SNMP exercises, part 1
APRICOT 2010, Kuala Lumpur

1. Getting packages:

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

2. GET and WALK

To control that your SNMP installation works:

- The backbone router and net routers

```
> snmpstatus -c s3cr3t -v2c 169.223.142.1
> snmpstatus -c s3cr3t -v2c 169.223.142.10
> snmpstatus -c s3cr3t -v2c 169.223.142.20
> snmpstatus -c s3cr3t -v2c 169.223.142.30
```

- The NOC server

```
> snmpstatus -c s3cr3t -v2c 169.223.142.3
```

- The network switches:

```
> snmpstatus -c s3cr3t -v2c 169.223.142.2
> snmpstatus -c s3cr3t -v2c 169.223.142.34
> snmpstatus -c s3cr3t -v2c 169.223.142.65
> snmpstatus -c s3cr3t -v2c 169.223.142.97
```

- Try to snmpwalk of this particular OID on these equipments' MIBs:

```
> snmpwalk -c s3cr3t -v2c  169.223.142.3  1.3.6.1.4.1.9.9.13.1.3 | more

> snmpwalk -c s3cr3t -v2c 169.223.142.1   1.3.6.1.4.1.9.9.13.1.3 | more
> snmpwalk -c s3cr3t -v2c 169.223.142.10  1.3.6.1.4.1.9.9.13.1.3 | more
> snmpwalk -c s3cr3t -v2c 169.223.142.20  1.3.6.1.4.1.9.9.13.1.3 | more
> snmpwalk -c s3cr3t -v2c 169.223.142.30  1.3.6.1.4.1.9.9.13.1.3 | more

> snmpwalk -c s3cr3t -v2c 169.223.142.2   1.3.6.1.4.1.9.9.13.1.3 | more
> snmpwalk -c s3cr3t -v2c 169.223.142.34  1.3.6.1.4.1.9.9.13.1.3 | more
> snmpwalk -c s3cr3t -v2c 169.223.142.65  1.3.6.1.4.1.9.9.13.1.3 | more
> snmpwalk -c s3cr3t -v2c 169.223.142.97  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) and change community:

```
#com2sec readonly  default         public
```

... so that it becomes:

```
com2sec readonly  default         s3cr3t
```

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 s3cr3t -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
```

(the IP is 169.223.142.X where X is the IP of one of your neighbors, for example: .38, .69, .100 , ...)

- Check snmp against their machine:

```
> snmpstatus -c public -v2c 169.223.142.X
```

6. SNMPwalk - the rest of MIB-II

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

```
> snmpwalk -c s3cr3t -v2c 169.223.142.X  (.1, .3, .10, .34, .68, etc...)
```

Note the kind of information you can obtain.

```
> snmpwalk -c s3cr3t -v2c 169.223.142.X ifDescr
> snmpwalk -c s3cr3t -v2c 169.223.142.X ifTable
> snmpwalk -c s3cr3t -v2c 169.223.142.X ifAlias
> snmpwalk -c s3cr3t -v2c 169.223.142.X ifOperStatus
> snmpwalk -c s3cr3t -v2c 169.223.142.X ifAdminStatus
> snmpwalk -c s3cr3t -v2c 169.223.142.X if
```

7. Adding MIBs

Remember when you ran:

```
> snmpwalk -c s3cr3t -v2c 169.223.142.1  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.9.9.13.1.3.1.6.1 = INTEGER: 5

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

  > cd /usr/share/snmp/mibs
  > wget ftp://ftp.cisco.com/pub/mibs/v2/CISCO-SMI.my
  > wget ftp://ftp.cisco.com/pub/mibs/v2/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 s3cr3t -v2c 169.223.142.1  1.3.6.1.4.1.9.9.13.1.3 | more
> snmpwalk -c s3cr3t -v2c 169.223.142.34  1.3.6.1.4.1.9.9.13.1.3 | more

What do you notice ?
```