Ejercicios con SNMP, parte I

Nota: muchos de los comandos en este ejercicio no tienen que ejecutarse como root, pero no hay problema con ejecutarlos todos como root. Así que sería más sencillo si inicia una shell de root y los ejecuta todos desde ahí. Puede iniciar una shell de root así:

```
$ sudo -s
```

0. Instalación del los programas de gestion del cliente

```
# apt-get install snmp
# apt-get install snmp-mibs-downloader
```

El segundo paquete (snmp-mibs-downloader) baja los MIBs estandares de IANA y de IETF que no estan incluidos por defecto.

Para que esto funciona tiene que habilitar el fuente "multiverse" en su configuracion de APT - hemos hecho esto para Ud.

Ahora tiene que editar el archivo /etc/snmp/snmp.conf

```
# vi /etc/snmp/snmp.conf
```

y cambiar este linea:

```
mibs :
```

... para que se vea asi:

```
# mibs :
```

Ahora graba el archivo y salga de ello.

Esta accion deshabilito la linea de mibs vacia que estaba indicando a las herramientas de SNMP de *no* automaticamente cargar los mibs en el directorio /usr/share/mibs/.

1. Configuración de SNMP en el enrutador

Para esta parte del ejercicio, necesitan trabajar en grupos. Una persona estará asignada para escribir en el teclado.

Si no está seguro de a qué grupo pertenece, refiérase al diagrama de red en la wiki del taller, en http://noc.ws.nsrc.org/

Ahora conéctese a su enrutador:

```
$ ssh cisco@rtrN.ws.nsrc.org    (ó "ssh cisco@10.10.N.254")

username: cisco
password: <CLASS PASSWORD>

rtrN> enable
Password: <CLASS PASSWORD>
rtrN# configure terminal            (conf t)
```

Ahora es necesario agregar una lista de control de acceso (ACL) para acceso a SNMP. Luego iniciaremos el agente SNMP, asignaremos una "comunidad" de sólo lectura y le indicaremos al enrutador que nunca cambie los índices de interfaces al reiniciarse. Para ello, haremos lo siguiente:

```
rtrN(config)# access-list 99 permit 10.10.0.0 0.0.255.255
rtrN(config)# snmp-server community NetManage ro 99
rtrN(config)# snmp-server ifindex persist
```

Ahora salgamos del modo configuración y grabemos:

```
rtrN(config)# exit
rtrN# write memory              (wr mem)
rtrN# exit                  (volver al shell del PC)
```

Ahora, probaremos si estos cambios han hecho efecto.

2. Comprobación de SNMP

Para verificar que su instalación de SNMP funciona, ejecute el comando 'snmpstatus' en cada uno de los siguientes nodos:

```
$ snmpstatus -c 'NetManage' -v2c <IP_ADDRESS>
```

Donde <IP_ADDRESS> es cada uno de los siguientes:

* El servidor NOC: 10.10.0.254
* Su enrutador: 10.10.N.254
* El switch dorsal: 10.10.0.253
* Los puntos de acceso: 10.10.0.251, 10.10.0.252 (no siempre funcionan)

Qué pasa si intenta usando la comunidad incorrecta (ej. cambie "NetManage" por algo diferente)

3. SNMP Walk y los OIDs

Ahora, utilizará el comando 'snmpwalk', parte de la suite SNMP, para listar las tablas asociadas con los OIDs más abajo, para cada dispositivo que probó más arriba:

```
.1.3.6.1.2.1.2.2.1.2
.1.3.6.1.2.1.31.1.1.1.18
.1.3.6.1.4.1.9.9.13.1
.1.3.6.1.2.1.25.2.3.1
.1.3.6.1.2.1.25.4.2.1
```

```
$ snmpwalk -c 'NetManage' -v2c <IP_ADDRESS> <OID>
```

y

```
$ snmpwalk -On -c 'NetManage' -v2c <IP_ADDRESS> <OID>
```

… Donde <OID> es uno de los OIDS más arriba: .1.3.6…

… Donde <IP_ADDRESS> puede ser su enrutador...

Nota: la opcion "-On" habilita salida numerica, asi no traduccion del OID <-> MIB pasara.

Con estos OIDs:

a) Responden todos los dispositivos ?
b) Nota algo interesante en los OIDS de las respuestas ?

4. Configuración del agente SNMP en su PC

Para este ejercicio su grupo necesita verificar que el servicio SNMP está activo y respondiendo a solicitudes desde todas las máquinas de su grupo. Primero active el demonio snmpd en su máquina, luego pruebe si su máquina está respondiendo, y luego compruebe cada máquina de sus compañeros de grupo.

* Instalar el agente SNMP (demonio)

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

* Configuración:

Haremos una copia de respaldo del archivo que viene con el paquete, y luego crearemos uno propio:

```
# cd /etc/snmp
# mv snmpd.conf snmpd.conf.dist
# editor snmpd.conf
```

Luego, copiar/pegar lo siguiente (no incluya las líneas -- cortar aquí --)

```
-- cortar aquí -------------------------

#  Escuchar en todas las interfaces (en IPv4 *e* IPv6)
agentAddress udp:161,udp6:[::1]:161

# Configurar comunidad de "sólo lectura"
# y restringir quién se puede conectar
rocommunity NetManage  10.10.0.0/16
rocommunity NetManage  127.0.0.1

# Información sobre este servidor
sysLocation    NSRC Network Management Workshop
sysContact     sysadm@pcX.ws.nsrc.org

# Cuáles capas OSI están activas
# (applicación + extremo a extremo)
sysServices    72

# Incluye MIB de dskTable que es propietario (además de hrStorageTable)
includeAllDisks  10%
-- cortar aquí -------------------------
```

Ahora grabe y salga del editor.

* Reinicie snmpd

```
# service snmpd restart
```

5. Compruebe que está funcionando:

```
    $ snmpstatus -c 'NetManage' -v2c localhost
```

Qué puede observar ?

6. Pruebe con sus vecinos

Compruebe que ahora puede ejecutar snmpstatus con cada uno de los servidores de su grupo:

```
    $ snmpstatus -c 'NetManage' -v2c pcN.ws.nsrc.org
```

Por ejemplo, en el grupo 4:

```
    pc17.ws.nsrc.org
    pc18.ws.nsrc.org
    pc19.ws.nsrc.org
    pc20.ws.nsrc.org
```

7. Agregar MIBs

Recuerde que cuando ejecutó:

```
    $ snmpwalk -c 'NetManage' -v2c 10.10.X.254  .1.3.6.1.4.1.9.9.13.1
```

El cliente SNMP (snmpwalk) no pudo interpretar todos los OIDS que venían en la respuesta:

```
    SNMPv2-SMI::enterprises.9.9.13.1.3.1.2.1 = STRING: "chassis"
    SNMPv2-SMI::enterprises.9.9.13.1.3.1.6.1 = INTEGER: 1
```

Qué es '9.9.13.1.3.1' ?

Para poder interpretar esta información, necesitamos instalar MIBs adicionales:

* Utilizaremos las siguientes MIBs (no las descargue todavía!):

    MIBS de Cisco:

    ftp://ftp.cisco.com/pub/mibs/v2/CISCO-SMI.my
    ftp://ftp.cisco.com/pub/mibs/v2/CISCO-ENVMON-MIB.my

    Para hacerlo más fácil, tenemos una copia local en
    http://noc.ws.nsrc.org/mibs/ :

```
    # apt-get install wget
    # cd /usr/share/mibs
    # mkdir cisco
    # cd cisco

    # wget http://noc.ws.nsrc.org/mibs/CISCO-ENVMON-MIB.my
    # wget http://noc.ws.nsrc.org/mibs/CISCO-SMI.my
```

Ahora tenemos que decir a las herramientas de snmp que tenemos los MIBS que deberia cargar. Edite el archivo /etc/snmp/snmp.conf y agrega los dos siguiente lineas:

```
    mibdirs +/usr/share/mibs/cisco
    mibs +CISCO-ENVMON-MIB:CISCO-SMI
```

Grabe el archivo y salga.

Ahora, pruebe de nuevo:

```
    $ snmpwalk -c 'NetManage' -v2c 10.10.X.254  .1.3.6.1.4.1.9.9.13.1
```

Qué puede notar?

8. SNMPwalk - el resto de MIB-II

Intente ejecutar snmpwalk en cualquiera de los nodos (enrutadores, switches, PCs) que no haya probado todavía, en la red 10.10.0.X.

Note el tipo de información que obtiene.

```
    $ snmpwalk -c 'NetManage' -v2c 10.10.0.X ifDescr
    $ snmpwalk -c 'NetManage' -v2c 10.10.0.X ifAlias
    $ snmpwalk -c 'NetManage' -v2c 10.10.0.X ifTable | less
    $ snmpwalk -c 'NetManage' -v2c 10.10.0.X ifXTable | less
    $ snmpwalk -c 'NetManage' -v2c 10.10.0.X ifOperStatus
    $ snmpwalk -c 'NetManage' -v2c 10.10.0.X ifAdminStatus
    $ snmpwalk -c 'NetManage' -v2c 10.10.0.X if
```

(Recuerda que con "less" apreta la barra del espacio por la proxima pagina, 'b' para ir atras una pagina y 'q' para salir)

Puede ver la diferencia entre `ifTable` y `ifXTable`?

Que puede ser la diferencia entre 'ifOperStatus' y 'ifAdminStatus' ? Puede imaginar en qué escenario esto sería útil?

9. Más diversión con las MIBs

* Use SNMP para examinar lo siguiente:

    a) los procesos activos en un servidor vecino (hrSWRun)
    b) el espacio de disco disponible en un servidor vecino (hrStorage)
    c) las interfaces en un servidor vecino (ifIndex, ifDescr)

    Puede usar nombres cortos para "caminar" estas tablas?

* Experimente con el comando "snmptranslate", ejemplo:

```
        $ snmptranslate .1.3.6.1.4.1.9.9.13.1
```

   Pruebe con otros varios OIDs