Simple Network Management Protocol

The SNMP protocol exists in three widely used versions; v1, v2c and v3.

All Eltek controllers with Ethernet port have support for one or more versions of SNMP. Controllers with SNMP agent that does not support v3 have setup of SNMP via the internal webpages.

For controllers with SNMP agent that support V3, all setup of SNMP is done via SNMP protocol as specified in RFC3411-RFC3418.

How to SNMP with Eltek controllers

This document describes setup for SNMPv3 agents and prior.

DOC 2155710 – 1

Table of Contents

Background

Traditionally the installation staff has often done the setup of SNMP via a web-browser on site during commissioning. With the release of controller firmware that includes SNMP agent that supports SNMPv3 this is not possible any more. It has been removed because v3 brings a far more secure communication compared to v2c, and keeping setup through webpages would be a security hole.

Setup through SNMP protocol is much more difficult to understand than typing in the web page text boxes. It also requires software that is not normally found on the average laptop.

Definitions

- **Eltek MIB**: the mib-file that follows the firmware in the controller to connect to. All Eltek mib-files have OIDs starting with .1.3.6.1.4.1.12148. If only one type of controller FW needs to supported, then load the 'EltekEnexusPowersystem.mib' or 'EltekDistributedPowerplantVx.mib' into the SNMP tool. For a typical application all the controllers which are required to monitor by a NMS may require various branches of the Eltek MIBs. If so first load the 'Eltek_Root.mib' and then the various branches that comes with the controller firmware, i.e 'EltekEnexusPowersystem_branch10.mib'

- **Generic SNMP MIBS:**
  - **RFC 1213 MIB**: Management Information Base for Network Management of TCP/IP-based internets: MIB-II. Basic identification and information OIDs starting with .1.3.6.1.2.1
  - **SMIv2 (RFC 2578, RFC 2579, RFC 2580):** MIB Syntax Specification for v2c
  - **SNMP-COMMUNITY-MIB (RFC 3584):** Coexistence between v1, v2c and v3. Actually it's community strings for v1 and v2c
  - **SNMP-FRAMEWORK-MIB (RFC 3411):** Agents SNMP engine information
  - **SNMP-MPD-MIB (RFC 3412):** SNMP engine dispatcher information
  - **SNMP-TARGET-MIB (RFC 3413):** Notification targets and routes
  - **SNMP-NOTIFICATION-MIB (RFC 3413):** Holds information of which management targets should receive notification and type of notification. (Eltek has only implemented 'trap' type. NotifyFilter is also not implemented yet)
  - **SNMP-USER-BASED-SM-MIB (RFC3414 - USM):** Stores information about users and their protocol (SNMP v1/v2c/v3) and security setup (noAuthNoPriv/authNoPriv/authPriv).
  - **SNMP-VIEW-BASED-ACM-MIB (RFC 3415 - VACM):** Defines the users groups and the view/write/notify access for the groups.

DEFAULT SNMP & WEB ACCESS SETTINGS

If not specifically ordered to be changed, the controllers come with the following default SNMP settings:

Controllers with SNMP v3 support

The controllers come with 6 default users which has the following access levels:

User name	Authentication protocol	Privacy protocol	Access Level
Admin	sha	Aes	Read,Write and Notify access to all sub-trees of 1.3.6
Control	sha	Des	Read,Write and Notify access of Eltek mib.
status1	md5	Des	Read and Notify access of Eltek mib.
status2	md5	Aes	Read and Notify access of Eltek mib.
snmpv1-usr	NA	NA	Read and Notify access of Eltek mib.
snmpv2c-usr	NA	NA	Read and Notify access of Eltek mib.

Only the admin user has access to the parts of the mib that does the setup of the SNMP. The other users are only set up to access the Eltek mib

Adminstrator:

- **Protocol required: v3**
- **defSecurityName admin**
- **defAuthPassphrase adminauth**
- **defPrivPassphrase adminpriv**
- **defAuthType sha**
- **defSecurityLevel authPriv**
- **defPrivType AES**

SNMP v2/v1 on all controllers

The controllers' web interface has the following default users and passwords:

Community Name	Access Level
Public	.
Private	.

* SSL encryption supported on most, but not all, controller FW revisions

Web setting on all controllers

The controllers' web interface has the following default users and passwords:

User name	Password	Privacy protocol	Access Level
Admin	admin	http/https*	Read and Write of all parameters including user setup and network configuration
Control	control	http/https*	Read and write of all power system configuration, but not user and network setup
Status	status	http/https*	Read/view all fields

* SSL encryption supported on most, but not all, controller FW revisions

USING Net-SNMP

Net-SNMP is an open-source distribution of applications used for communication on SNMP v1, SNMP v2c and SNMP v3. The suite has code licenced under various BSD licenses (see http://www.net-snmp.org/about/license.html for details).

Net-SNMP is widely used and by many seen upon as the reference for SNMP communication, and one of the very few free applications that offers SNMPv3. Hence, these applications were chosen when writing this manual.

In order to communicate with the SNMPv3 supporting Eltek controllers, the Open-SSL library is needed to support the authentication and encryption.

Get and Install Open-SSL

Version 0.9.8 is needed. Windows installer for 32 bit and 64 bit can be downloaded from here:
http://slproweb.com/products/Win32OpenSSL.html

32 bit: http://www.slproweb.com/products/Win32OpenSSL_Light-0_9_8y.exe (or a newer build than 'y')

64 bit: http://www.slproweb.com/products/Win64OpenSSL_Light-0_9_8y.exe (or a newer build than 'y')

Please note Open-SSL requires "Microsoft Visual C++ 2008 Redistributable Package". If it is not installed on the computer the Open-SSL installer will notify, abort the Open-SSL installation; install the above C++ package before continuing.

Run the installer. Please choose default location.

Get and Install Net-SNMP

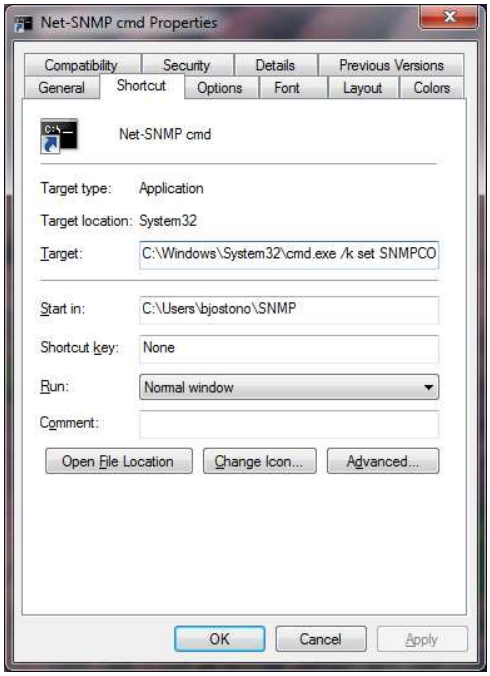
Get the SNMP installation files form http://sourceforge.net/projects/net-snmp/files/net-snmp%20binaries/. During the creation of this manual (August 2013) version 5.7 (32 bit version) and 5.5 (64 bit version) were used.

Run the installer and make sure 'Encryption support (OpenSSL)' checkbox is ticked off.

Configure and test Net-SNMP

Net-SNMP is run in the command line. The location of the Net-SNMP binaries needs to be added to the PATH environmental variable and also the location of the configuration file 'snmp.conf' needs to be specified. This can be done in (at least) three ways:

1. Create a "Net-SNMP Cmd" short-cut on the desktop that sets these variables when launching the default windows command line. The start-up folder can also be specified under 'Start-in'. The command for setting the environmental variable is (change path_to_snmp.conf (this should have forward slashes for folder separation, i.e 'C:/Users/bjostono/SNMP/Setup'), verify Net-SNMP path):
   'C:\Windows\System32\cmd.exe /k set PATH=c:\usr\bin;%path% &
   set SNMPCONFPATH=path_to_snmp.conf'
2. Start the cmd.exe, and then run a bat-file that has the two above 'set' commands or type them each session.
3. Open "Control Panel", click on 'System' and then 'Advanced system settings'. Under the 'Advanced' tab you'll find 'Environmental Variables'. Click on this and insert 'c:\usr\bin' at the end of the 'PATH' variable. Add a new variable called 'SNMPCONFPATH' and then type the correct path.



The snmp.conf file should contain information about where to find the Eltek Powersystem MIB file(s) and also it is very convenient to add the administrator as default user and his/hers credentials to save time when typing the commands. An example file is found below. The '#' denotes comments not read/used by Net-SNMP.

```
# Set the admin user and its credentials as default to avoid typing them in each command
defSecurityName  admin
defAuthPassphrase adminauth
defPrivPassphrase adminpriv
defAuthType      sha
defSecurityLevel  authPriv
defPrivType      AES
# Specify folder where the Eltek MIB is located and within this folder add a MIB containing SP2-MIB definitions
mibdirs +C:\Users\bjostono\Documents\Eltek\MIB
mibs +SP2-MIB
```

Example 1: snmp.conf

So, once this is in place it is time to test the installation (change the IP address to a controller on your network);

```
C:\Users\bjostono\SNMP>snmpget 172.16.7.140 sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: ELTEK Power System

C:\Users\bjostono\SNMP>snmpget -lauthPriv -v3 -u admin -a sha -A adminauth -x AES -X adminpriv 172.16.7.140
.1.3.6.1.2.1.1.1.0
SNMPv2-MIB::sysDescr.0 = STRING: ELTEK Power System

C:\Users\bjostono\SNMP>snmpget 172.16.7.140 batteryVoltageValue.0
SP2-MIB::batteryVoltageValue.0 = INTEGER: 5379

C:\Users\bjostono\SNMP>
```

Example 2: First commands to test the installation and setup

The first command reads the sysDescr.0 parameter which is defined in the generic RFC1213 MIB. The 3rd command reads the battery voltage value which is specified in the Eltek MIB. These two commands verify the administrator credentials are correct in the 'snmp.conf' and that it has the Eltek MIB loaded.

More details on the 1st and 2nd commands: Net-SNMP will search through its loaded mibs for the text 'sysDescr' to find it's corresponding OID and then issue a SNMP GET request using version 3 and the default user (since no user is specified). The second command describes this;

-lauthPriv - use authentication and encryption
-v3 - use SNMP version 3
-u admin - user is 'admin'
-a sha - use SHA authentication protocol
-A adminauth - admin user's authentication passphrase/password
-x - privacy/encryption protocol to use
-X adminpriv - admin user's encryption passphrase/key
172.16.7.140 - the target controller IP address
.1.3.6.1.2.1.1.1.0 – the OID of sysDescr.0

It is really not a good idea to move forward in this 'How-to' before these commands runs correctly. Here are a couple of error messages and what to check if you do not get the responses above from your controller;

- "No log handling enabled - using stderr logging, snmpget: Timeout" → verify the connection to the controller; run a ping command; 'ping IP_address'
- "No log handling enabled - using stderr logging; batteryVoltageValue.0: (Sub-id not found: (top) -> BatteryVoltageValue)" → verify that the path to Eltek MIB file is correct.
- "No log handling enabled - using stderr logging, snmpget: No securityName specified (Sub-id not found: (top) -> sysDescr)" → verify that the path to the 'snmp.conf' file is correct
- "No log handling enabled - using stderr logging, snmpget: Authentication failure (incorrect password, community or key) (Sub-id not found: (top) -> sysDescr)" → verify the administrator user credentials in 'snmp.conf'.

SNMPv2c-ing with SNMPv3 supporting controllers

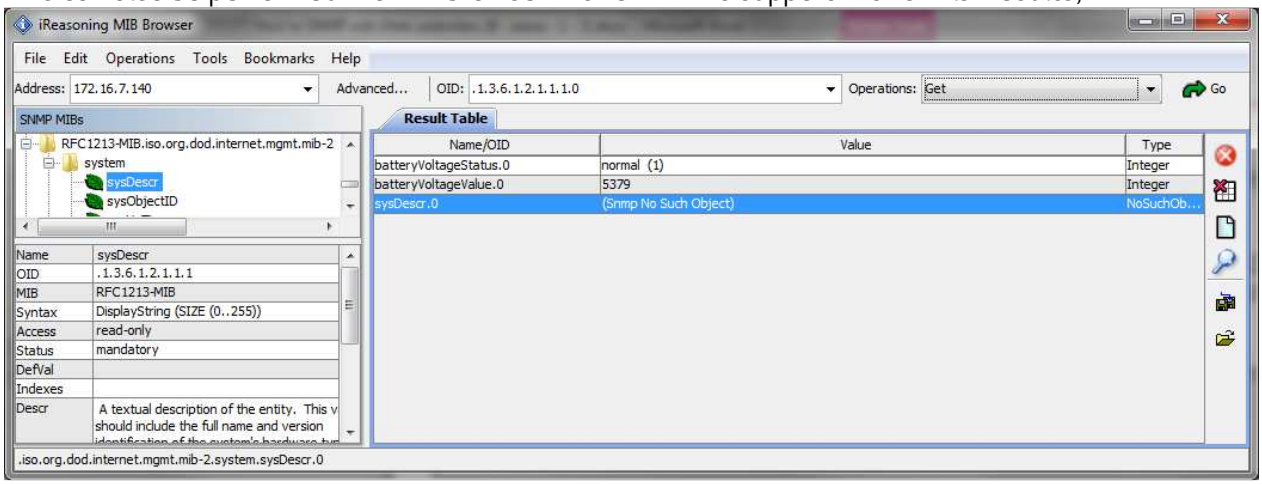
As stated in the default settings chapter it is by default set up a user that communicates over SNMPv2c in the controller. This user has Read and notify access to the Eltek MIB, but not the generic parts where the SNMP setup is stored.

So, for the exercise we performed to test the Net-SNMP, we would for the snmpv2c-usr get the following results;

```
C:\Users\bjostono\SNMP>snmpget -v2c -c public 172.16.7.140 sysDescr.0
SNMPv2-MIB::sysDescr.0 = No Such Object available on this agent at this OID

C:\Users\bjostono\SNMP>snmpget -v2c -c public 172.16.7.140 batteryVoltageValue.0
SP2-MIB::batteryVoltageValue.0 = INTEGER: 5372

C:\Users\bjostono\SNMP>
```

Example 3 : Getting information using the snmpv2c_usr user

This can also be performed in a MIB browser with SNMPv2c support with similar results;



Example 4 : Getting information using the snmpv2c_usr user in a MIB browser.

WRITE ACCESS VIA SNMPv2c

By default, only the SNMPv3 users 'admin' and 'control' has write or set access via SNMP. To gain write access via v2c or v1 their corresponding groups' rows in the vacmAccessTable must be altered. Since this table is only accessible via SNMPv3 by factory settings, the Example 5 bellow shows a few commands using Net-SNMP to gain write access via the SNMPv2c community access;

1. Try to set a parameter - fails
2. Prints the vacmAccessTable – no WriteView set for the 'snmpv2c-group'
3. Delete access line for snmpv2c-group
4. Create access for snmpv2c-group including write view
5. Prints the table to verify change (optional)
6. Try to set a parameter – success

Write access to the ELTEK part of the MIB is now granted. If desirable, complete access can be granted by specifying 'admin-view' (all sub-trees under 1.3.6) for the snmpv2c-group. By doing this the SNMP setup MIBs can be accessed and setting up users, trap receivers and access can be done via SNMPv2c.

1. Delete access line for snmpv2c-group
2. Create access for snmpv2c-group including write view
3. Try to read a parameter under the setup subtree 'sysDescr'– success
4. Try to change access; remove access for SNMPv1_group – success

```
C:\Users\bjostono\SNMP>snmpset -v 2c -c private 172.16.7.148 powerSystemCompany.0 s "Eltek - Always on"
Timeout: No Response from 172.16.7.148

C:\Users\bjostono\SNMP>snmptable -Cbi 172.16.7.148 vacmAccessTable
SNMP table: SNMP-VIEW-BASED-ACM-MIB::vacmAccessTable

                    index ContextMatch ReadViewName WriteViewName NotifyViewName StorageType Status
    "admin-group"."".3.authPriv     exact  admin-view    admin-view     admin-view  non-volatile active
 "snmpv1-group"."".1.noAuthNoPriv   exact  snmpv1-view                  snmpv1-view  nonVolatile active
"snmpv2c_group"."".2.noAuthNoPriv   exact  snmpv2c_view                 snmpv2c_view nonVolatile active
   "readonly-group"."".3.authPriv   exact  readonly-view                readonly-view  non-volatile active
"snmpv12c-group"."".1.noAuthNoPriv  exact  snmpv1-view                  snmpv1-view  non-volatile active
  "readwrite-group"."".3.authPriv   exact  readwrite-view readwrite-view readwrite-view non-volatile active

C:\Users\bjostono\SNMP>snmpvacm 172.16.7.148 deleteAccess snmpv2c_group 2 1
Access successfully deleted.

C:\Users\bjostono\SNMP>snmpvacm 172.16.7.148 createAccess "snmpv2c-group" 2 1 1 snmpv2c-view snmpv2c-
view snmpv2c-view
Access successfully created.

C:\Users\bjostono\SNMP>snmptable -Cbi 172.16.7.148 vacmAccessTable
SNMP table: SNMP-VIEW-BASED-ACM-MIB::vacmAccessTable

                    index ContextMatch ReadViewName WriteViewName NotifyViewName StorageType Status
    "admin-group"."".3.authPriv     exact  admin-view    admin-view     admin-view  nonVolatile active
 "snmpv1-group"."".1.noAuthNoPriv   exact  snmpv1-view                  snmpv1-view  nonVolatile active
"snmpv2c-group"."".2.noAuthNoPriv   exact  snmpv2c-view snmpv2c-view    snmpv2c-view    volatile active
   "readonly-group"."".3.authPriv   exact  readonly-view                readonly-view  nonVolatile active
"snmpv12c-group"."".1.noAuthNoPriv  exact  snmpv1-view                  snmpv1-view  nonVolatile active
  "readwrite-group"."".3.authPriv   exact  readwrite-view readwrite-view readwrite-view nonVolatile active

C:\Users\bjostono\SNMP>snmpset -v 2c -c private 172.16.7.148 powerSystemCompany.0 s "Eltek - Always on"
SP2-MIB::powerSystemCompany.0 = STRING: Eltek - Always on

 C:\Users\bjostono\SNMP>snmpvacm 172.16.7.148 deleteAccess snmpv2c-group 2 1
Access successfully deleted.

C:\Users\bjostono\SNMP>snmpvacm 172.16.7.148 createAccess "snmpv2c-group" 2 1 1 admin-view admin-view
admin-view
Access successfully created.

C:\Users\bjostono\SNMP>snmpget -v 2c -c private 172.16.7.148 sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: ELTEK Power System

C:\Users\bjostono\SNMP>snmpvacm -v 2c -c private 172.16.7.148 deleteAccess snmpv1_group 1 1
Access successfully deleted.
```

Example 5: Setting write access for SNMPv2c users

CHANGING THE COMMUNITY NAMES

The community names which are sort of the password or passphrase when communicating over v1 or v2c, are specified in the SnmpCommunityTable. This table is only accessible via the SNMPv3 admin user. The example below shows how this is done using Net-SNMP:

5. Prints the table
6. Sets the row/instance to be change out of service
7. Changes the community name to 'new_private'
8. Prints the table to verify change (optional)
9. Puts the row/instance back in service
10. Tests the new community name by reading the battery voltage value of the system.

```
C:\Users\bjostono\SNMP>snmptable -Cbli 172.16.7.141 snmpCommunityTable
SNMP table: SNMP-COMMUNITY-MIB::snmpCommunityTable

index      Name     SecurityName ContextEngineID ContextName TransportTag StorageType Status
'private-v2c'"private" snmpv2c-usr  "78901"              group-v2    volatile   active
'public-v12c'"public"  snmpv2c-usr  "12345"              group-v2    volatile   active

C:\Users\bjostono\SNMP>snmpset 172.16.7.141 snmpCommunityStatus.'private-v2c' i 2
SNMP-COMMUNITY-MIB::snmpCommunityStatus.'private-v2c' = INTEGER: notInService(2)

C:\Users\bjostono\SNMP>snmpset 172.16.7.141 snmpCommunityName.'private-v2c' s new_private
SNMP-COMMUNITY-MIB::snmpCommunityName.'private-v2c' = STRING: "new_private"

C:\Users\bjostono\SNMP>snmptable -Cbli 172.16.7.141 snmpCommunityTable
SNMP table: SNMP-COMMUNITY-MIB::snmpCommunityTable

index      Name        SecurityName ContextEngineID ContextName TransportTag StorageType Status
'private-v2c'"new_private" snmpv2c-usr  "78901"              group-v2    volatile   notInService
'public-v12c'"public"     snmpv2c-usr  "12345"              group-v2    volatile   active

C:\Users\bjostono\SNMP>snmpset 172.16.7.141 snmpCommunityStatus.'private-v2c' i 1
SNMP-COMMUNITY-MIB::snmpCommunityStatus.'private-v2c' = INTEGER: active(1)

C:\Users\bjostono\SNMP>snmpget -v 2c -c new_private 172.16.7.141 batteryVoltageValue.0
SP2-MIB::batteryVoltageValue.0 = INTEGER: 13625
```

Example 6: Change community names

TRAPS

Setting the trap receiver address is the only action that needs to be performed via the SNMPv3 admin user.

	A	B	C	D	E	F	G	H
1	Rev 2	Decimal		Hex		Commands		
2	IPadr	172		AC		=DEC2HEX(B2;2)		
3		16		10		=DEC2HEX(B3;2)		
4		5		05		=DEC2HEX(B4;2)		
5		76		4C		=DEC2HEX(B5;2)		
6	Port	162		00A2		=DEC2HEX(B6;4)		
7								
8	Total Hex String			0xAC10054C00A2		="0x"&D2&D3&D4&D5&D6		
9								
10	Copy 'value' of D8			0xAC10054C00A - textstring to be pasted into bat file or cmd				
11	(Keys: Crtl+[V], Ctrl, V)							

The trap-receivers IP address and port are to be specified in a hexadecimal string. For those of us not doing this by mind, the calculation can easily be done in a excel sheet.

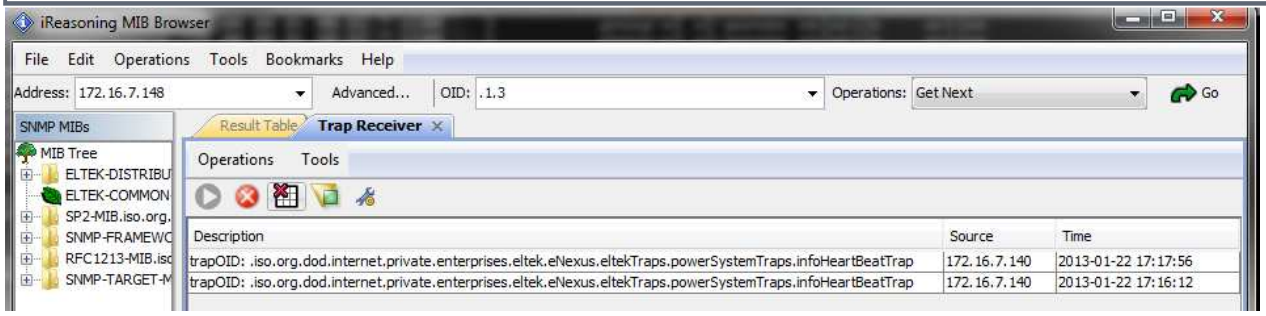
The controllers comes by default setup to send traps to the community strings “public” and “private” using SNMPv2 transportation. However the IP address and network port of such a SNMPv2c TRAP receiver must be specified. This is done by issuing a line into the target address table as shown below. The blue-ish text is what is typed, and the black are the response. So, the line is created with bJoeRn-PC-WLAN as index/identifier, UDP protocol, the IP address and default port in Hexadecimal, which tag list and parameters. Then the controller responds for each parameter in the new row. Then the table is read back in the next command, just for the sake of reassuring.

```
C:\Users\bjostono\SNMP>snmpset 172.16.7.140 ^
More? snmpTargetAddrRowStatus.'bJoeRn-PC-WLAN'   i createAndGo ^
More? snmpTargetAddrTDomain.'bJoeRn-PC-WLAN'     o snmpUDPDomain ^
More? snmpTargetAddrTAddress.'bJoeRn-PC-WLAN'    x 0xAC10054C00A2 ^
More? snmpTargetAddrTagList.'bJoeRn-PC-WLAN'     s group-v2 ^
More? snmpTargetAddrParams.'bJoeRn-PC-WLAN'      s v2-params ^
More? snmpTargetAddrStorageType.'bJoeRn-PC-WLAN' i nonVolatile
SNMP-TARGET-MIB::snmpTargetAddrRowStatus.'bJoeRn-PC-WLAN' = INTEGER: createAndGo(4)
SNMP-TARGET-MIB::snmpTargetAddrTDomain.'bJoeRn-PC-WLAN' = OID: SNMPv2-TM::snmpUDPDomain
SNMP-TARGET-MIB::snmpTargetAddrTAddress.'bJoeRn-PC-WLAN' = Hex-STRING: AC 10 05 4C 00 A2
SNMP-TARGET-MIB::snmpTargetAddrTagList.'bJoeRn-PC-WLAN' = STRING: group-v2
SNMP-TARGET-MIB::snmpTargetAddrParams.'bJoeRn-PC-WLAN' = STRING: v2-params
SNMP-TARGET-MIB::snmpTargetAddrStorageType.'bJoeRn-PC-WLAN' = INTEGER: nonVolatile(3)

C:\Users\bjostono\SNMP>snmptable -Cbli 172.16.7.140 targetAddrTable
SNMP table: SNMP-TARGET-MIB::snmpTargetAddrTable

index          TDomain                TAddress                  Timeout RetryCount TagList  Params      StorageType RowStatus
'bJoeRn-PC-WLAN' SNMPv2-TM::snmpUDPDomain "AC 10 05 4C 00 A2 " 1500    3          group-v2 v2-params  nonVolatile active
'trap-host-v1'   SNMPv2-TM::snmpUDPDomain "7F 00 00 01 00 A2 " 1500    3          group-v1 v1-params  volatile    active
'trap-host-v2'   SNMPv2-TM::snmpUDPDomain "7F 00 00 01 00 A2 " 1500    3          group-v2 v2-params  volatile    active
'trap-host-v3'   SNMPv2-TM::snmpUDPDomain "7F 00 00 01 00 A2 " 1500    3          group-v3 v3-params  volatile    active
```

Example 7 : Adding a SNMPv2 trap target

So, it is time to see the TRAPs being sent. An alarm could be triggered on the system or the Heart Beat Trap could be activated:

```
C:\Users\bjostono\SNMP>snmpset 172.16.7.140 snmpHeartBeatTrapRepeatRate.0 i 1
SP2-MIB::snmpHeartBeatTrapRepeatRate.0 = INTEGER: 1
```



Example 8: Turning on heart beat trap and receiving the trap in v2 MIB browser

And then (finally) the TRAPs should start showing up in your favourite TRAP receiver.

Document Change Record

Rev.	Date (dd.mm.yyyy)	Pages affected	Change Description
1	27.08.2013	All	First revision