SNMP exercises, part I

Note: many of the commands in this exercise do not have to be run as root, but it is safe to run them all as root. So it's simpler if you start a root shell and enter them all there. You can start a root shell like this:

```
$ sudo bash
```

1. Installing client tools

```
# apt-get install snmp
```

2. Testing SNMP

To control that your SNMP installation works, run the snmpstatus command on each of the following devices

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

Where IP_ADDRESS is the following list:

* The NOC server: 10.10.0.254
* The backbone switch: 10.10.0.253
* Classroom routers: 10.10.1-9.254
* The access points: 10.10.0.(251,252)

3. SNMP Walk and OIDs

Now, you are going to use the 'snmpwalk' command, part of the SNMP toolkit, to list the tables associated with the OIDs listed below, on each piece of equipment you tried above:

```
.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
.1.3.6.1.4.1.11.2.14.11.1.2
.1.3.6.1.2.1.25.2.3.1
.1.3.6.1.2.1.25.4.2.1
```

You will try this with two forms of the 'snmpwalk' command:

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

and

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

... where OID is one of the three OIDs listed above: .1.3.6...

Note: the "-On" option turns on numerical output, i.e.: no translation of the OID <-> MIB object takes place.

For these OIDs:

a) Do all the devices answer ?

b) Do you notice anything important about the OID on the output ?

4. Configuration of snmp on your Cisco router

Connect to your virtual Cisco router:

```
$ ssh 10.10.X.254        # where X is 1-9
```

Default login: "cisco", password "cisco", enable secret "cisco"

Configure it to enable SNMP:

```
enable
conf t
snmp-server community NetManage ro 99
access-list 99 permit 10.10.0.0 0.0.255.255
exit
```

```
    exit     # until you get back to your PC

Now back on your PC, test using some of the OIDs from section 3 above.

    $ snmpwalk -c 'NetManage' -v2c 10.10.X.254 <OID>

What happens if you try using the wrong community string (i.e. change
'NetManage' to something else?)

5. Configuration of snmpd on your PC
------------------------------------

* Install the SNMP agent (daemon)

    # apt-get install snmpd

* Edit the following file:

        # editor /etc/snmp/snmpd.conf

    Comment this line (ADD '#' in front):

        com2sec paranoid  default         public

    ... so that it becomes:

        #com2sec paranoid  default         public

    And UNcomment the line (REMOVE the '#' in front) and change community:

        #com2sec readonly  default         public

    ... so that it becomes:

        com2sec readonly  default         NetManage

    Now save and exit from the file.

* Edit the file /etc/default/snmpd, and find the line:

        SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid 127.0.0.1'

    Remove 127.0.0.1 at the end, so you have:

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

* Restart snmpd

        # service snmpd stop
        # service snmpd start

6. Check that snmpd is working:
-------------------------------

    $ snmpstatus -c NetManage -v2c localhost

What do you observe ?

7. Test your neighbors
----------------------

Check now that you can run snmpstatus against your neighbor's servers:

    $ snmpstatus -c NetManage -v2c pcX


8. Adding MIBs
--------------

Remember when you ran:

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

or

    $ snmpwalk -c NetManage -v2c 10.10.0.253  .1.3.6.1.4.1.11.2.14.11.1.2

If you noticed, the SNMP client (snmpwalk) couldn't interpret
```

all the OIDs coming back from the Agent:

```
    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
```

or

```
    ...
    RFC1155-SMI::enterprises.11.2.14.11.1.2.6.1.4.1 = INTEGER: 4
    RFC1155-SMI::enterprises.11.2.14.11.1.2.6.1.4.2 = INTEGER: 4
    RFC1155-SMI::enterprises.11.2.14.11.1.2.6.1.4.3 = INTEGER: 5
    RFC1155-SMI::enterprises.11.2.14.11.1.2.6.1.4.4 = INTEGER: 4
    ...
```

What is '9.9.13.1.3.1' ?
What is '.11.2.14.11.1.2.6.1.4' ?

To be able to interpret this information, we need to download extra MIBs:

* You will download the following files to your machine:

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

        HP MIBS:    http://ftp.hp.com/pub/networking/software/mibs-Oct09.tar
```

    However we have a local mirror on http://noc.ws.nsrc.org/mibs/
    which will be much faster (especially for the large HP mib bundle)

```
        # apt-get install wget
        # cd /usr/share/snmp/mibs
        # wget http://noc.ws.nsrc.org/mibs/CISCO-SMI.my
        # wget http://noc.ws.nsrc.org/mibs/CISCO-ENVMON-MIB.my
        # wget http://noc.ws.nsrc.org/mibs/mibs-Oct09.tar
```

* Extract the HP SNMP MIBs (in the /usr/share/snmp/mibs):

```
        # cd /usr/share/snmp/mibs       # just in case!
        # mkdir hp
        # cd hp
        # tar -xvf ../mibs-Oct09.tar
```

    Note: You should see a lot of output on the screen (the HP MIB files)

* Create the file /etc/snmp/snmp.conf, and put into it:

```
        mibdirs /usr/share/snmp/mibs:/usr/share/snmp/mibs/hp
        mibs ALL
```

    This tells the snmp* commands that they should load ALL mibs in the
    mibdirs /usr/share/snmp/mibs and /usr/share/snmp/mibs/hp

* Save the file, quit.

Now, try again:

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

and

```
    $ snmpwalk -c 'NetManage' -v2c 10.10.0.253  .1.3.6.1.4.1.11.2.14.11.1.2
```

What do you notice ?

9. SNMPwalk - the rest of MIB-II

Try and run snmpwalk on any hosts (routers, switches, machines) you
have not tried yet, in the 10.10.0.X network

Note the kind of information you can obtain.

```
    $ snmpwalk -c NetManage -v2c 10.10.0.X ifDescr
    $ snmpwalk -c NetManage -v2c 10.10.0.X ifTable
    $ snmpwalk -c NetManage -v2c 10.10.0.X ifAlias
    $ 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
```

Can you explain the difference between ifOperStatus and ifAdminStatus ?

Can you imagine a scenario where this could be useful ?

10. More MIB-OID fun

* Use the OIDs from the beginning of this exercise set, and examine:

        a) the running processes on your neighbor's server (hrSWRun)
        b) the amount of free diskspace on your neighbor's server (hrStorage)
        c) the interfaces on your neighbor's server (ifIndex, ifDescr)

    Can you use short names to walk these OID tables ?

* Experiment with the "snmptranslate" command, example:

```
        $ snmptranslate .1.3.6.1.4.1.11.2.14.11.1.2
```

* Try with various OIDs