo de información) es una base de datos que contiene cada agente y cada NMS ubicados en la red donde se almacenan los objetos y atributos a administrar, cada uno de estos tiene un OID (identificador de objeto) diferente el cual es asignado de la estructura jerárquica de la MIB donde son los últimos dígitos que cambian y hacen la diferencia entre cada objeto. Las MIBs utilizan la SMI para definir las reglas usadas para describir los objetos, la descripción de estos objetos están compuestas por cinco campos los cuales son:

1. Descripción del objeto: como su nombre lo indica da una descripción del objeto, contiene un identificador. Todo objeto que puede ser descrito en una MIB estándar es identificado en el árbol global, el árbol global muestra como las diferentes organizaciones están interrelacionadas
2. Sintaxis: usa un subconjunto de ASN.1 (Abstract Syntax Notation Number – Notación Sintáctica Abstracta Numero 1; lenguaje descriptivo) conteniendo unos valores tales como enteros, cadena de octetos, identificador de objeto, nulo, tipos construidos, tipos definidos.
3. Definición: describe en texto planos de las reglas asociados con el tipo de objeto.
4. Acceso: acceso permitido a cada uno de los objetos descritos en la MIB tales como solo lectura, solo escritura, lectura-escritura, sin acceso.
5. Estatus: define si la descripción del objeto es obligatorio, opcional u obsoleto.

Las MIBs se dividen en 8 niveles que corresponde a los 8 diferentes tipos de objetos que pueden ser descriptos en la MIB.

1. Systems: información del sistema es opcional.
2. Interfaces: información de cómo los dispositivos están conectados en la red es opcional en la V3 y obligatoria para la V2.
3. Address translation: mapeo de las direcciones de red a las direcciones físicas.
4. Ip: (Internet Protocol) contador de paquetes, es obligatorio.
5. Icmp: (Internet Control Message Protocol) tipo de mensaje, es obligatorio.

6. Tcp: (Transmission Control Protocol) conexiones abierta obligatorio en tcp.

7. Udp: (User Datagram Protocol) intercambio de datagramas y estadísticas es obligatorio en conexiones UDP.

8. EGP: (Exterior Gateway Protocol) usado para intercambiar información de enrutamiento entre sistemas autónomos.

Sistema Operativo GNU/LINUX.

GNU/Linux es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre similar a Unix denominado Linux con el sistema GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (Licencia Pública General de GNU, en inglés: General Public License) y otra serie de licencias libres.

Herramientas a utilizar.

-Sistema Operativo GNU/Linux.

-Una computadora (donde se instalará el servicio de monitoreo)

-Una computadora cliente(a quién se monitoreara)

-Switch

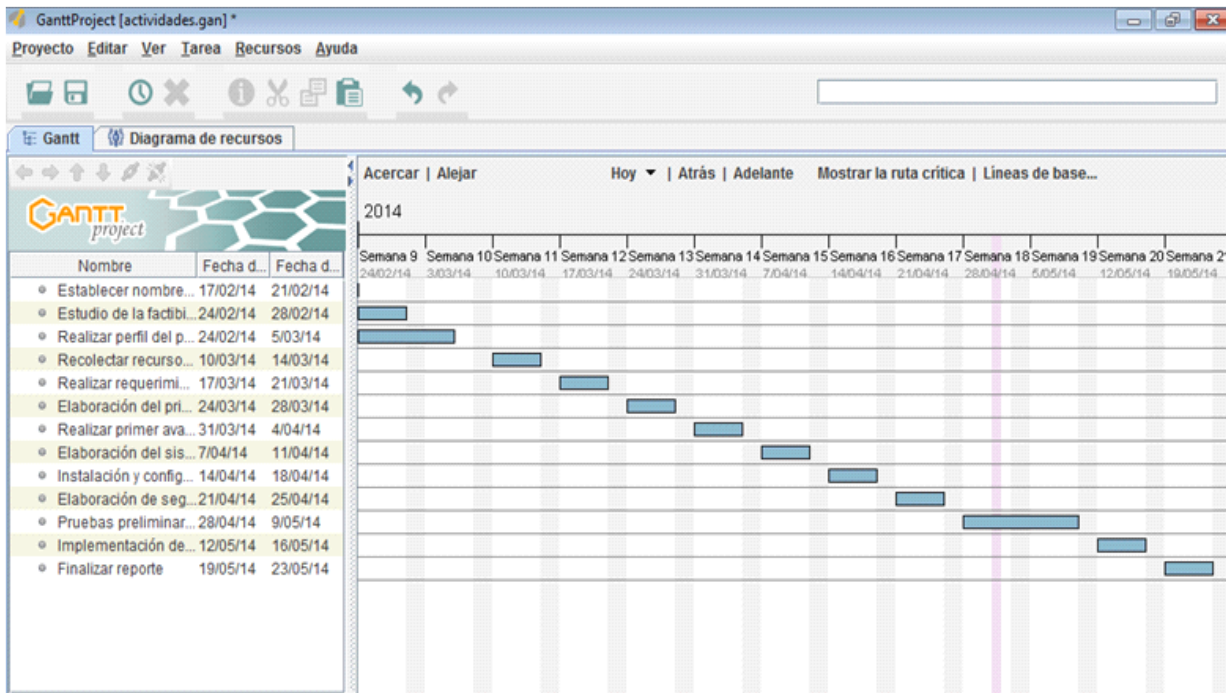
-cable UTP

-conectores RJ45

Listado de actividades.

- Elección del proyecto
- Estudio de la factibilidad del proyecto.
- Realizar perfil de proyecto.
- Recolectar recursos con los que se cuenta.
- Realizar requerimientos y operaciones necesarias.
- Elaboración del primer avance del prototipo.
- Realizar primer avance del reporte final.
- Elaboración del sistema para el monitoreo.
- Instalación y configuración de clientes snmp.
- Elaboración de segundo avance del prototipo.
- Pruebas preliminares de la implementación del sistema.
- Implementación del monitoreo.
- Finalizar reporte.

ORGANIGRAMA DE ACTIVIDADES



Factibilidad del proyecto.

Factibilidad técnica.

Estas serán todas aquellas metodologías y todo el software que usaremos en la implementación de nuestro proyecto para un buen funcionamiento.

Factibilidad económica.

La economía es un factor muy importante en la creación de un proyecto, pero en nuestro caso utilizaremos software libre y ya contamos con nuestras máquinas listas para la ejecución y prueba de nuestro sistema.

Factibilidad operativa.

La determinación de que un nuevo sistema sea de agrado y se utilice como se debe, esto será lo que el proyecto deberá cumplir.

Factibilidad legal.

Este proyecto se realizara con software libre bajo la Licencia Pública General de GNU (GPL) versión 3.

Presupuesto del proyecto.

Nombre	Imagen	Características	Unidades	Precio	Total
Computadora		Herramienta por la cual realizaremos las pruebas del SNMP	2	\$240	\$480
Switch		Medio que es importante en la comunicación entre computadoras	1	\$20	\$20
Cable de red		Medio de transferencia de datos ya sea entre dos maquinas o un switch y maquina	20 mts	\$0.30 el metro	\$6
Conectores		Lo usaremos para conectar redes de cableado estructurado	10	\$0.25 el conector	\$2.50
Protectores		Protecciones para los extremos del cable de red y no dañar las pestañas	10	\$0.50	\$5
Tarjeta de red		Medio por el cual compartiremos recursos.	2	\$7	\$14
Tenaza		Herramienta para la elaboración de los cables de red.	1	\$10	\$10

ANEXOS

1.instalar cacti snmp snmpd

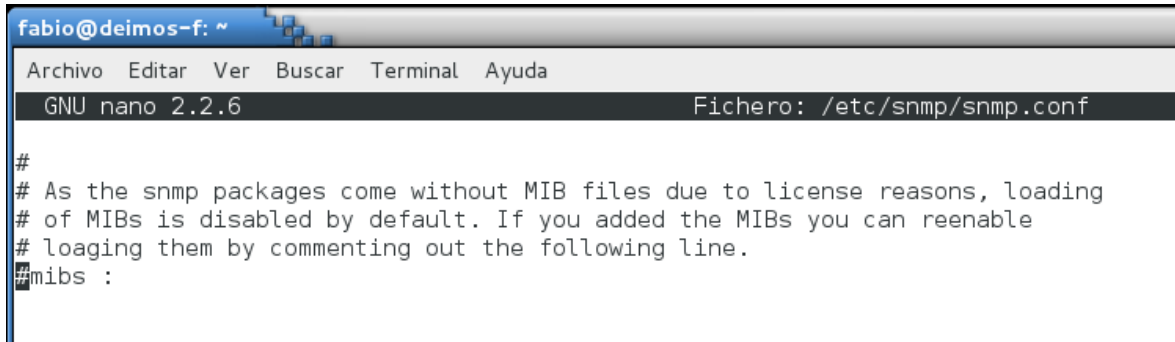
```
# apt-get install cacti snmp snmpd rrdtool
```

2.configurar archivo snmp.conf

```
# nano /etc/snmp/snmp.conf
```

comentando la ultima linea

mibs:

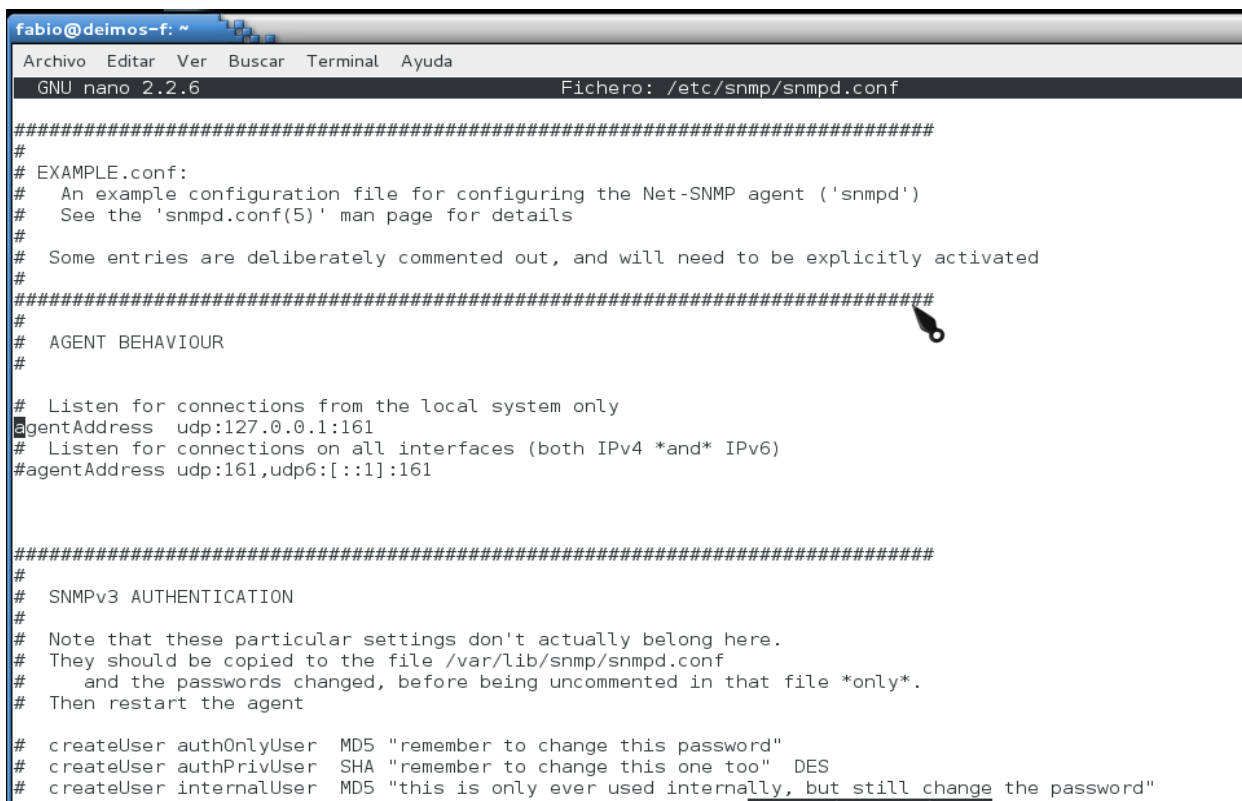


```
fabio@deimos-f: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Fichero: /etc/snmp/snmp.conf
#
# As the snmp packages come without MIB files due to license reasons, loading
# of MIBs is disabled by default. If you added the MIBs you can reenable
# loaging them by commenting out the following line.
#mibs :
```

3.configurar archivo snmpd.conf

```
# nano /etc/snmp/snmpd.conf
```

4.



```
fabio@deimos-f: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Fichero: /etc/snmp/snmpd.conf
#####
#
# EXAMPLE.conf:
# An example configuration file for configuring the Net-SNMP agent ('snmpd')
# See the 'snmpd.conf(5)' man page for details
#
# Some entries are deliberately commented out, and will need to be explicitly activated
#
#####
#
# AGENT BEHAVIOUR
#
# Listen for connections from the local system only
agentAddress udp:127.0.0.1:161
# Listen for connections on all interfaces (both IPv4 *and* IPv6)
#agentAddress udp:161,udp6:[::1]:161

#####
#
# SNMPv3 AUTHENTICATION
#
# Note that these particular settings don't actually belong here.
# They should be copied to the file /var/lib/snmp/snmpd.conf
# and the passwords changed, before being uncommented in that file *only*.
# Then restart the agent
#
# createUser authOnlyUser MD5 "remember to change this password"
# createUser authPrivUser SHA "remember to change this one too" DES
# createUser internalUser MD5 "this is only ever used internally, but still change the password"
```

5.

```
fabio@deimos-f: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Fichero: /etc/snmp/snmpd.conf

# then remember to update the other occurrences in this example config file to match.

#####
#
# ACCESS CONTROL
#
view systemonly included .1.3.6.1.2.1.1 # system + hrSystem groups only
view systemonly included .1.3.6.1.2.1.25.1
rocommunity public localhost # Full access from the local host
rocommunity public default -V systemonly # Default access to basic system info
#rocommunity public 10.0.0.0/16 # Full access from an example network
# Adjust this network address to match your local
# settings, change the community string,
# and check the 'agentAddress' setting above
#rocommunity secret 10.0.0.0/16
rouser authOnlyUser # Full read-only access for SNMPv3
# Full write access for encrypted requests
# Remember to activate the 'createUser' lines above
#rwuser authPrivUser priv
# It's no longer typically necessary to use the full 'com2sec/group/access' configuration
# r[ou]ser and r[ow]community, together with suitable views, should cover most requirements
```

6.

```
fabio@deimos-f: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Fichero: /etc/snmp/snmpd.conf

#####
#
# SYSTEM INFORMATION
#
# Note that setting these values here, results in the corresponding MIB objects being 'read-only'
# See snmpd.conf(5) for more details
sysLocation red.sv
sysContact me@example.org # Application + End-to-End layers
sysServices 72

#
# Process Monitoring
#
proc mountd # At least one 'mountd' process
proc ntalkd 4 # No more than 4 'ntalkd' processes - 0 is OK
proc sendmail 10 1 # At least one 'sendmail' process, but no more than 10

# Walk the UCD-SNMP-MIB::prTable to see the resulting output
# Note that this table will be empty if there are no "proc" entries in the snmpd.conf file

#
# Disk Monitoring
#
# 10MBs required on root disk, 5% free on /var, 10% free on all other disks

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt
```

7.configurar archivo snmpd

nano /etc/default/snmpd

editar line en el cliente

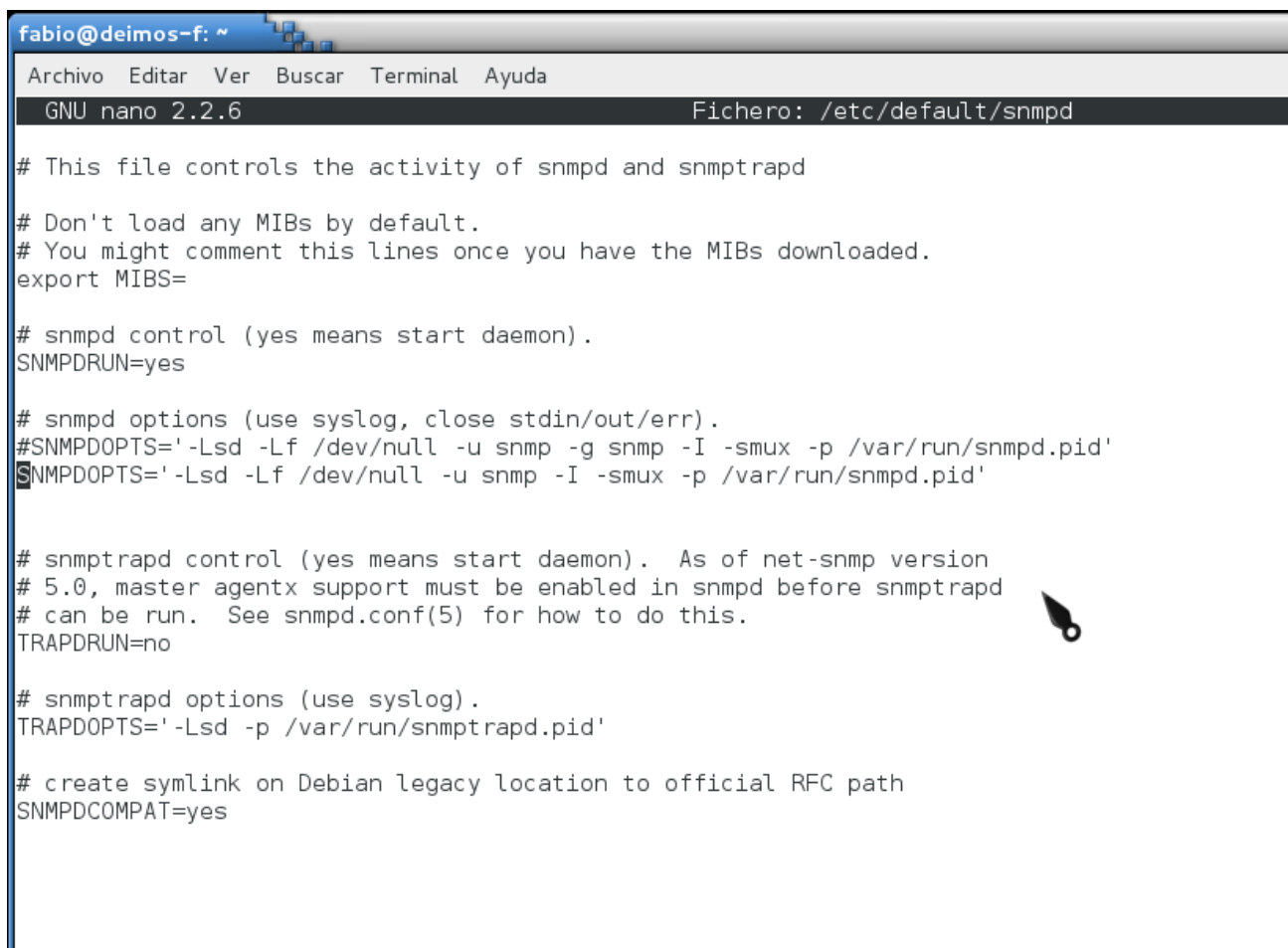
comentamos la siguiente linea

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
```

reemplazamos por

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid'
```

8



```
fabio@deimos-f: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 2.2.6                               Fichero: /etc/default/snmpd

# This file controls the activity of snmpd and snmptrapd

# Don't load any MIBs by default.
# You might comment this lines once you have the MIBs downloaded.
export MIBS=

# snmpd control (yes means start daemon).
SNMPDRUN=yes

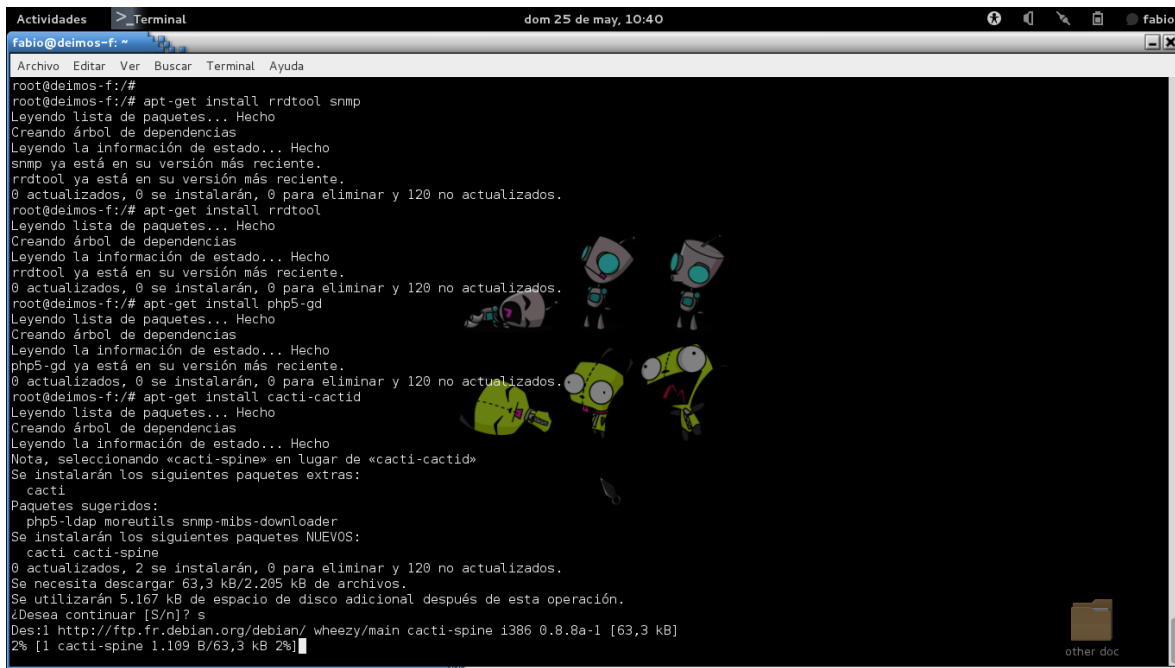
# snmpd options (use syslog, close stdin/out/err).
#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid'

# snmptrapd control (yes means start daemon). As of net-snmp version
# 5.0, master agentx support must be enabled in snmpd before snmptrapd
# can be run. See snmpd.conf(5) for how to do this.
TRAPDRUN=no

# snmptrapd options (use syslog).
TRAPDOPTS='-Lsd -p /var/run/snmptrapd.pid'

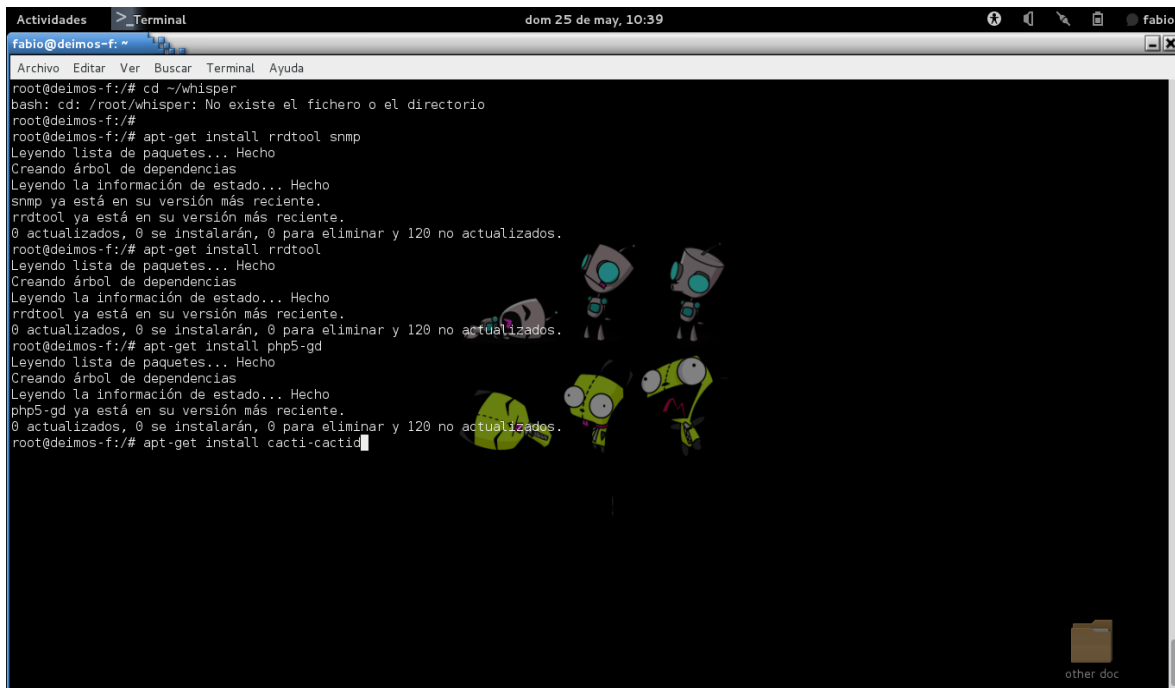
# create symlink on Debian legacy location to official RFC path
SNMPDCOMPAT=yes
```

9.



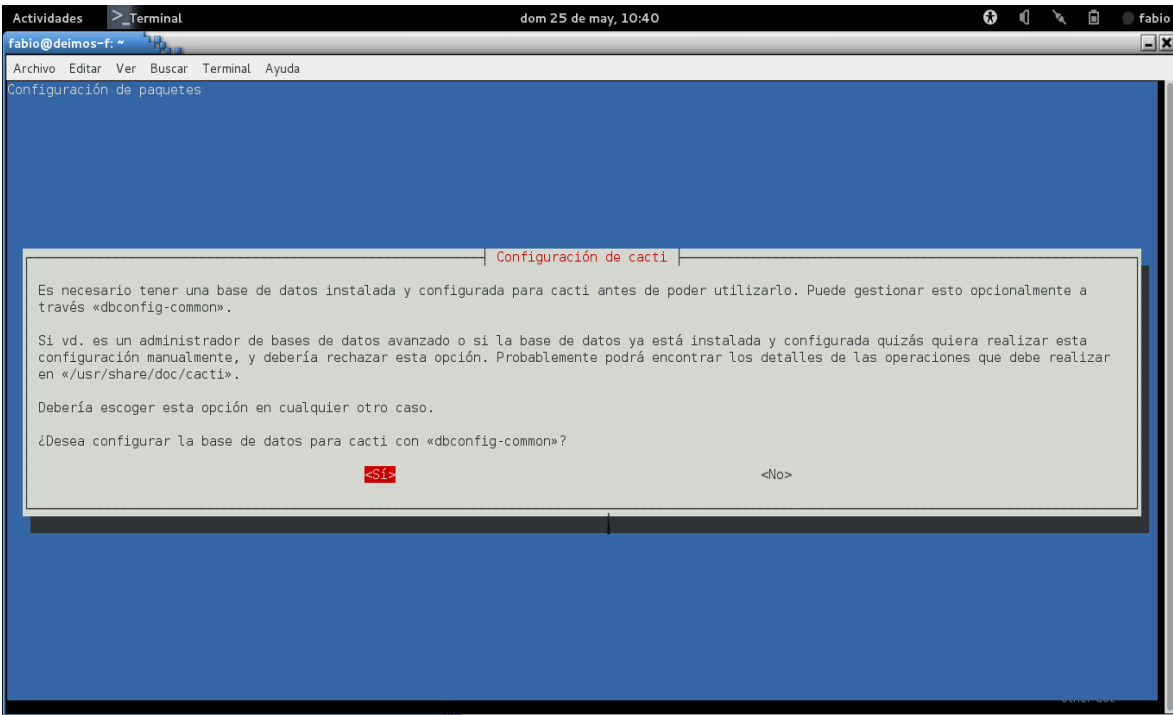
```
Actividades > Terminal dom 25 de may, 10:40
fabio@deimos-f: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@deimos-f:~#
root@deimos-f:~# apt-get install rrdtool snmp
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
snmp ya está en su versión más reciente.
rrdtool ya está en su versión más reciente.
0 actualizados, 0 se instalarán, 0 para eliminar y 120 no actualizados.
root@deimos-f:~# apt-get install rrdtool
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
rrdtool ya está en su versión más reciente.
0 actualizados, 0 se instalarán, 0 para eliminar y 120 no actualizados.
root@deimos-f:~# apt-get install php5-gd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
php5-gd ya está en su versión más reciente.
0 actualizados, 0 se instalarán, 0 para eliminar y 120 no actualizados.
root@deimos-f:~# apt-get install cacti-cactid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Nota: seleccionando «cacti-spine» en lugar de «cacti-cactid»
Se instalarán los siguientes paquetes extras:
  cacti
Paquetes sugeridos:
  php5-ldap moreutils snmp-mibs-downloader
Se instalarán los siguientes paquetes NUEVOS:
  cacti cacti-spine
0 actualizados, 2 se instalarán, 0 para eliminar y 120 no actualizados.
Se necesita descargar 63,3 kB/2,205 kB de archivos.
Se utilizarán 5.167 kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? s
Des:1 http://ftp.fr.debian.org/debian/ wheezy/main cacti-spine i386 0.8.8a-1 [63,3 kB]
2% [1 cacti-spine 1.109 B/63,3 kB 2%]
```

10

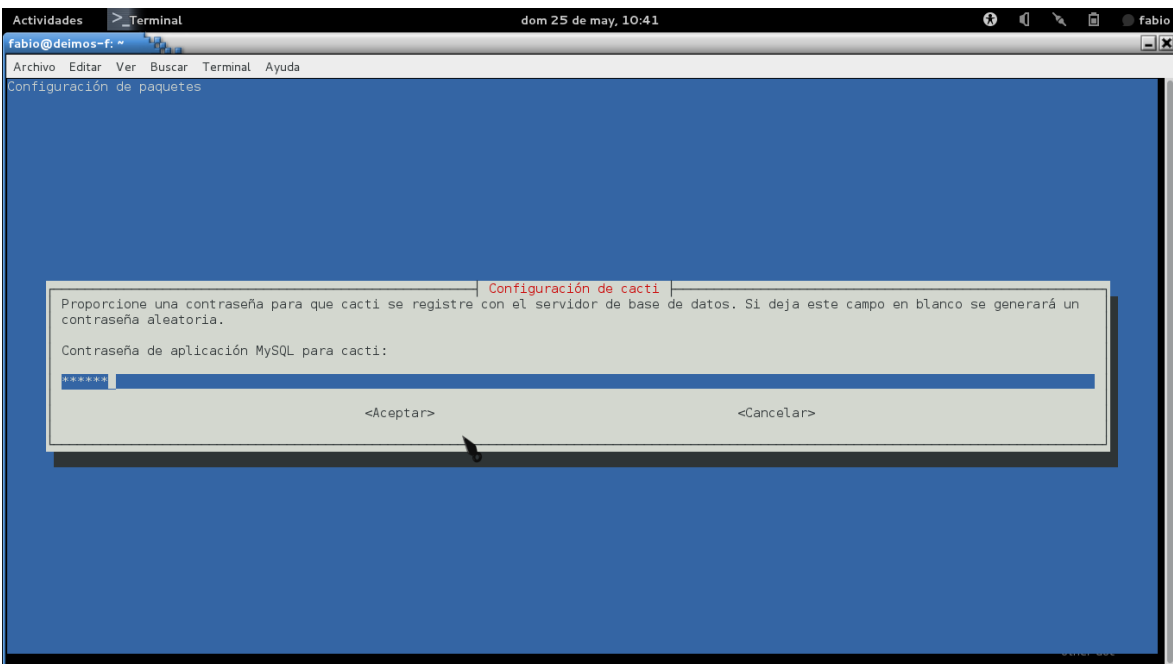


```
Actividades > Terminal dom 25 de may, 10:39
fabio@deimos-f: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@deimos-f:~# cd ~/whisper
bash: cd: /root/whisper: No existe el fichero o el directorio
root@deimos-f:~#
root@deimos-f:~# apt-get install rrdtool snmp
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
snmp ya está en su versión más reciente.
rrdtool ya está en su versión más reciente.
0 actualizados, 0 se instalarán, 0 para eliminar y 120 no actualizados.
root@deimos-f:~# apt-get install rrdtool
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
rrdtool ya está en su versión más reciente.
0 actualizados, 0 se instalarán, 0 para eliminar y 120 no actualizados.
root@deimos-f:~# apt-get install php5-gd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
php5-gd ya está en su versión más reciente.
0 actualizados, 0 se instalarán, 0 para eliminar y 120 no actualizados.
root@deimos-f:~# apt-get install cacti-cactid
```

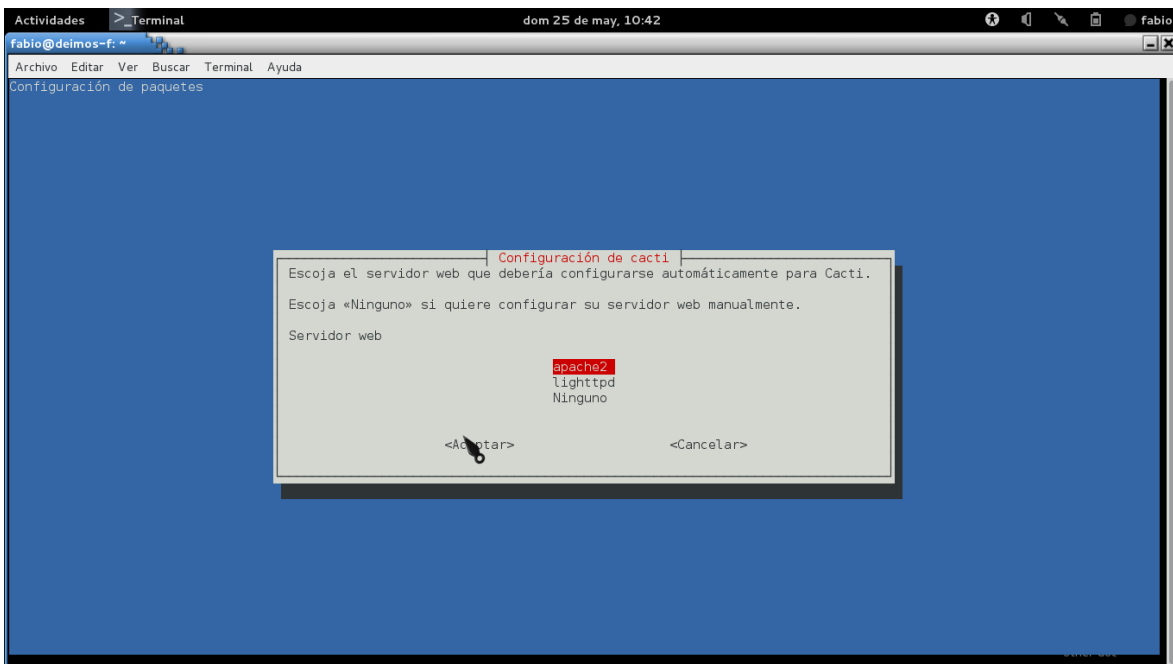
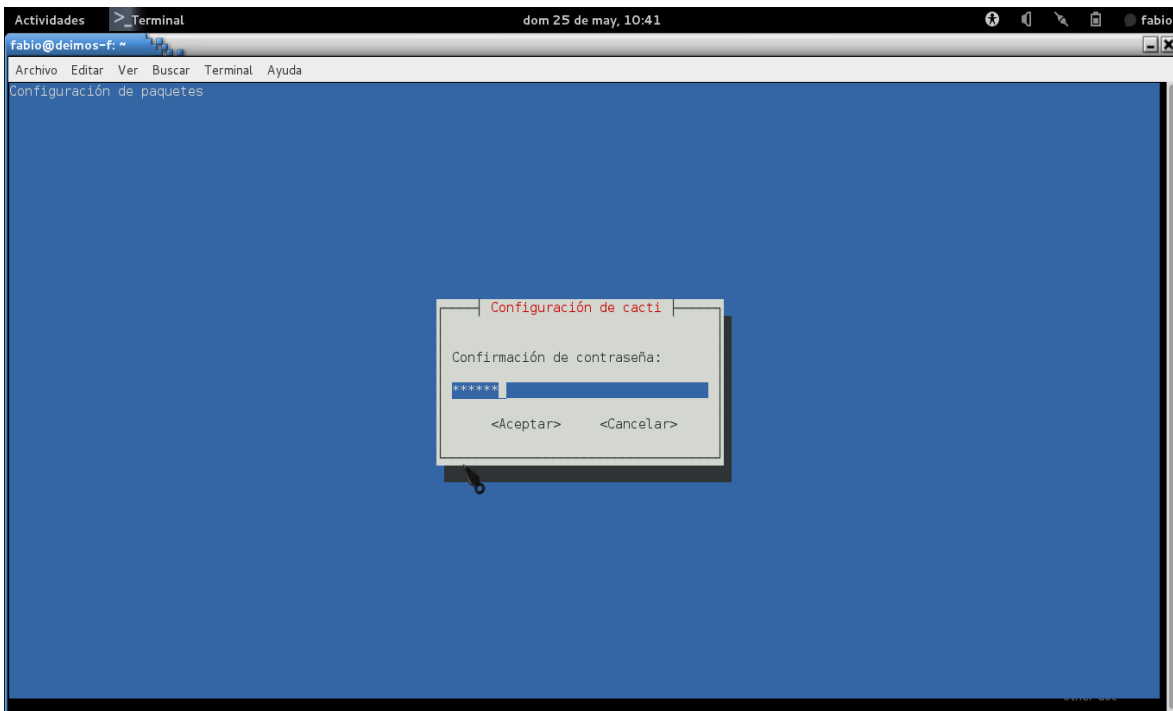
11.



12.



13.



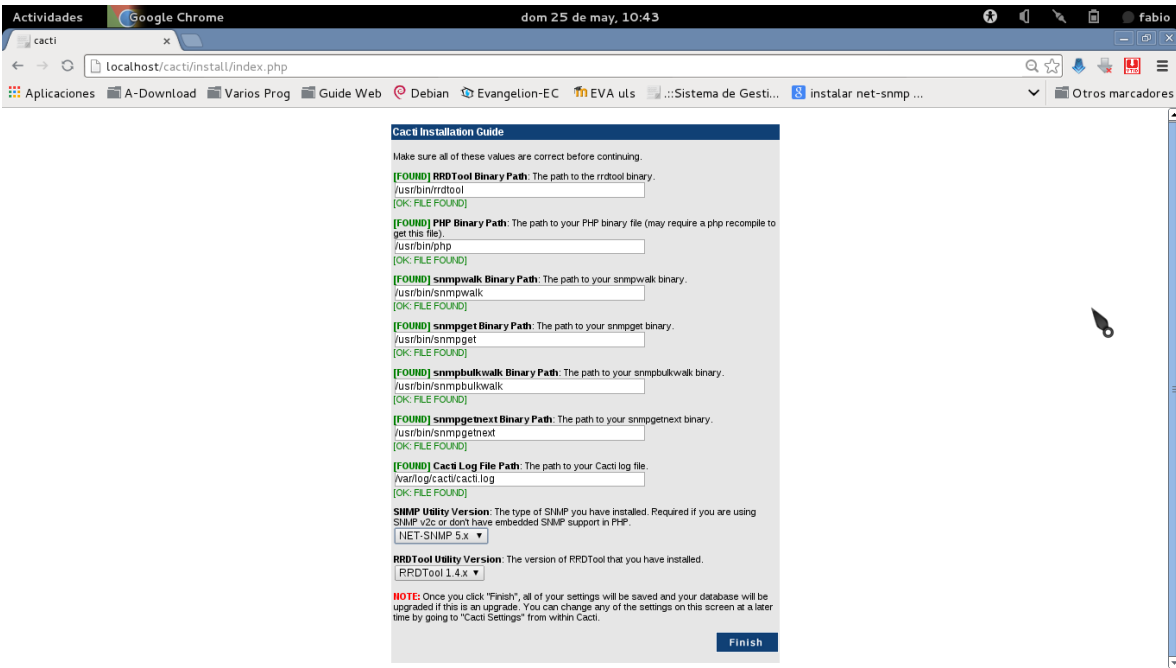
15.



16.



17.



18.



19.

console **graphs**

Console -> Devices -> (Edit)

Localhost (127.0.0.1)

SNMP Information
 System: Linux deimos-f 3.2.0-4-686-pae #1 SMP Debian 3.2.51-1 i686
 Uptime: 308124 (0 days, 0 hours, 51 minutes)
 Hostname: deimos-f
 Location: Dock Bay
 Contact: ma@example.org

Devices [edit: Localhost]

General Host Options

Description: Give this host a meaningful description.

Hostname: Fully qualified hostname or IP address for this device.

Host Template: Choose the Host Template to use to define the default Graph Templates and Data Queries associated with this Host.

Number of Collection Threads: The number of concurrent threads to use for polling this device. This applies to the Spine poller only.

Disable Host: Check this box to disable all checks for this host. Disable Host

Availability/Reachability Options

Downed Device Detection: The method Cacti will use to determine if a host is available for polling. NOTE: It is recommended that, at a minimum, SNMP always be selected.

Ping Timeout Value: The timeout value to use for host ICMP and UDP pinging. This host SNMP timeout value applies for SNMP pings.

Ping Retry Count: After an initial failure, the number of ping retries Cacti will attempt before failing.

SNMP Options

SNMP Version: Choose the SNMP version for this device.

SNMP Community: SNMP read community for this device.

SNMP Port: Enter the UDP port number to use for SNMP (default is 161).

SNMP Timeout: The maximum number of milliseconds Cacti will wait for an SNMP response (does not work with php-snmp support).

Maximum OID's Per Get Request: Specified the number of OID's that can be obtained in a single SNMP Get request.

Associated Graph Templates

Graph Template Name	Status
1) Linux - Memory Usage	Is Being Graphed (Edit)
2) Unix - Load Average	Not Being Graphed
3) Unix - Logged in Users	Is Being Graphed (Edit)
4) Unix - Processes	Is Being Graphed (Edit)

Add Graph Template:

Associated Data Queries

Data Query Name	Debugging	Re-index Method	Status
1) Unix - Get Mounted Partitions	(Verbose Query)	None	Success [6 Items, 3 Rows]

Add Data Query: Re-index Method:

20

Associated Graph Templates

Graph Template Name	Status
1) Linux - Memory Usage	Is Being Graphed (Edit)
2) Unix - Load Average	Not Being Graphed
3) Unix - Logged in Users	Is Being Graphed (Edit)
4) Unix - Processes	Is Being Graphed (Edit)

Add Graph Template:

Associated Data Queries

Data Query Name	Debugging	Re-index Method	Status
1) Unix - Get Mounted Partitions	(Verbose Query)	None	Success [6 Items, 3 Rows]

Add Data Query: Re-index Method:

21.

E1red2 (192.168.0.2)

SNMP Information
 System: Linux spike 3.2.0-4-686-pae #1 SMP Debian 3.2.57-3 i686
 Uptime: 390686 (0 days, 1 hours, 5 minutes)
 Hostname: spike
 Location: red_grupo2
 Contact: grupos@netfit.net

Ping Results
 UDP Ping Success (0.46 ms)

Devices [edit: E1red2]

General Host Options

Description: E1red2
 Hostname: 192.168.0.2
 Host Template: Karinet Wireless Bridge
 Number of Collection Threads: 1 Thread (default)
 Disable Host: Disable Host

Availability/Reachability Options

Downed Device Detection: Ping and SNMP Uptime
 Ping Method: UDP Ping
 Ping Port: 23
 Ping Timeout Value: 400
 Ping Retry Count: 1

SNMP Options

SNMP Version: Version 1
 SNMP Community: public

22

NOTE: ICMP on Linux/UNIX requires root privileges.

Ping Port: 23
 Ping Timeout Value: 400
 Ping Retry Count: 1

SNMP Options

SNMP Version: Version 1
 SNMP Community: public
 SNMP Port: 161
 SNMP Timeout: 500
 Maximum OID's Per Get Request: 10

Additional Options

Notes:

Associated Graph Templates

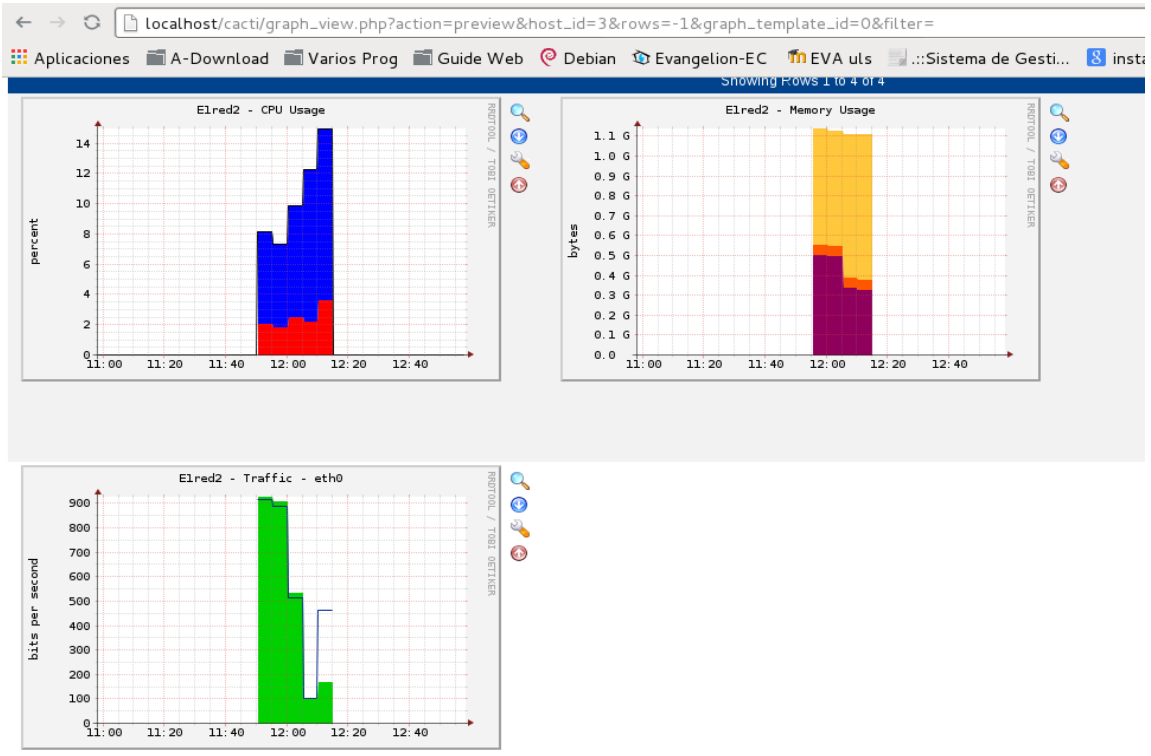
Add Graph Template: Cisco - CPU Usage

Associated Data Queries

Data Query Name	Debugging	Re-index Method	Status
1) Karinet - Wireless Bridge Statistics	(Verbose Query)	Uptime Goes Backwards	Success [0 Items, 0 Rows]
2) SNMP - Interface Statistics	(Verbose Query)	Uptime Goes Backwards	Success [29 Items, 3 Rows]

Add Data Query: Netware - Get Available Volumes

23.



24.

Graph Settings	
General	
Default RRA The default RRA to use when thumbnail graphs are not being displayed or when 'Thumbnail Timespan' is set to '0'.	Monthly (2 Hour Average) ▾
Default View Mode Which mode you want displayed when you visit 'graph_view.php'	Tree View ▾
Default Graph View Timespan The default timespan you wish to be displayed when you display graphs	Last 12 Hours ▾
Display Graph View Timespan Selector Choose if you want the time span selection box to be displayed.	<input checked="" type="checkbox"/> Display Graph View Timespan Selector
Default Graph View Timeshift The default timeshift you wish to be displayed when you display graphs	12 Hours ▾
Allow Graph to extend to Future When displaying Graphs, allow Graph Dates to extend 'to future'	<input checked="" type="checkbox"/> Allow Graph to extend to Future
First Day of the Week The first Day of the Week for weekly Graph Displays	Monday ▾
Start of Daily Shift Start Time of the Daily Shift.	07:00
End of Daily Shift End Time of the Daily Shift.	18:00
Graph Date Display Format The date format to use for graphs	Year, Month Number, Day ▾
Graph Date Separator The date separator to be used for graphs	/ ▾
Page Refresh The number of seconds between automatic page refreshes.	30
Graph Thumbnails	
Thumbnail Height The height of thumbnail graphs in pixels.	200
Thumbnail Width The width of thumbnail graphs in pixels.	310
Thumbnail Columns The number of columns to use when displaying thumbnail graphs.	3
Thumbnail Sections Which sections of Cacti thumbnail graphs should be used for.	<input checked="" type="checkbox"/> Preview Mode <input checked="" type="checkbox"/> Tree View (Single Pane) <input type="checkbox"/> Tree View (Dual Pane)

25

Tree View Mode	
Default Graph Tree The default graph tree to use when displaying graphs in tree mode.	Default Tree ▾
Default Tree View Mode The default mode that will be used when viewing tree mode.	Dual Pane ▾
Graphs Per-Page The number of graphs to display on one page in preview mode.	10 ▾
Dual Pane Tree Width When choosing dual pane Tree View, what width should the tree occupy in pixels.	200
Expand Hosts Choose whether to expand the graph templates used for a host on the dual pane tree.	<input type="checkbox"/> Expand Hosts
Show Graph Title Display the graph title on the page so that it may be searched using the browser.	<input type="checkbox"/> Show Graph Title
Preview Mode	
Graphs Per-Page The number of graphs to display on one page in preview mode.	10 ▾
List View Mode	
Graphs Per-Page The number of graphs to display on one page in list view mode.	20 ▾
Graph Fonts (RRDtool 1.2.x and Above)	
Use Custom Fonts Choose whether to use your own custom fonts and font sizes or utilize the system defaults.	<input type="checkbox"/> Use Custom Fonts

Conclusiones

SNMP es un protocolo sencillo pero potente que puede ayudar a monitorizar los recursos de red sin sobrecargar mucho la red. Quizás las extensiones que se están llevando a cabo actualmente incrementarán la complejidad y las posibilidades de esta herramienta pero a cambio incrementará los recursos necesarios para implementarla.

Con la interfaz gráfica Cacti para la creación y visualización de las gráficas del monitoreo de los equipos en red, esto resulta ser mucho más fácil de llevar un control de los equipos que están conectados en red.

El paquete de snmp y snmpd son dos cosas diferentes, una indica donde se guardan las MIBs y la otra indica las configuraciones para la comunicación entre las máquinas.

Snmp se puede integrar diferentes tipos de redes, toma en consideración el punto de la seguridad y no produce sobrecargos en la red.

FUENTES BIBLIOGRÁFICAS

BLOG DE ALFREDO CAMPOS - OCTUBRE - 2006

- <http://alfredocampos.blogspot.com/2006/10/qu-es-snmp.html>

ENCICLOPEDIA LIBRE - 2014

- http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol 24/02/14 10:07am

BLOG DE SAFEMODE - CL - JULIO - 2006

- <http://safemode-cl.blogspot.com/2006/07/para-que-sirve-el-protocolo-snmp.html>

MIBs 07-03-2014

- http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol

SNMP 07-03-2014

- <http://www.chw.net/foro/internet-y-redes/984077-introduccion-snmp-equipos-comunicacion.html>

- <http://www.publicaciones.urbe.edu/index.php/telematique/article/viewArticle/782/1886>