SNMP Manual

Version 5

SHAPING THE FUTURE OF SATELLITE COMMUNICATIONS

Newtec

Newtec cy
Laarstraat 5
9100 Sint-Niklaas, Belgium

General: +32 (0)3 780 65 00
www.newtec.eu
Fax +32 (0)3 780 65 49
General: general@newtec.eu

Release History

Edit	Date	Author	Approved by	Description
0	July 13, 2004	GDR		First version
1	July 26, 2004	GDR		Official release
2	September 23, 2004	GDR		Community definition
3	January 6, 2005	GDR		New entry second Trap IP address
4	December 21, 2005	GDR		New agent NTC/6281

Abstract.

This document describes the SNMP functionality for the Azimuth series of products.

TABLE OF CONTENTS

1 INTRODUCTION.

SNMP (Simple Network Management Protocol) is an application-layer protocol for managing TCP/IP based networks. It runs over UDP at the transport level.

Newtec's devices are SNMP manageable.

This means that they have an SNMP agent and can be polled for information from a Network Management Station (NMS).

Our SNMP agent is considered MIB-II compliant.

The Newtec Management Information Base (MIB) provides a standard representation of the SNMP Agent's available information and where it is stored. The MIB is defined according to the ASN.1. Newtec SNMP manageable devices also support the Trap PDU.

A trap is a mechanism to trigger the NMS that a change in the device has occurred. After receiving the trap the NMS still has to poll the device to find out the details of the change.

2 HOW IT WORKS.

The standard boot procedure for an Azimuth device with regards to SNMP includes:

1. Starting the NTC/6281 SNMP daemon.
2. Creating the oidmap.txt file which contains the mapping of all available RMCP commands for a specific unit onto RMCP commands.

Once booted, the Newtec SNMP agent is running and will reply to the standard SNMP commands.

In order for the agent to reply to specific information about the device, the SNMP capability must be turned on. Only then the agent will be able to request information from the different boards inside the Azimuth unit.

The SNMP agent will translate incoming SNMP Protocol Data Units or PDUs' (Get, GetNext, Set) from the NMS into RMCP commands. The RMCP command is passed on to the appropriate board of the device and executed. The RMCP reply is sent back to the SNMP Agent.

The SNMP Agent in turn responds to all requests or commands with the Response

3 PREREQUISITES

3.1 Version verification.

- SNMP Agent firmware: version 1.01 or higher must be installed.
- M&C software: please check with Newtec customer support what version is required. The version should be lined-up with the SNMP agent version.

3.2 SNMP capability

In order to be fully SNMP manageable the Newtec device must have the 'SNMP capability' enabled. This capability is reflected in the unit's product ID e.g. AZ…/Unit/Architecture/General/Product Id

A product ID ending in 'A' means SNMP capability is not enabled, a product ID ending in 'B' means SNMP capability is enabled.

The SNMP capability can be specified upon ordering. Customers that request SNMP support for existing units that do not have SNMPcapability activated should contact Newtec's sales department.

3.3 MIB

The Newtec MIB is derived from the SEMS device definition database and allows full monitor and control over the complete device using any SNMP browser (HPOpenView, NetworkView).

We support the basic standard MIB (monitor and control of IP interface, versions of the software …) and above that we have a full proprietary MIB. There is only one MIB for all of the Newtec devices.

The customer must compile the obtained .mib files from within his Network Management Software.

There are two MIB files:

1. NEWTEC-MAIN-MIB: This is the Newtec top level MIB containing 3 subtrees
   a. ntcSems: Subtree for definitions for SEMS (Newtec's Satellite Earth-station Management System.
   b. ntcPlex: Extensions of ntcSems specific for the SkyPlex system.
   c. ntcDevices: Subtree to manage Newtec devices.
2. NEWTEC-DEVICES-MOD01-MIB: MIB Module for the management of devices of the AZIMUTH series (sub-tree 3; fully documented with MIB object descriptions as in the RMCP manual).

This MIB contains the SystemTable, AlarmTable (which are common to all devices) and device specific tables necessary to control every Azimuth device.

Note that in order to have read/write access the community should be set to‘public’.

Please contact Newtec Customer Support at Techsupport@newtec.be for the latest version of these MIB files.

4 TRAP MECHANISM

4.1 Introduction

A trap will be sent by the Agent whenever a state change (off or on) in the alarm status of the device occurs.

The Agent encapsulates the trap PDU in UDP datagrams and generates trap messages from port 161. The NMS will receive trap messages on port 162.

The trap message consists of 3 varbinds:

1. Binding #1: sysUpTime.0 *** (timeticks) 0 days 16h:41m:39s.03th
2. Binding #2: internet.6.3.1.1.4.1.0 *** (oid) ntcDevsMod01StatusChange
3. Binding #3: ntcDevsMod01AlAlarmsCur.0.1 *** (octets) 00000000010000000000 [30.30.30.30.30.30.30.30.30.31.30.30.30.30.30.30.30.30.30.30 (hex)]

Binding #3 contains the current alarm buffer contents.

The counting of the bytes starts from 0 and is from left to right.

4.2 How to determine the TRAP state

When the NMS receives a trap it should check whether the trap is related to an ‘alarm on’ or ‘alarm off’ occurrence (since UDP is a connectionless protocol a trap might get lost).

First, the alarm buffer should be cleared to get rid of all memorized alarms. Therefore, an NMS should execute a SET operation with value ‘0’ on ntcDevsMod01AlAlarmscur.0.1 (O.I.D. 1.3.6.1.4.1.5835.3.1.2.1.9.0.1). This will return the current alarm buffer contents and reset the buffer.

Then a GET operation should be executed.

When the GET reply is a null string then the trap resulted from the alarm going to ‘off’ state.

When the GET reply is a string containing at least one byte set to ‘1’ then the trap resulted from the alarm going to ‘on’ state.

By interpreting the individual bytes of the concatenated alarm string, the exact cause of the alarm can be deducted.

4.3 Alarm string contents.

Note: All SNMP commands hereafter reside under the ntcDevsMod01AlarmTable.

The alarm string of a device is dynamically built up during booting of the device. The contents/length of the string is determined by the hardware installed. Consequently the 'AlAlarmsCur' string will be different between devices and could even different between two devices of the same type.

An NMS should therefore always perform the following operations after the device has booted.

4.3.1 Determine the length of the AlAlarmsCur string.

This is done by executing a GET operation on

ntcDevsMod01AlAlarmCount.1.1 (oid 1.3.6.1.4.1.5835.3.1.2.1.3).

The response binding will give the length of the string.

Example:

Request binding:

1. ntcDevsMod01AlAlarmCount.1.1 (null) null

Response binding:

1. ntcDevsMod01AlAlarmCount.1.1 (octet string) 20 [32.30 (hex)]

The length of the alarm string is 20.

4.3.2 Determine the description of the n-th alarm-buffer of the device.

This is done by executing a GET operation on

ntcDevsMod01AlAlarmDesc.1.1 (oid 1.3.6.1.4.1.5835.3.1.2.1.5).

This get-request actually requires parameters. In order to pass these parameters, the parameters must be set into the relevant OID preceded with a question-mark (?).

The result of this get-request can then be read in the ntcDevsMod01LastReply object.

The reply will consist of two parts separated by a semicolon ';'. The first part is the alarm name (intended for SW managing the device, like Newtec SEMS), while the second part is a short description of the alarm.

Remark

When running a diagnostic report on the device the output of the NTCxxx/Alarm/Device menu should correspond to the length/description of the alarm buffer as determined with the above procedure.

4.3.3 Example

SET operation

GET operation

Request binding:

1: ntcDevsMod01LastReply.0 (null) null

Response binding:

1: ntcDevsMod01LastReply (octet string) ntcSeEqAlDevTemp;Device temperature

[6E.74.63.53.65.45.71.41.6C.44.65.76.54.65.6D.70.3B.44.65.76.69.63.65.2

0.74.65.6D.70.65.72.61.74.75.72.65 (hex)]

5 SNMP MENU ITEMS

There is a special menu item that encloses all of the settings related to SNMP:

AZ…/Unit/Setup/SNMP settings

It contains the following entries:

5.1 Read community

The SNMP community name with read-only access.

Default set to 'public'.

RMCP info:

SNMP read only community - SyROCommunity

Description: The SNMP community name with read-only access

Rmcp header: SRo (expert: get and set, normal: no access)

Example:

Get	SRo?	//get read only community
Get Reply	SRo?public	//get read only community is public

SNMP info:

Name: ntcDevsMod01SyROCommunity

Type: OBJECT-TYPE

OID: 1.3.6.1.4.1.5835.3.1.1.1.70

5.2 Read/write community

The SNMP community name with read-write access

Default set to 'public'.

RMCP info:

SNMP read only community - SyRWCommunity

Description: The SNMP community name with read-write access

Rmcp header: SRw (expert: get and set, normal: no access)

Example:

Get	SRw?	//get read-write community
Get Reply	SRw?public	//get read-write community is public

SNMP info:

Name: ntcDevsMod01SyRWCommunity

Type: OBJECT-TYPE

OID: 1.3.6.1.4.1.5835.3.1.1.1.71

5.3 Trap IP address 1 and 2

Entries for the address of the management station where TRAPs need to be send to.

RMCP info:

SNMP trap IP address - SyTrapIPAddr

Description: SNMP trap IP address.

Rmcp header: TIP (get and set)

Example:

Get	TIP?[1]	//get trap IP address 1
Get Reply	TIP?[1]10.0.0.1	//trap IP address is 10.0.0.1

SNMP info:

Name: ntcDevsMod01SyTrapIPAddr

Type: OBJECT-TYPE

OID: 1.3.6.1.4.1.5835.3.1.1.1.69

5.4 Trap community 1 and 2

The SNMP trap community 1 and 2 related to the above mentioned trap IP address 1 and 2.

RMCP info:

Trap community - SyTrapCommunity

Description: SNMP trap IP address.

Rmcp header: TCO (get and set)

Example:

Get	TCO?[2]	//get trap community 2
Get Reply	TCO?[2]public	//trap community is public

SNMP info:

Name: ntcDevsMod01SyTrapCommunity

Type: OBJECT-TYPE

OID: 1.3.6.1.4.1.5835.3.1.1000.1.5

5.5 Version of SNMP daemon

Specifies the version of the SNMP daemon.

RMCP info:

SNMP demon version - SySnmpVer

Description: SNMP demon version and release date.

Rmcp header: SDv (get only)

Example:

Get	SDv?	//get SNMP demon version & release date
Get reply	SDv?v1.01 Nov 10 2005 10:30:24	//version v1.01 date Nov 10

SNMP info:

Name: ntcDevsMod01SySnmpVer

Type: OBJECT-TYPE

OID: 1.3.6.1.4.1.5835.3.1.1.1.68