SNMP Troubleshooting

Sometimes with NMIS and Network Management in general, you get these funny products, like wierd devices which don't really conform to the best practices and standards for SNMP. They can be a pain to troubleshoot. Here are some tips for things we have found.

SNMP Working, but not finding Interfaces with ifIndex

When running an NMIS update, e.g. nmis.pl type=update node=NODENAME debug=true, you might stop at this line "SNMP ERROR" see below:

```
01:35:35 getIntfInfo, Get Interface Info of node STRANGENODENAME, model TELDAT
01:36:23 checkResult, SNMP ERROR (STRANGENODENAME) (ifIndex) No response from remote host "STRANGENODENAME"
01:36:23 getIntfInfo, ERROR (STRANGENODENAME) on get interface index table
01:36:23 notify, Start of Notify
01:36:23 eventAdd, event added, node=STRANGENODENAME, event=SNMP Down, level=Critical, element=, details=SNMP
error
```

This looks odd because SNMP is working, but this very important operation is failing. So the problem is likely to be with support for the maximum SNMP packet size which is controlled by something called max repetition, which is actually how many SNMP PDU's will be packed into the SNMP packet.

So to troubleshoot the above you might run an SNMPWALK like this:

```
NMIS# snmpwalk -v 2c -c COMMUNITYSTRING STRANGENODENAME ifIndex
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
IF-MIB::ifIndex.6 = INTEGER: 6
IF-MIB::ifIndex.7 = INTEGER: 7
IF-MIB::ifIndex.8 = INTEGER: 8
IF-MIB::ifIndex.9 = INTEGER: 9
IF-MIB::ifIndex.10 = INTEGER: 10
IF-MIB::ifIndex.11 = INTEGER: 11
IF-MIB::ifIndex.12 = INTEGER: 12
```

If you ran a TCP DUMP which you would run with this command, you will need to make sure you are using TCPDUMP on the interface you are sending packets out of, check the route table on the server if you have multiple interfaces:

```
tcpdump -i INTERFACE host 2.3.4.5
```

You would see this:

```
01:31:37.093751 IP 1.2.3.4.48560 > 2.3.4.5.snmp:  C=COMMUNITYSTRING GetBulk(29)  N=0 M=10 interfaces.ifTable.
ifEntry.ifIndex
01:31:37.115557 IP 2.3.4.5.snmp > 1.2.3.4.48560:  C=COMMUNITYSTRING GetResponse(185)  interfaces.ifTable.
ifEntry.ifIndex.1=1 interfaces.ifTable.ifEntry.ifIndex.2=2 interfaces.ifTable.ifEntry.ifIndex.3=3 interfaces.
ifTable.ifEntry.ifIndex.4=4 interfaces.ifTable.ifEntry.ifIndex.5=5 interfaces.ifTable.ifEntry.ifIndex.6=6
interfaces.ifTable.ifEntry.ifIndex.7=7 interfaces.ifTable.ifEntry.ifIndex.8=8 interfaces.ifTable.ifEntry.
ifIndex.9=9 interfaces.ifTable.ifEntry.ifIndex.10=10
01:31:37.116194 IP 1.2.3.4.48560 > 2.3.4.5.snmp:  C=COMMUNITYSTRING GetBulk(30)  N=0 M=10 interfaces.ifTable.
ifEntry.ifIndex.10
01:31:37.139792 IP 2.3.4.5.snmp > 1.2.3.4.48560:  C=COMMUNITYSTRING GetResponse(241)  interfaces.ifTable.
ifEntry.ifIndex.11=11 interfaces.ifTable.ifEntry.ifIndex.12=12 interfaces.ifTable.ifEntry.ifDescr.1="ethernet0
/0" interfaces.ifTable.ifEntry.ifDescr.2="ethernet0/1" interfaces.ifTable.ifEntry.ifDescr.3="serial0/0"
interfaces.ifTable.ifEntry.ifDescr.4="bri0/0" interfaces.ifTable.ifEntry.ifDescr.5="x25-node" interfaces.
ifTable.ifEntry.ifDescr.6="voip1/0" interfaces.ifTable.ifEntry.ifDescr.7="serial2/0" interfaces.ifTable.ifEntry.
ifDescr.8="fr2"
```

What is interesting here is this: GetBulk(29) **N=0 M=10 i**nterfaces.ifTable.ifEntry.ifIndex, this is using a maximum of 10 SNMP PDU's in a packet, NET-SNMP on the command line appears to use 10 as a default OR not use bulk walks.

If you have not configured max repetitions in NMIS, you would see this:

```
01:41:37.093751 IP 1.2.3.4.48560 > 2.3.4.5.snmp:  C=COMMUNITYSTRING GetBulk(29)  N=0 M=25 interfaces.ifTable.
ifEntry.ifIndex
01:51:37.093751 IP 1.2.3.4.48560 > 2.3.4.5.snmp:  C=COMMUNITYSTRING GetBulk(29)  N=0 M=25 interfaces.ifTable.
ifEntry.ifIndex
```

Then NMIS would give you the errors above. This is using a default of M=25 which set in the Perl NET-SNMP libraries or somewhere even more obscure.

Net Result, you will need to configure your NMIS Node with

'max_repetitions' => ’10',

You can find more details about SNMP things @ SNMP Tuning

snmpd returns "invalid(4)" process state (hrSWRunStatus) for process names containing spaces

net-snmp version 5.7.2 is known to be affected:
https://bugzilla.redhat.com/show_bug.cgi?id=1782180

When querying the hrSWRunStatus table via SNMP when using snmpd, it should generally return 1 or 2 for processes that are running or runnable. However, if the process name contains a space, snmpd return 4 (invalid) for the process state.

This appears to be because it's reading /proc/$PID/stat and simply splitting on space and then grabbing the third element,
which would normally be the process status, but when the process name contains a space, this is no longer true.

```
NMIS# systemctl status omkd
 omkd.service - Opmantek Webserver
   Loaded: loaded (/etc/systemd/system/omkd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2020-09-24 11:02:54 UTC; 10h ago
 Main PID: 3137 (opmantek.pl web)
   CGroup: /system.slice/omkd.service
           3137 opmantek.pl webserver                                        -f -p /var/run
/opmantek.exe.pid -r
           3253 opmantek.pl webserver                                        -f -p /var/run
/opmantek.exe.pid -r
           3254 opmantek.pl webserver                                        -f -p /var/run
/opmantek.exe.pid -r
           3255 opmantek.pl webserver                                        -f -p /var/run
/opmantek.exe.pid -r
           3256 opmantek.pl webserver                                        -f -p /var/run
/opmantek.exe.pid -r
           3257 opmantek.pl webserver                                        -f -p /var/run
/opmantek.exe.pid -r

Sep 24 11:02:22 omk-vm9-centos7 systemd[1]: Starting Opmantek Webserver...
Sep 24 11:02:54 omk-vm9-centos7 systemd[1]: Started Opmantek Webserver.

NMIS# snmpd --version
NET-SNMP version:  5.7.2

NMIS# cat /proc/3253/stat
3253 (opmantek.pl web) S 3137 3137 3137 0 -1 4202816 5749 0 0 0 390 43 0 0 20 0 1 0 4442 543064064 64976
18446744073709551615 1 1 0 0 0 0 0 4224 5 18446744073709551615 0 0 17 0 0 0 0 0 0 0 0 0 0 0 0 0 0

NMIS# snmpwalk -v 2c -c COMMUNITYSTRING 127.0.0.1 1.3.6.1.2.1.25.4.2.1.7.3253
HOST-RESOURCES-MIB::hrSWRunStatus.3253 = INTEGER: invalid(4)
```

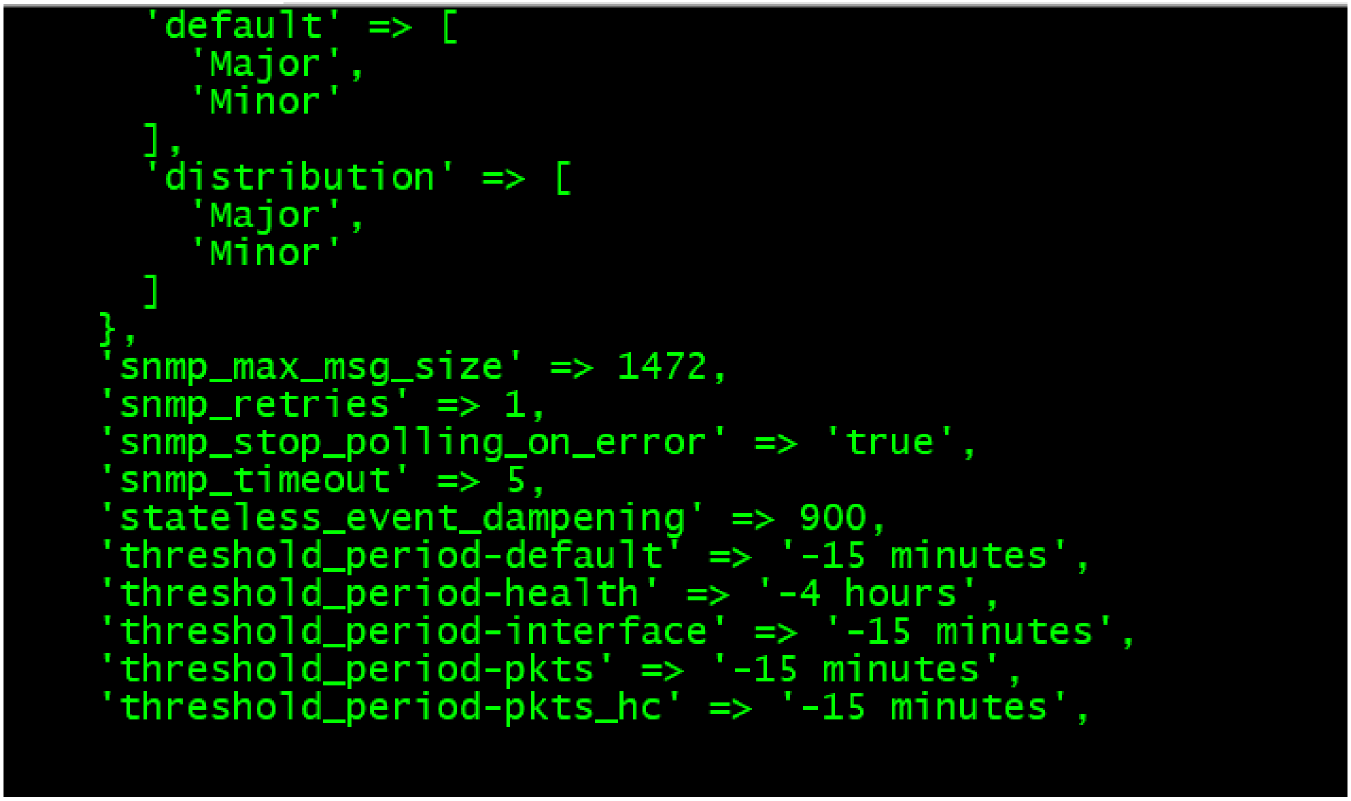
A consequence of this issue is that when an affected version of snmp is installed,
MMIS will report a monitored service as 'down' when it is 'running' if the process name contains a space.

Max Message size too small/large

snmp_max_msg_size

Go to /usr/local/nmis9/Conf/

vim Conf.nmis



```
      'default' => [
        'Major',
        'Minor'
      ],
      'distribution' => [
        'Major',
        'Minor'
      ]
    },
    'snmp_max_msg_size' => 1472,
    'snmp_retries' => 1,
    'snmp_stop_polling_on_error' => 'true',
    'snmp_timeout' => 5,
    'stateless_event_dampening' => 900,
    'threshold_period-default' => '-15 minutes',
    'threshold_period-health' => '-4 hours',
    'threshold_period-interface' => '-15 minutes',
    'threshold_period-pkts' => '-15 minutes',
    'threshold_period-pkts_hc' => '-15 minutes',
```

The primary tunable NMIS configuration setting for SNMP is `snmp_max_msg_size`, which controls how large a single SNMP packet may be.

This can be set as a system-wide default (in the System menu, under System Configuration), or as a per-host setting (in the Edit Node menu, under Advanced Options).

The default for `snmp_max_msg_size` is 1472 bytes, just below the 1500 byte packet limit for normal Ethernets. In LAN-only scenarios it is possible to increase this past 1500 bytes: this causes IP fragments and packet reassembly, but unless your LAN is saturated and starving for bandwidth fragmentation is not a problem. The benefit of a larger SNMP packet would be that the data to be collected fits into fewer packets.

To quickly adjust this setting you could run the following command using the node_admin.pl tool that ships with NMIS. The max_msg_size value of course can be increased or decreased as desired.

```
/usr/local/nmis9/admin/node_admin.pl act=set node=nodename entry.configuration.max_msg_size=2800
```

SNMP Partially Working in NMIS but SNMPWALK works no problem

Many SNMP agents to not comply to the SNMPv2c specifications so do not support multiple SNMP PDU's in a single packet. This feature can be disabled by setting max_repetitions to 1, which means one SNMP PDU per SNMP packet.

```
/usr/local/nmis9/admin/node_admin.pl act=set node=nodename entry.configuration.max_repetitions=1
```