



Universidad de San Carlos de Guatemala  
Facultad de Ingeniería  
Escuela de Ciencias y Sistemas

Curso: Redes 2  
Plataforma: Linux



# Configuración Protocolo SNMP

## Descripción:

SNMP facilita el obtener información de intercambio de información entre nuestros dispositivos de red únicamente para conocer lo que pasa en nuestra red, el cual lo podemos utilizar cuando queremos verificar el estado de nuestra red, por cuestiones de seguridad para verificar que únicamente trabaje en nuestra red lo que necesitamos, con esto llevamos un control sobre la red que administramos.



## **Índice**

Introducción-----	2
Objetivos-----	3
Marcoteorico-----	4
Configuración-----	6
Conclusiones-----	8
Bibliografía-----	9
Recomendaciones-----	10



## **Introducción**

En una red uno de los aspectos mas importantes es la seguridad ya que debemos de asegurarnos que la mayoría de nuestros nodos esten utilizando la red adecuadamente, para ello podemos utilizar aplicaciones que monitoreen nuestra red y que nos den un diagnostico para poder tomar desiciones, respecto a que es en prioridad importante para un conjunto de computadores.

SNMP es un protocolo simple de administración de red el cual facilita el intercambio de informacion entre los dispositivos, ademas de supervisar el desempeño de nuestra red, y para ello planear o generar nuevas politicas para el crecimiento de nuestra red.

SNMP se compone de dispositivos administrados , agentes y los sistemas que administran la red, estos ultimos se encargan de controlar nuestros dispositivos administrados.

A continuacion veremos los archivos de configuración y los paquetes necesarios para que funcione este protocolo, tambien los comandos relacionados a su ejecucion.



## **Objetivos**

### **Generales**

- Configuración e instalación del protocolo SNMP para obtener información de nuestra red.

### **Especificos**

- configuración de nuestros archivos necesarios
- edición de las opciones de configuración
- generar reportes según nuestra configuración
- analizar la información según la configuración generada para este protocolo.



## Marco teórico

### 1. Historia

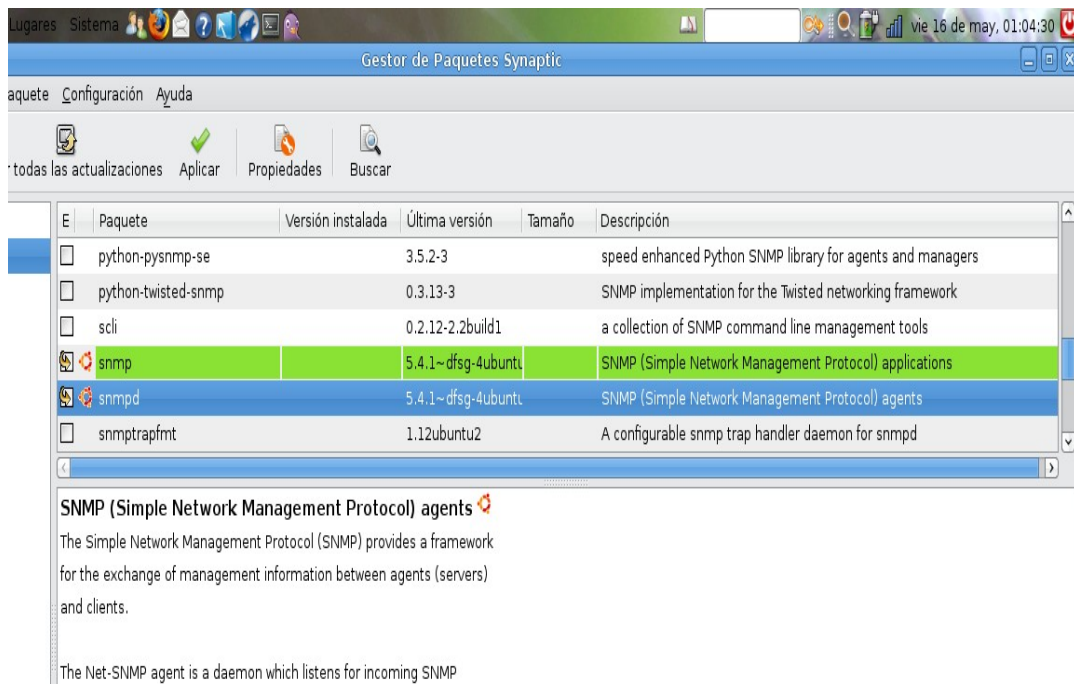
El protocolo SNMP se ha beneficiado de importantes mejoras desde su introducción en 1988.

2. Las computadoras utilizan el protocolo entre si, para transmitirse información administrativa de la red, este protocolo y sus agentes 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, computadores o impresoras. Y es aca donde se hace la recolección de datos. Esto puede ser importante a la hora de administrar la red, es por eso que resulta muy util, con tar con una herramienta, que sintenize y la información que se transmite entre los elementos de nuestra red.

### 3. Definición de dependencias:

- Maquina con intefaz de red
- Sistema operativo Ubuntu GNU/Linux para configuración
- Paquetes snmpd, snmp

La instalcion de los paquetes se realiza por medio de un gestor de paquetes como synaptic, haciendo la busqueda de los paquetes y porsteriormente instalandolos.



O bien

```
#apt-get install snmpd
```

**Localización de los archivos de configuración:**



el archivo snmpd.conf snmptrapd.conf son los archivos que contiene la configuración de nuestro agent y trap daemon los cuales se encuentran en el direccion /etc/snmp/

## Configuración o Utilización

### Configuración Archivosnmpd.conf

Para la configuración de de nuestro servicio debemos editar nuestro archivo de configuración, esto lo podemos hacer por medio de gedit.

Antes de realizar algun cambio hacemos una copia del archivo original por si en algun momento necesitamos restaurar el servicio.

```
#cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.backup
```

Habilitamos snmp server para permitir la lectura de acceso de las maquinas in nuestra red, a continuación editamos nuestro archivo

Configuración archivo default.

```
# sec.name source community
com2sec paranoid default public
#com2sec readonly default public
#com2sec readwrite default private
```

modificamos estas líneas a

```
#com2sec paranoid default public
com2sec local localhost public
com2sec localNet 192.168.0.0 /24 public
#com2sec readwrite default private
```

Nuestro archivo configurado snmpd.conf

```
# manual page.

####
# First, map the community name (COMMUNITY) into a security name
# (local and mynetwork, depending on where the request is coming
# from):

#       sec.name source          community
#com2sec paranoid default      public
#com2sec readonly default      public
com2sec local localhost public
com2sec localNet 192.168.0.0/24 public
#com2sec readwrite default     private

####
# Second, map the security names into group names:

#       sec.model sec.name
group MyROSystem v1 local
group MyROSystem v2c local
group MyROSystem usm local
group MyROGroup v1 localnet
group MyROGroup v2c localnet
group MyROGroup usm localnet
```

a continuación creamos el segundo mapa de seguridad del cual vamos a monitorizar para ello editamos el archivo snmpd.conf



####

# Second, map the security names into group names:

# sec.model sec.name

group MyROSystem v1 paranoid

group MyROSystem v2c paranoid

group MyROSystem usm paranoid

group MyROGroup v1 readonly

group MyROGroup v2c readonly

group MyROGroup usm readonly

group MyRWGroup v1 readwrite

group MyRWGroup v2c readwrite

group MyRWGroup usm readwrite

a estos datos unicamente le modificamos algunos permisos anuestros grupos.

### Nueva configuración

group MyROSystem v1 local

group MyROSystem v2c local

group MyROSystem usm local

group MyROGroup v1 localnet

group MyROGroup v2c localnet

group MyROGroup usm localnet

group MyRWGroup v1 local

group MyRWGroup v2c local

group MyRWGroup usm local

Por ultimo creamos permisos para acceder a los dos grupos con una sola vista con dos diferentes permisos de lectuar y escritura.

####

# Finally, grant the 2 groups access to the 1 view with different

# write permissions:

# context sec.model sec.level match read write notif

access MyROSystem "" any noauth exact system none none

access MyROGroup "" any noauth exact all none none

access MyRWGroup "" any noauth exact all all none

### Modificaciones opcionales

Podriamos configurar tambien el correo de comunicación si existiese alguna falla.

El siguiente configuracion la podemos modificar a partir de:

# System contact information

syslocation Unknown (configure /etc/snmp/snmpd.local.conf)

syscontact Root <root@localhost> (configure /etc/snmp/snmpd.local.conf)

y de esta pues la modificamos unicamente agregando un correo electronico para enviar los bugs de falla.

syslocation MainDatacenter

syscontact vicomix@gmail.com

ahora tenemos que habilitar el servicio para nuestra red.



**Universidad de San Carlos de Guatemala**  
**Facultad de Ingeniería**  
**Escuela de Ciencias y Sistemas**

Se hace a andar el servicio, corriendo el daemon snmpd

```
#/etc/init.d/snmpd restart
```

Ahora nuestro SNMP server esta configurado y corriendo

para comprobar nuestra configuración, escribimos en una consola

```
#snmpwalk localhost -c public -v1
```

el cual nos enviara el siguiente reporte

```
End of MIB
inicio@vicomix:~$ gedit /etc/snmp/snmpd.conf
inicio@vicomix:~$ snmpwalk localhost -c public -v1
SNMPv2-MIB::sysDescr.0 = STRING: Linux vicomix 2.6.24-17-generic #1 SMP Thu May 1 14:31:33 UTC 2008 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3102636) 8:37:06.36
SNMPv2-MIB::sysContact.0 = STRING: webmaster@debianhelp.co.uk
SNMPv2-MIB::sysName.0 = STRING: vicomix
SNMPv2-MIB::sysLocation.0 = STRING: MainDatacenter
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.8 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (0) 0:00:00.00
End of MIB
inicio@vicomix:~$
```



**Universidad de San Carlos de Guatemala**  
**Facultad de Ingeniería**  
**Escuela de Ciencias y Sistemas**

## **Conclusiones**

Este protocolo provee de informacion de nuestra red, tambien detecta algun error y sirve tambien para planear el crecimiento de nuestra red.

A este servicio tambien se le puede agregar interfaz grafica para ello podemos utilizar mrtg, este lo podemos instalarlo por medio del gestor de paquetes synaptic.



**Universidad de San Carlos de Guatemala**  
**Facultad de Ingeniería**  
**Escuela de Ciencias y Sistemas**

**Tutorial desarrollado por:**

200212355      Vinicio Rodolfo Miranda Orozco  
200217739      Miguel Enrique Gerra Conor  
200212383      Carlos Enrique Rodas Galvez

**Bibliografía**

[http://arpaneting.es/stuff/mrtg\\_howto.html](http://arpaneting.es/stuff/mrtg_howto.html)

[http://es.wikipedia.org/wiki/Simple\\_Network\\_Management\\_Protocol](http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol)

<http://www.debianhelp.co.uk/snmp.htm>



**Universidad de San Carlos de Guatemala**  
**Facultad de Ingeniería**  
**Escuela de Ciencias y Sistemas**

## **Recomendaciones**

Se recomienda instalar la interfaz grafica para mostrar la información a mas detalle y mas identificada

En la configuración del archivo de snmp, deben de conceder permisos y permitir a los grupos entrar según su importancia.