

SNMP exercises, part 1
Apricot 2009, Manila

1. Getting packages (should already be installed)

```
> apt-get install snmp
> apt-get install snmpd
> apt-get install mbrowse
```

2. GET and WALK

To control that your SNMP installation works:

- The backbone router and net routers

```
> snmpstatus -c aprlcot29 -v2c 169.223.140.201
> snmpstatus -c aprlcot29 -v2c 169.223.140.202
> snmpstatus -c aprlcot29 -v2c 169.223.140.254
```

- The NOC server

```
> snmpstatus -c aprlcot29 -v2c 169.223.140.130
```

- The network switches:

```
> snmpstatus -c aprlcot29 -v2c 169.223.140.200
> snmpstatus -c aprlcot29 -v2c 169.223.140.210    (might not be available)
> snmpstatus -c aprlcot29 -v2c 169.223.140.220    (might not be available)
```

- Try to snmpwalk different parts of these equipments' MIBs:

```
> snmpwalk -c aprlcot29 -v2c 169.223.140.Y 1.3.6.1.4.1.9.9.13.1.3 | more
> ...
```

a) Do all the devices answer ?

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

3. Configuration of snmpd

- Edit the following file:

```
> vi /etc/snmp/snmpd.conf
```

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

```
com2sec paranoid default public
```

... so that it becomes:

```
#com2sec paranoid default public
```

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

```
#com2sec readonly default public
```

... so that it becomes:

```
com2sec readonly default aprlcot29
```

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`

```
> /etc/init.d/snmpd stop
> /etc/init.d/snmpd start
```

4. Check that `snmpd` is working:

```
> snmpstatus -c aprlcot29 -v2c localhost
```

- What do you observe ?

5. Check now that you can run `snmpstatus` against your neighbor's server:

- Find out what your neighbor's IP is, ask them to run:

```
> ifconfig eth0
```

(your IP is 169.223.140.X where X is the IP of the PC of your neighbor)

- Check `snmp` against their machine:

```
> snmpstatus -c public -v2c 169.223.140.X
```

6. `SNMPwalk` - the rest of MIB-II

- Try and run `snmpwalk` on the routers, switches, and other hosts in the network:

```
> snmpwalk -c aprlcot29 -v2c 169.223.140.X
```

Note the kind of information you can obtain.

```
> snmpwalk -c aprlcot29 -v2c 169.223.140.X ifDescr
> snmpwalk -c aprlcot29 -v2c 169.223.140.X ifTable
> snmpwalk -c aprlcot29 -v2c 169.223.140.X ifDescr
> snmpwalk -c aprlcot29 -v2c 169.223.140.X ifOperStatus
> snmpwalk -c aprlcot29 -v2c 169.223.140.X ifAdminStatus
> snmpwalk -c aprlcot29 -v2c 169.223.140.X if
```

7. Adding MIBs

Remember when you ran:

```
> snmpwalk -c aprlcot29 -v2c 169.223.140.201 1.3.6.1.4.1.9.9.13.1.3 | more
```

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

```
SNMPv2-SMI::enterprises.9.9.13.1.3.1.2.1 = STRING: "chassis"
SNMPv2-SMI::enterprises.9.9.13.1.3.1.3.1 = Gauge32: 23
```

```
SNMPv2-SMI::enterprises.9.9.13.1.3.1.4.1 = INTEGER: 65
SNMPv2-SMI::enterprises.9.9.13.1.3.1.5.1 = INTEGER: 0
SNMPv2-SMI::enterprises.9.9.13.1.3.1.6.1 = INTEGER: 1
```

What is '9.9.13.1.3.1.3' ?

To be able to interpret this information, we need to download extra mibs...

- Download the following files to your machine:

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

Note: passive FTP seems to fail with Cisco.com, so fetch them from here:

```
> cd /usr/share/snmp/mibs
> wget http://169.223.140.130/mibs/CISCO-SMI.my
> wget http://169.223.140.130/mibs/CISCO-ENVMON-MIB.my
```

- Create the file /usr/share/snmp/snmp.conf, and put into it:

```
mibdirs /usr/share/snmp/mibs

mibs ALL
```

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

Save the file, quit.

Now, try again:

```
> snmpwalk -c apricot29 -v2c 169.223.140.254 1.3.6.1.4.1.9.9.13.1.3 | more
```

What do you notice ?