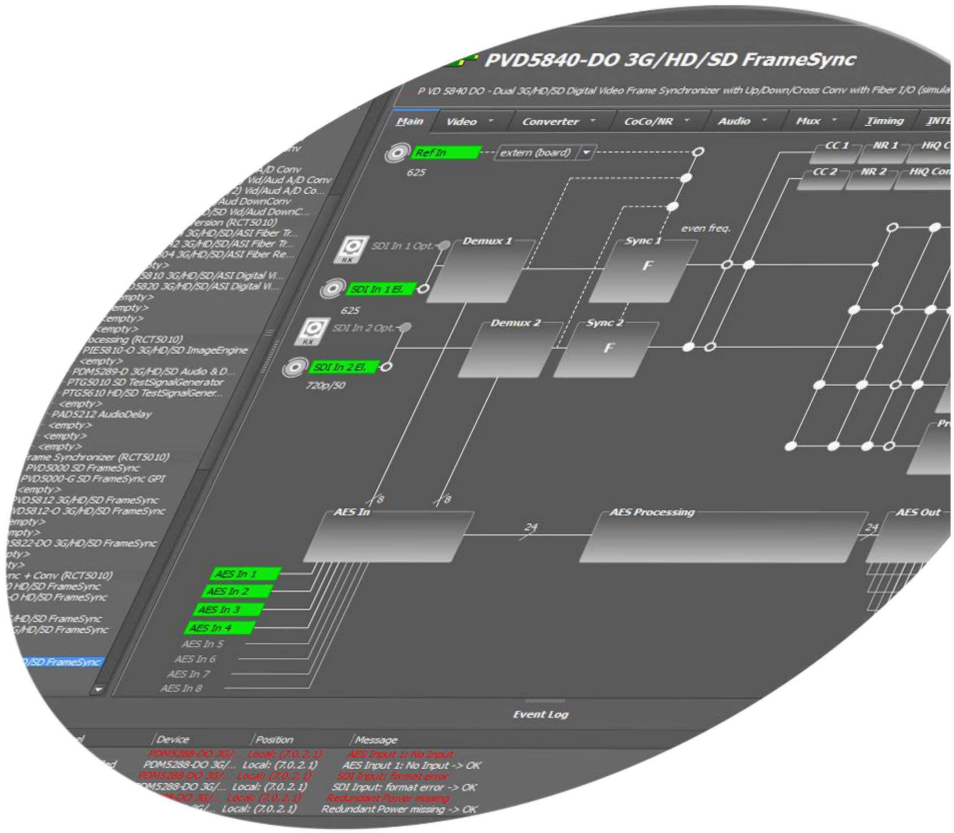
APPolo | Control™

RemoteControl SNMP

User Guide

Revision: 1.1
Last Updated: June 2014
Support Contact: support@lynx-technik.com



Contents

Overview

This document provides an overview and introduction to the SNMP capabilities of the LYNX APPolo Control System. More general information on SNMP can be found by the links at the end of this document.

General Info on SNMP

SNMP (Simple Network Management Protocol) is a standardized protocol (IETF RFC1157) that has been developed for the supervision and management of IP network equipment. Three major versions of SNMP have been defined over the years. The capabilities of SNMPv1 have been extended by SNMPv2. While all communication over the network is basically open (and can potentially be monitored by 3rd parties), SNMPv3 adds some possibilities for secured login and transmission. SNMPv3 does, however, not provide any significant functional additions. See section "Network Security" below and [1].

In an SNMP infrastructure, a "Master" talks to several "Agents" (Clients) over the IP network. A static interface document describes all the capabilities that an Agent provides to the Master. This interface document is called a MIB (Management Information Base). A MIB is a structured collection of information in the form of a

tree. Strictly speaking, there is only one MIB on the world, where many common types of information are pre-defined. Every manufacturer can register their own node in that tree, and define the structure behind that node on their own behalf. Accordingly, the LYNX part of the global MIB starts at 1.3.6.1.4.1.14755. The MIB is structured as a tree and contains multiple branches and leafs. Each node (branch or leaf) can be identified by a specific OID (Object Identifier). A fully-qualified OID is expressed as a chain of individual numbers (representing the nodes), connected by dots. And since each node does not only have a numerical but also a textual name, each OID can be expressed in any mixture of numerical and/or textual form. So, the following OIDs are absolutely identical:

.1.3.6.1.4.1.14755
.iso.org.dod.internet.private.enterprise.lynx-technik
.iso.3.6.1.private.1.lynx-technik

More general information about SNMP and MIB structures can be found in [2].

Traps and Control

The functionality of SNMP is divided into two parts:

(1) The SNMP Agent can send spontaneous messages to the Master, to announce any unexpected change. These spontaneous alarm messages are called „SNMP-Traps".

(2) The Agent can offer the ability for the Master to actively ask for the current status of a certain value (read-only), or even to modify such values (read-write). This General Control capability is often referred to as „SNMP Get/Set".

SNMP Support in the LYNX APPolo Control System

The LYNX APPolo Control System fully supports SNMPv2. Any LYNX MasterController (RCT5031 or RCT5023_SERVER) can work as an SNMPv2 Agent (all you have to do is to enable the OC_RSL_CTRL Option in that MasterController). Once enabled, the SNMP Agent supports the regular SNMPv2 command-set.

The SNMP community strings are set to the standard values "public" (for reading) and "private" (for writing). These can be adapted by modifying the Server's configuration values SNMP_COMMUNITY_READ and SNMP_COMMUNITY_WRITE.

LYNX MIBs

The current set of LYNX MIB files is available for download from the internet [3], either as a combined ZIP package (all MIB files) or as individual files from the "SNMP" sub-folder. These files are organized as follows:

- LYNX-SMI.mib General definitions. Entry point into LYNX MIB tree
- LYNX-TYPES.mib Various type definitions used through other MIB files
- LYNX-TRAPS.mib Definition of the general TRAP-type, used for sending alarms from individual LYNX CardModuls (see below)

- PRODUCT_CODE_swXXX.mib
  For every individual LYNX Product (CardModule), one MIB file is provided. The file name follows this pattern: <PRODUCT> is the regular product name, <CODE> is the technical four-digit product code, and <XXX> is the tree-digit firmware version number.
  As an example, the MIB-file PVD5822-D_07ec_sw567.mib contains the complete SNMP control interface definition of the "PVD5822 dual SDI Framesync" (code 07EC) for firmware version 567 (see below for details).

LYNX SNMP Traps

Every LYNX Processing CardModule provides an individual set of Events. Such Events will be set to ACTIVE state by the CardModule to signalize an unusual state (such as e.g. "SDI input missing" or similar). The individual set of Events per product can be seen in the LYNX APPolo GUI on the "Events" tab per product.

Whenever an Event of an individual CardModule changes its state (passive->active or active->passive), an appropriate entry is added to the LYNX MasterController's Logfile. Additional notification options can be controlled from the individual CardModules "Events" Tab in the APPolo GUI (see figure 1):

- an optional message can displayed in the APPolo GUI Event Log
- an optional SNMPv2 Trap can be sent to the network

The SNMP trap will be generated and sent from the LYNX

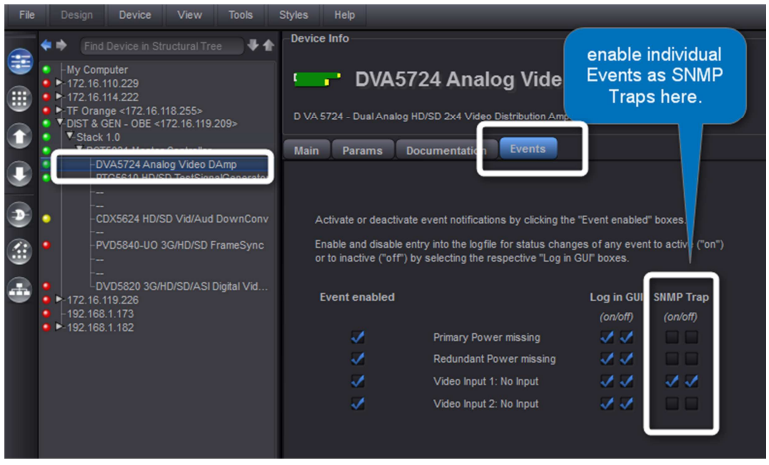


figure 1: SNMP Traps are enabled per individual CardModule

MasterController (RCT5031 or RCT5023_SERVER) to the host that has been specified in the Server's configuration variable SNMP_TRAP_TARGETHOST (this can be a list of multiple IP addresses, separated by a colon ':')

The LYNX MIB defines exactly one type of SNMP Trap. All the details about the specific processing device which has generated the Event and about the individual Event (what type of signal has actually failed?) are contained inside this generic Trap and need to be collected from there.

Example: Receiving an SNMP Trap

The following steps show how a Trap can be received from a real LYNX Device. This makes use of the freely available set of tools from the Net-SNMP project [4].

(1) Enable the Option OC_RSL_CTRL in the MasterController that hosts the CardModule in question.

(2) Use the LYNX APPolo GUI to navigate to the CardModule, go to the Events-tab and enable the SNMP-Traps for any event (for example: "Video Input 1: No Input") at the DVA5724 as shown in figure 1.

(3) Set the configuration variable SNMP_TRAP_TARGETHOST of the LYNX Master-Controller to the IP-Address of the system that runs the snmptrapd-tool (next step). See figure 2.

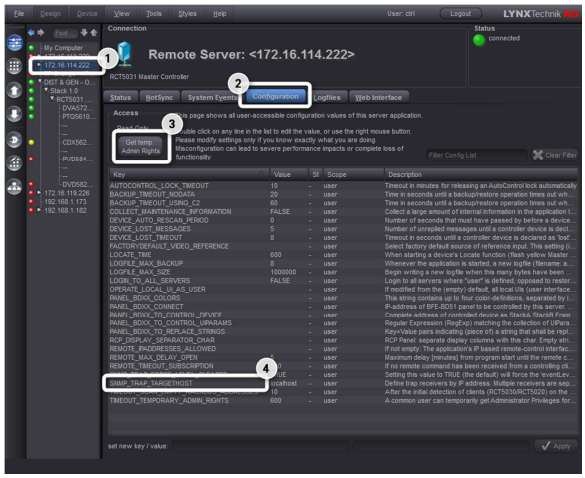


figure 2: set SNMP_TRAP_TARGETHOST

(4) On the target-system (as specified in the previous step), run the command-line tool snmptrapd (from the Net-SNMP tools) to receive and display incoming traps. *(Please note that this program opens UDP/IP port 162, which may require special administration privileges)*

```
% snmptrapd -f -Le -M +[path_to_directory_with_all_LYNX_MIB_files] -m all
NET-SNMP version 5.3.0.1
```

(5) Trigger the Event in question on the CardModule (here: remove video input 1 from the DVA5724). This will make the LYNX system generate the Event and the appropriate Trap. The Trap will be sent from the LYNX Controller over the network to the configured targethost. There it will be

received by the snmptrapd program. This program will generate the commandline output as shown here:

```
2010-12-17 09:23:22 172.16.114.222 [UDP: [172.16.114.222]:57843]:
DISMAN-EVENT-MIB::sysUpTimeInstance       = Timeticks: (5588422) 15:31:24.22
SNMPv2-MIB::snmpTrapOID.0                 = OID: LYNX-TRAPS-MIB::deviceEvent
LYNX-TYPES-MIB::dpSerialPort              = INTEGER: 1
LYNX-TYPES-MIB::dpStack                   = INTEGER: 0
LYNX-TYPES-MIB::dpFrame                   = INTEGER: 0
LYNX-TYPES-MIB::dpSlot                    = INTEGER: 1
LYNX-TYPES-MIB::dpIpAddress               = Hex-STRING: AC 10 77 D1
LYNX-TYPES-MIB::devicePositionAsciiString = STRING: "172.16.119.209:1.0.0.1"
LYNX-TYPES-MIB::eventClass                = INTEGER: 2
LYNX-TYPES-MIB::eventLevel                = INTEGER: error(2)
LYNX-TYPES-MIB::eventID                   = INTEGER: 3
LYNX-TYPES-MIB::eventON                   = INTEGER: on(1)
LYNX-TYPES-MIB::eventAsciiMsg             = STRING: "Video Input 1: No Input"
LYNX-TYPES-MIB::eventAsciiExpl            = ""
LYNX-TYPES-MIB::deviceName                = STRING: "DVA5724 Analog Video DAmp"
LYNX-TYPES-MIB::deviceTypeCode            = INTEGER: 1488
```

NOTE: In this example, the command line program snmptrapd has been configured to deliver all details of the Trap as a text-output. Alternatively, that same tool could be configured to trigger many different types of actions, e.g. send emails or trigger other programs to execute any complex operation.

LYNX SNMP Control (Get/Set)

The LYNX SNMP interface allows to control (Get/Set) all parameters of all CardModules in a given system. The exact list of controllable parameters is, of course, documented in the MIB files. But to get an overview, it is much easier to look at the "Main Control" tool in the LYNX APPolo GUI, go to the device-specific page and open the "Params"-Tab. All the parameters that are shown here are available on the SNMP Get/Set interface from the LYNX MasterController.

Product specific MIB Structure

The LYNX MIB tree provides a dedicated branch for every single LYNX product type (CardModule). Each such product specific branch is then subdivided into one branch per released firmware for the product. As a consequence, when you update a particular CardModule from one firmware to another, you will have to adapt your numerical OIDs to reflect this change (i.e. exchange the old numerical firmware version by the new numerical firmware version).

NOTE: The different firmware-specific sub-branches of a given product are very similar to each other (because newer firmware versions might introduce new features, but they will never deprecate older features). But the numerical OIDs are different.

Internal addressing of CardModules

When it comes to addressing a particular OID, one structural speciality has to be considered. While the LYNX MasterController is the SNMP Agent and has its own IP address, the individual CardModules themselves do not have individual IP addresses. Instead, the CardModules are "hidden" behind the one IP Address of the LYNX MasterController (The MasterController serves as a proxy for the individual CardModules). This type of structure requires a special adaption of the SNMP addressing scheme. In this case, it is not enough to declare the specific properties of a known device type (e.g. a SVD5812 CardModule) as a set of fixed OIDs. Because there can be any number of processing CardModules in a given LYNX system. And all of them are (potentially) of the same type (e.g. SVD5812), thus all of them have the same properties (variables, OIDs). But they obviously all have different current values for each such parameter – because they all are individual instances of the same abstract product type.

figure 3: identify LYNX internal address

This issue of variable internal addressing is solved by LYNX in a common way, as explained in the following paragraphs. The pattern used here is a common approach to this type of problem and has been adopted by other vendors also.

The basic idea is that the numerical OIDs (as documented in the MIB) are extended by the numerical position-information that is assigned by the LYNX System infrastructure. As a simple example:

- The OID of the parameter "Reclock" of the SVD5812 product is declared in the appropriate MIB file as .1.3.6.1.4.1.14755.2.2256.516.1.1.20
- We are assuming, that an individual SVD5812 CardModule is installed in a LYNX system with the MasterController IP-adress of 192.168.1.182 at the internal position **6.16.0.4**
- So the "Reclock" parameter of this particular SVD5812 at this particular address will be available at the OID .1.3.6.1.4.1.14755.2.2256.516.1.1.20.**6.16.0.4**

The current internal position information of any LYNX CardModule (as used throughout the LYNX system) can easily be found in the APPolo GUI, see figure 3.

Note: The same example as above is executed in detail in the next section.

Example: Verification of SNMP Get/Set

The following example will show how to control (Get/Set) the "Reclock" parameter of a "SVD5812 ChangeOverSwitch" which is installed in a system at position 6.16.0.4

The MasterController at IP address 192.168.1.182 has the option OC_RSL_CTRL enabled.

(1) Read the current setting of the "Reclock" parameter, using the command-line tool snmpget (from the NetSNMP tools [4])

```
% snmpget -v2c -c public -M ./mibs -m all 192.168.1.182 .1.3.6.1.4.1.14755.2.2256.516.1.1.20.6.16.0.4
.1.3.6.1.4.1.14755.2.2256.516.1.1.20.6.16.0.4 = INTEGER: 0
```

The reply prints a current value of "0" which means that this Reclock-parameter has the current value "OFF"

(2) Set the current setting of the "Reclock" parameter to ON, using the command-line tool snmpset (from the NetSNMP tools [4])

```
% snmpset -v2c -c private -M ./mibs -m all 192.168.1.182 .1.3.6.1.4.1.14755.2.2256.516.1.1.20.6.16.0.4 i 1
.1.3.6.1.4.1.14755.2.2256.516.1.1.20.6.16.0.4 = INTEGER: 1
```

This command sets the specified parameter of type "integer" ("I") to the current value of "1". An immediate get-command (same as above) will verify the result:

```
% snmpget -v2c -c public -M ./mibs -m all 192.168.1.182 .1.3.6.1.4.1.14755.2.2256.516.1.1.20.6.16.0.4
.1.3.6.1.4.1.14755.2.2256.516.1.1.20.6.16.0.4 = INTEGER: 1
```

The reply prints a current value of "1" which means that this Reclock-parameter has the current value "ON"

If you had a LYNX APPolo GUI connected to this SVD5812 while executing the above commands, you could monitor the change of state of this parameter at runtime.

The same model can now be used to Get / Set any parameter of any CardModule.

Network Security

The LYNX MasterControllers support SNMPv2, and thus provides only limited security against intentional misuse and intrusion. The additional security level provided by SNMPv3 might be desirable if a LYNX Controller would be operated in an in-secure network environment and thus would have to be protected against attempts of malicious intrusion.

The general LYNX networking concept assumes, however, that this is not the case. Instead, it assumes that the appropriate level of security is already provided by the surrounding network infrastructure (e.g. by firewalls, physical separation or other appropriate means).

Accordingly, the LYNX system provides protection against unintentional mal-operation only, e.g. by authentication through username and password, respectively the SNMP community strings (see "General Info on SNMP").

Further Reading

[1] Overview and differences SNMPv1, SNMPv2, SNMPv3:
http://tools.ietf.org/html/rfc1157
http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
http://www.webnms.com/snmputilities/help/quick_tour/snmp_and_mib/snmpmib_snmpv3.html
http://www.networkmanagementsoftware.com/snmp-tutorial

[2] SNMP terminology, components, MIB
http://www.webnms.com/cagent/help/technology_used/c_snmp_overview.html#mib
https://blogs.oracle.com/jmxetc/entry/simple_is_not_easy
http://publib.boulder.ibm.com/infocenter/aix/v6r1/index.jsp?topic=%2Fcom.ibm.aix.progc
omm%2Fdoc%2Fprogcomc%2Fmib.htm

[3] LYNX MIB files
http://www.lynx-technik.com/en/support/download-area/appolo/

[4] The Net-SNMP project is a free collection of software tools that cover all SNMP functionalities
http://www.net-snmp.org/
http://www.net-snmp.org/docs/man/snmptrapd.html
http://www.net-snmp.org/docs/man/snmptrapd.conf.html
http://www.net-snmp.org/tutorial/tutorial-5/demon/snmpd.html

Please visit http://appolo.lynx-technik.com
for more information on the LYNX APPolo Control System.

Document	*LYNX_APPolo_UserGuide_RemoteControl_SNMP.docx*
Last Printed:	*28.05.2014 13:03*