SNMP Hands - On

Goals

- Configure SNMP Agent on managed devices like Routers, Switches and Linux servers
- Configure SNMP Client Tools (Manager) in Linux servers.
- Install and learn to use the SNMP commands
- Install vendor specific MIBs and use those with the SNMP commands

Notes

- For below hands-on we will be using Ubuntu 20.04 version.
- You may use Putty or any kind supported terminal programs to connect remote devices.

Installing SNMP Client (Manager) tools

Connect to the server which will be used as the NMS (Network Management Station) and Open the Terminal program.

Update your software package repository

```
$ sudo apt-get update
```

This might take a few moments if everyone in class is doing this at the same moment.

Install the net-snmp tools:

```
$ sudo apt-get install snmp

$ sudo apt-get install snmp-mibs-downloader
```

The second of the two commands downloads the standard IETF and IANA SNMP MIBs which are not included by default.

Now, edit the file /etc/snmp/snmp.conf:

```
$ sudo vi /etc/snmp/snmp.conf
```

Note: Here we are using **vi** editor. You can use any text editor you are familiar with

Change this line:

```
mibs :
```

so that it looks like:

```
# mibs :
```

(You are "commenting out" the empty mibs statement, which was telling the snmp* tools not to automatically load the mibs in the /usr/share/mibs/ directory)

User specific SNMP configurations

Now, in your home directory make a .snmp directory with file snmp.conf inside it, make it readable only be you, and add the credentials to it:

```
$ cd

$ mkdir .snmp

$ chmod 700 .snmp/

$ vi .snmp/snmp.conf
```

Put the following contents in the file:

```
defVersion 3

defSecurityLevel authPriv

defSecurityName admin

defAuthPassphrase NetAdmin@1

defAuthType SHA

defPrivPassphrase NetPrivacy@1

defPrivType DES


# Default community when using SNMP v2c

defCommunity NetCommunity

defaultPort 161
```

Configuration of SNMP Agent on Routers and Switches

Cisco Router/Switch

connect to your router and go to configure mode.

```
Router> enable



Router# configure terminal
```

Now we need to add an Access Control List(ACL) for controlling SNMP access to the router. This ACL will be used in both SNMPv2c and SNMPv3 configurations.

```
Router(config)# access-list 99 permit 192.248.4.0 0.0.0.255
```

SNMPv1 and SNMPv2c Configuration

Below shows how to configure SNMPv1/v2c for the Cisco router.

```
Router(config)# snmp-server community NetCommunity ro 99
```

SNMPv3 Configuration

Below shows how to configure SNMPv3 for the Cisco router.

```
Router(config)# snmp-server group GroupR v3 priv access 99

Router(config)# snmp-server user admin GroupR v3 auth sha NetAdmin@1
priv des NetPrivacy@1
```

After all make sure to save the configuration to the router.

```
Router(config)# exit

Router# write memory

Router# exit
```

HP Router

Connect to the Router and go to config mode

```
<Router> system-view
```

Add the following to create an ACL. This also can be used in both SNMPv2c and SNMPv3 configurations.

```
[Router]acl basic 2000

[Router-acl-ipv4-basic-2000]rule 0 permit source 192.248.4.0 0.0.0.255

[Router-acl-ipv4-basic-2000]rule 5 deny
```

SNMPv1 and SNMPv2c Configuration

Below shows how to configure SNMPv1/v2c for the HP router.

```
[Router]snmp-agent

[Router]snmp-agent community read NetCommunity acl 2000
```

SNMPv3 Configuration

Below shows how to configure SNMPv3 for the HP router.

```
[Router]snmp-agent sys-info version all

[Router]snmp-agent group v3 GroupR privacy acl 2000

[Router]snmp-agent usm-user v3 admin GroupR simple authentication-mode
sha NetAdmin@1 privacy-mode des56 NetPrivacy@1
```

HP Aruba/Procurve

```
Switch-HP#conf

Switch-HP(config)# snmpv3 enable

SNMPv3 Initialization process.

Creating user 'initial'

Authentication Protocol: MD5
```

```
Enter authentication password: ********

Privacy protocol is DES

Enter privacy password: ********

User 'initial' has been created

Would you like to create a user that uses SHA? [y/n] y

Enter user name: admin

Authentication Protocol: SHA

Enter authentication password: ********

Privacy protocol is DES

Enter privacy password: ********

User creation is done. SNMPv3 is now functional.

Would you like to restrict SNMPv1 and SNMPv2c messages to have read
only

access (you can set this later by the command 'snmp restrict-access')?
[y/n] n
```

Now you can add the user to the group GroupR,

```
Switch-HP(config)# snmpv3 group GroupR user admin sec-model ver3
```

Later you can remove initial user,

```
Switch-HP(config)#no snmpv3 user initial
```

Aruba Virtual Controller

Go to `Configuration` --> `System` --> `Monitoring` and under SNMP, you may add SNMPv2 or SNMPv3 string details. If SNMPv3, use Authentication MD5 and AES Privacy.

Testing SNMP

Now we have both a SNMP Manager and SNMP Agent. To check that your SNMP installation works, run the snmpstatus command on the SNMP Manager host.

```
$ snmpstatus <IP_ADDRESS>
```

Note that you just used was the SNMPv3 because we set the default version as SNMPv3. Try again, adding "-v2c" as a parameter. Notice that the command automatically uses the community string in the snmp.conf file instead of the v3 user credentials. Try "-v1".

To use the SNMP v2 or v1 we can add an option as below. Which will override the settings in the configuration file(/.snmp/snmp.conf).

```
$ snmpstatus -v2c <IP_ADDRESS>

$ snmpstatus -v1 <IP_ADDRESS>
```

Again we didn't want set Community string as it was set in the manager configuration file.

For the Router,

```
#snmpstatus <Router IP>
```

For the Switch,

```
#snmpstatus <Switch IP>
```

More useful OIDs for Cisco devices

System Name:

```
snmpget -v 2c 192.248.4.22 sysName.0 (SNMPv2-MIB)
```

System Up time,

```
snmpget -v 2c 192.248.4.22 sysServices.0 (SNMPv2-MIB)
```

Interface Status:

```
snmpwalk -v 2c 192.248.4.22 ifOperStatus

snmpwalk -v 2c 192.248.4.22 IF-MIB::ifOperStatus
```

Average CPU load in 5 minutes:

```
snmpget -v 2c 192.248.4.22  .1.3.6.1.4.1.9.2.1.58.0 (OLD-CISCO-CPU-MIB::avgBusy5)
```

Free memory:

```
snmpget -v 2c 192.248.4.22 1.3.6.1.4.1.9.2.1.8.0 (OLD-CISCO-MEMORY-MIB::freeMem)
```

Configuration of SNMP Agent on a Linux server

We also need to monitor the servers and workstations. Here we do this by installing and configuring a SNMP agent on a server.

Install the SNMP agent (daemon) on your host

```
$ sudo apt install snmpd

$ sudo apt install libsnmp-dev
```

Before making any changes to configurations files of a new installation it is a good practice to backup the original configuration.

```
$ cd /etc/snmp

$ sudo mv snmpd.conf snmpd.conf.orig

$ sudo nano snmpd.conf
```

Now enter the below configurations,

```
#  Listen for connections on all interfaces (both IPv4 *and* IPv6)

agentAddress udp:127.0.0.1:161,udp:192.248.4.23:161



# For SNMPv2: Configure Read-Only community and restrict who can connect

rocommunity NetCommunity  192.248.4.0/24

rocommunity NetCommunity  127.0.0.1
```

```
# Information about this host

sysLocation    LEARN Workshop

sysContact     sysadm@ws.ac.lk


# Which OSI layers are active in this host

# (Application + End-to-End layers)

sysServices    72


# Include proprietary dskTable MIB (in addition to hrStorageTable)

includeAllDisks  10%
```

Now save and exit from the editor.

Now Go to the SNMP Manager and enter below,

```
snmpwalk -v 2c 192.248.4.23 upTime
```

The request should be successful. Now enter the below,

```
snmpwalk -v 3 192.248.4.23 upTime
```

It should give an error. This is because we haven't created a SNMP v3 user at the Agent. Now we will add the same SNMPv3 user to your PC. We need to stop snmpd before adding the user, and restart it to read the above changes as well as the new user:

```
$ sudo systemctl stop snmpd.service

$ sudo net-snmp-config --create-snmpv3-user -a NetAdmin@1 -A SHA -x
NetPrivacy@1 -X DES admin

$ sudo systemctl start snmpd.service
```

Now check whether SNMP v3 is working:

```
$ snmpwalk -v 3 192.248.4.23 upTime

$ snmpwalk 192.248.4.23 sysServices
```