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
```

0. Installing client tools

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

1. Configure SNMP on Your Router

For this exercise you need to work in groups. Assign one person to type on the keyboard. There should be 4 people in group. For instance, members of Group 1 are those on pc1-pc4, Group 2 use pc5-pc8, Group 3 use pc9-12, etc…

If you are unsure of what group you are in refer to the Network Diagram on the classroom wiki by going to http://noc.ws.nsrc.org/ and clicking on the Network Diagram link.

Now connect to your router:

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

username: cisco
password: <CLASS PASSWORD>

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

Now we need to add an Access Control List rule for SNMP access, turn on SNMP, assign a read-only SNMP community string and tell the router to maintain SNMP information across reboots. To do this we do:

```
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
```

Now let's exit and save this new configuration to the routers permanent config.

```
rtrN(config)# exit
rtrN# write memory              (wr mem)
rtrN# exit                  (until you return to your pc)
```

Now to see if your changes are working.

2. Testing SNMP

To verify 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 each of the following:

* The NOC server: 10.10.0.254
* Your group's router: 10.10.N.254

    * The backbone switch: 10.10.0.253
    * The access points: 10.10.0.25

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

3. Configuration of snmpd on your PC

For this exercise your group needs to verify that the snmpd service is running and
responding to queries for all machines in your group. First enable snmpd on your machine,
then test if your machine is responding, then check each machine of your other group
members.

* 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

5. Check that snmpd is working:

    $ snmpstatus -c 'NetManage' -v2c localhost

What do you observe ?

6. Test your neighbors

Check now that you can run snmpstatus against your other group members servers:

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

For instance, in group 4, you should verify against:

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


OPTIONAL
--------

7. Adding MIBs
--------------

Remember when you ran:

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

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

What is '9.9.13.1.3.1' ?

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

    However we have a local mirror on http://noc.ws.nsrc.org/mibs/
    which will be much faster

        # 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

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

        mibs ALL

    This tells the snmp* commands that they should load ALL mibs installed
    in the mib directories, rather than a default subset.

* 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

What do you notice ?


8. 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
```

What do you think might be the difference between ifOperStatus and ifAdminStatus?

Can you imagine a scenario where this could be useful ?

9. 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 .1.3.6.1.4.1.9.9.13.1
```

* Try with various OIDs