LOYTEC Device

Device Operation for LOYTEC Products

User Manual

LOYTEC electronics GmbH



Contact

LOYTEC electronics GmbH
Blumengasse 35
1170 Vienna
AUSTRIA/EUROPE
support@loytec.com
http://www.loytec.com

Version 8.2

Document № 88086512

LOYTEC MAKES AND YOU RECEIVE NO WARRANTIES OR CONDITIONS, EXPRESS, IMPLIED, STATUTORY OR IN ANY COMMUNICATION WITH YOU, AND
LOYTEC SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THIS PRODUCT IS NOT DESIGNED OR INTENDED FOR USE IN EQUIPMENT INTENDED FOR SURGICAL IMPLANT INTO THE BODY OR OTHER APPLICATIONS INTENDED TO SUPPORT OR SUSTAIN LIFE, FOR USE IN FLIGHT CONTROL OR ENGINE CONTROL EQUIPMENT WITHIN AN AIRCRAFT, OR FOR ANY OTHER APPLICATION IN WHICH IN THE FAILURE OF SUCH PRODUCT COULD CREATE A SITUATION IN WHICH PERSONAL INJURY OR DEATH MAY OCCUR. LOYTEC MAKES NO REPRESENTATION AND OFFERS NO WARRANTY OF ANY KIND REGARDING OF ANY THIRDPARTY COMPONENTS MENTIONED IN THIS MANUAL.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of LOYTEC.

LC3020™, L-Chip™, L-Core™, L-DALI™, L-GATE™, L-INX™, L-IOB™, LIOB-Connect™, LIOB-FT™, L-IP™, LPA™, L-Proxy™, L-Switch™, L-Term™, L-VIS™, L-WEB™, L-ZIBI™, ORION™ stack and Smart Auto-Connect™ are trademarks of LOYTEC electronics GmbH.

LonTalk®, LONWORKS®, Neuron®, LONMARK®, LonMaker®, *i*.LON®, and LNS® are trademarks of Echelon Corporation registered in the United States and other countries.

Contents

1 Introduction 15
1.1 Overview 15
1.2 CEA-709.1 15
1.3 BACnet 16
1.4 M-Bus 17
1.5 Modbus 17
1.6 KNX 17
1.7 EnOcean 18
1.8 SMI 18
1.9 MP-Bus 18
1.10 L-IOB 18
1.11 LTE and SMS 19
1.12 Scope 19
2 LCD Display 20
2.1 Device Setup 20
2.2 BACnet Settings 21
2.3 WLAN Settings 22
2.4 Local I/O Settings 24
2.4.1 I/O Page 24
2.4.2 Unconfigured Mode 25
2.4.3 Manual / Quick Edit Mode 25
2.4.4 I/O Configuration 25
2.5 LIOB-IP Page 26
2.6 Firmware Upgrade 26
2.7 PIN Code Protection 27
3 Web Interface 28
3.1 Device Information and Account Management 28
3.1.1 Device Setup 28
3.1.2 Device Information 28
3.1.3 Device Login 29
3.2 Device Statistics 30
3.2.1 System Log 30
3.2.2 IP Statistics 30
3.2.3 E-mail 31
3.2.4 CEA-852 Statistics 32
3.2.5 Enhanced Communications Test 32

3.2.6 Global Connections Statistics ... 33
3.2.7 CEA-709 Statistics ... 34
3.2.8 OPC XML-DA Server Statistics Page ... 34
3.2.9 BACnet MS/TP Statistics ... 35
3.2.10 BACnet Bindings Statistics ... 38
3.2.11 BACnet/SC Statistics ... 38
3.2.12 BACnet FDT Statistics ... 39
3.2.13 Scheduler Statistics Page ... 39
3.2.14 Packet Capture ... 39
3.2.15 Mobile Network ... 39
3.3 Data Management ... 40
3.3.1 Data Points ... 40
3.3.2 Priority Array ... 42
3.3.3 Manual Override ... 43
3.3.4 Trend ... 44
3.3.5 Scheduler ... 46
3.3.6 Calendar ... 48
3.3.7 iCalendar Scheduler ... 49
3.3.8 Alarm ... 50
3.3.9 Alarm Log Page ... 51
3.4 Commission ... 52
3.4.1 BACnet ... 52
3.5 Device Configuration ... 53
3.5.1 System Configuration ... 53
3.5.2 Port Configuration ... 55
3.5.3 IP Configuration ... 55
3.5.4 Using Multiple IP Ports ... 57
3.5.5 802.1X Port Authentication ... 57
3.5.6 IP Host Configuration ... 58
3.5.7 Dynamic DNS Configuration ... 59
3.5.8 WLAN Configuration ... 60
3.5.9 Mesh Configuration ... 62
3.5.10 VNC Configuration ... 67
3.5.11 CEA-709 Configuration ... 67
3.5.12 CEA-852 Device Configuration ... 68
3.5.13 Global Connections Configuration ... 69
3.5.14 CEA-709 Router Configuration ... 70
3.5.15 CEA-852 Server Configuration ... 70
3.5.16 CEA-852 Channel List ... 72
3.5.17 BACnet Configuration ... 73

3.5.18 BACnet/IP Configuration 74
3.5.19 BACnet/IPv6 Configuration 75
3.5.20 BACnet/SC Configuration 75
3.5.21 MS/TP Configuration 76
3.5.22 BACnet Recipients 77
3.5.23 BACnet Time Master 77
3.5.24 BACnet Restart Notifications 78
3.5.25 BACnet BDT (Broadcast Distribution Table) 78
3.5.26 BACnet ACL (Access Control List) 79
3.5.27 BACnet Slave Proxy 80
3.5.28 E-mail Configuration 80
3.5.29 SSH Server Configuration 81
3.5.30 SNMP 81
3.5.31 VPN Configuration 82
3.5.32 LTE Configuration 84
3.5.33 SMS Gateway 85
3.5.34 License 85
3.6 Programming 86
3.6.1 L-STUDIO Configuration 86
3.6.2 L-LOGICAD Configuration 87
3.6.3 Scripting 88
3.6.4 Node-RED™ Editor 88
3.7 Security 90
3.7.1 Change Passwords 90
3.7.2 Certificate Management 91
3.7.3 User Management 94
3.8 L-WEB 95
3.8.1 Installation 95
3.8.2 LWEB-802 Config 96
3.8.3 Access Control List 97
3.9 L-IOB Host and Local I/Os 98
3.9.1 LIOB-IP Bus 98
3.9.2 L-IOB Installation Page 98
3.9.3 L-IOB Scan and Configuration Run 100
3.9.4 L-IOB Device Information and Statistics 101
3.9.5 L-IOB Overview Page 102
3.9.6 L-IOB I/O Test Page 104
3.10 Documentation 105
3.11 Maintenance 105
3.11.1 Backup and Restore 105

3.11.2 Firmware 106
3.11.3 Documentation 107
3.11.4 Rebooting and Clearing Project Data 108
3.11.5 Safe Reboot 108
3.12 Contact, Logout 108
4 The CEA-709 Router 109
4.1 CEA-709 Router 109
4.1.1 Configured Router Mode 110
4.1.2 Smart Switch Mode 110
4.1.3 Store-and-Forward Repeater 111
4.1.4 Smart Switch Mode with No Subnet Broadcast Flooding 111
4.2 CEA-852 Device of the Router 111
4.3 Configuration Server for Managing the IP-852 Channel 112
4.3.1 Overview 112
4.3.2 Configuration Server Contacts IP-852 Device 113
4.3.3 IP-852 Device Contacts Configuration Server 113
4.3.4 Using the Built-In Configuration Server 113
4.4 Firewall and NAT Router Configuration 114
4.4.1 Automatic NAT Configuration 114
4.4.2 Multiple IP-852 Devices behind a NAT: Extended NAT Mode 115
4.4.3 Multiple IP-852 devices behind a NAT: Classic Method 117
4.5 Multi-Cast Configuration 118
4.6 Remote LPA Operation 119
4.7 Internet Timing Aspects 119
4.7.1 Channel Timeout 120
4.7.2 Channel Delay 120
4.7.3 Escrowing Timer (Packet Reorder Timer) 120
4.7.4 SNTP Time Server 121
4.8 Advanced Topics 121
4.8.1 Aggregation 121
4.8.2 MD5 Authentication 121
4.8.3 Dynamic NAT Addresses 121
5 Remote Network Interface 123
5.1 RNI Function 123
5.2 Remote LPA Operation 123
6 OPC Server 124
6.1 XML-DA OPC Server 124
6.1.1 Access Methods 124
6.1.2 Data Points 125

6.1.3 AST Objects 128
6.1.4 OPC Groups 130
6.2 OPC UA Server 131
6.2.1 Introduction 131
6.2.2 OPC UA and Security 131
6.2.3 OPC UA Trusted Clients 133
6.2.4 OPC UA Client Setup 134
6.2.5 Connect with an OPC UA Client 135
6.2.6 OPC UA Address Space 135
6.2.7 AST Objects 137
6.2.8 Subscriptions and Monitored Items 137
6.2.9 OPC UA Statistics 138
6.2.10 Error Codes and Solutions 140
6.3 Using Custom Web Pages 141
7 M-Bus 143
7.1 Introduction 143
7.2 Hardware Installation 143
7.2.1 Console Connector 143
7.2.2 Extension Port 144
7.3 M-Bus Network 145
7.4 Web Interface 146
7.4.1 Configuration 146
7.4.2 Data Points 146
7.4.3 Commission 146
7.4.4 Statistics 147
7.4.5 M-Bus Protocol Analyzer 149
8 Modbus 150
8.1 Introduction 150
8.2 Modbus Network 150
8.3 Web Interface 151
8.3.1 Port Configuration 151
8.3.2 Data Points 152
8.3.3 Commission 152
8.3.4 Statistics 153
8.3.5 Modbus Protocol Analyzer 154
8.3.6 L-STAT Device Management 155
9 KNX 157
9.1 Introduction 157
9.2 Hardware Installation 157

9.2.1 LKNX-300 Installation ... 157
9.3 KNX Network ... 158
9.4 Web Interface ... 158
9.4.1 Configuration ... 158
9.4.2 Data Points ... 159
9.4.3 KNX Protocol Analyzer ... 159
10 SMI ... 161
10.1 Introduction ... 161
10.2 Hardware Installation ... 161
10.2.1 LSMI-800 ... 161
10.2.2 LSMI-804 ... 162
10.3 Web Interface ... 163
10.3.1 Configuration ... 163
10.3.2 Data Points ... 163
10.3.3 Commissioning ... 163
10.3.4 Calibration ... 165
10.3.5 Statistics ... 166
10.3.6 Protocol Analyzer ... 167
11 EnOcean ... 168
11.1 Introduction ... 168
11.2 Hardware Installation ... 168
11.3 Web Interface ... 169
11.3.1 Configuration ... 169
11.3.2 Data Points ... 169
11.3.3 Commissioning ... 169
11.3.4 Configure a Transmission ID ... 170
11.3.5 Statistics ... 171
11.3.6 Protocol analyzer ... 171
12 MP-Bus ... 173
12.1 Introduction ... 173
12.2 Hardware Installation ... 173
12.2.1 Built-In MP-Bus Port ... 173
12.2.2 LMPBUS-804 ... 174
12.3 Web Interface ... 175
12.3.1 Configuration ... 175
12.3.2 Data Points ... 176
12.3.3 Auto-Commission in PP Mode ... 176
12.3.4 Commissioning in MP Mode ... 176
12.3.5 Statistics ... 178

12.3.6 Protocol Analyzer 179
13 OPC Client 180
13.1 Introduction 180
13.2 Web UI 180
13.2.1 Data Points 180
13.2.2 Commissioning 180
13.2.3 Statistics 181
14 ekey 183
14.1 Introduction 183
14.1.1 Supported ekey models 184
14.2 Web UI 184
14.2.1 Data Points 184
14.2.2 Commissioning 184
15 Bluetooth 186
15.1 Introduction 186
15.1.1 Bluetooth Mesh Basics 186
15.1.2 Bluetooth Mesh Network Limitations 188
15.1.3 Bluetooth on LOYTEC controller 188
15.2 Bluetooth Mesh Device Types 190
15.2.1 Templates for Bluetooth Generic Devices 190
15.2.2 Datapoint Description 192
15.2.3 LOYTEC Controller with Bluetooth interface 194
15.2.4 LOYTEC bluetooth mesh system overview 195
15.3 Web UI 195
15.3.1 Data Points 195
15.3.2 Commissioning 195
15.3.3 Groups 202
15.3.4 Scenes 202
15.3.5 Statistics 202
15.3.6 Protocol Analyzer 203
15.4 Troubleshooting 205
15.4.1 Device Recovery 205
16 DALI 206
16.1 Introduction 206
16.1.1 DALI Wiring 206
16.1.2 DALI Interface and DALI Bus Power Consumption 207
16.1.3 Multi-Master Operation 208
16.2 DALI Device Types 209
16.3 LOYTEC DALI Interface 211

16.3.1 LOYTEC Controller Types and Features ... 211
16.3.2 DALI Channel Limitations ... 212
16.3.3 Device Class – Lamps ... 213
16.3.4 Device Class – Buttons ... 216
16.3.5 Device Class – Sensors ... 217
16.3.6 Proprietary DALI sensors and buttons ... 221
16.3.7 Power Failure Recovery ... 222
16.3.8 DALI Channel Bridging ... 222
16.3.9 Reducing ballast standby energy consumption ... 222
16.4 Web UI ... 225
16.4.1 DALI Groups ... 225
16.4.2 DALI Installation ... 226
16.4.3 DALI Scene ... 237
16.4.4 Statistics ... 240
16.4.5 Protocol Analyzer ... 241
16.4.6 Emergency Logs ... 242
16.5 LCD UI ... 243
16.6 Troubleshooting ... 244
16.7 DALI Error Codes ... 245
17 Operating Interfaces ... 246
17.1 Common Interface ... 246
17.1.1 Schedule and Calendar XML Files ... 246
17.1.2 Trend Log CSV File ... 246
17.1.3 Alarm Log CSV File ... 247
17.1.4 DALI Emergency Light Test Log CSV File ... 248
17.1.5 DALI Status CSV ... 248
17.2 CEA-709 Interface ... 251
17.2.1 Node Object ... 251
17.2.2 Real-Time Keeper Object ... 252
17.2.3 Channel Monitor Object ... 252
17.2.4 Calendar Object ... 254
17.2.5 Scheduler Object ... 254
17.2.6 Clients Object ... 254
17.2.7 Gateway/PLC Objects ... 254
17.3 BACnet Interface ... 254
17.3.1 Device Object ... 254
17.3.2 Device Name and ID ... 256
17.3.3 Device Information ... 256
17.3.4 Object Database ... 257
17.3.5 Protocol Parameters ... 257

17.3.6 Diagnostics 257
17.3.7 Date & Time 258
17.3.8 Time Master 258
17.3.9 Backup & Restore 260
17.3.10 Slave Proxy 260
17.3.11 Client Mapping CSV File 261
17.3.12 EDE Export of BACnet Objects 261
17.4 SNMP Interface 262
17.4.1 SNMP Features 262
17.4.2 Configuration 262
17.4.3 Exposing Data Points to SNMP 264
17.4.4 Alarming 264
17.4.5 SNMP Security 265
18 Network Media 266
18.1 FT 266
18.2 M-Bus 266
18.3 Modbus RS-485 267
18.4 MS/TP 267
18.5 Physical Connection of Inputs 268
18.5.1 Connection of Switches 268
18.5.2 Connection of S0 Pulse Devices (Meters) 269
18.5.3 Connection of Voltage Sources to Universal Inputs 269
18.5.4 Connection of 4-20mA Transmitters to Universal Inputs 270
18.5.5 Connection of Resistive Sensors 271
18.5.6 Connection of STId Card Readers 271
18.6 Physical Connection of Outputs 271
18.6.1 6A Relays with one External Fuse 271
18.6.2 6A Relays on LIOB-xx2 using Separate Fuses 272
18.6.3 16A and 6A Relays on LIOB-xx3 272
18.6.4 External Relays and Inductive Loads 273
18.6.5 Triacs 273
18.6.6 Analog Outputs 274
18.7 Redundant Ethernet 274
18.7.1 Ethernet Cabling Options 274
18.7.2 Upstream Options 276
18.7.3 Preconditions 276
18.7.4 Switch Settings 277
18.7.5 Testing 277
18.7.6 Example switch configuration 278
18.8 WLAN 278

18.8.1 Introduction 278
18.8.2 802.11s Mesh Networking 279
18.8.3 Hardware Installation 280
19 Firmware Update 281
19.1 Firmware Update via the Configurator 281
19.2 Firmware Update via the Web Interface 283
19.3 Firmware Update via USB Memory Stick 283
19.4 Firmware Update of L-IOB I/O Modules 283
20 Troubleshooting 286
20.1 Technical Support 286
20.2 Packet Capture 286
20.2.1 Configure Remote Packet Capture 286
20.2.2 Enable Local Capture 287
20.2.3 Run Wireshark Remote Capture 288
21 References 292
22 Revision History 293

Abbreviations

100Base-T	100 Mbps Ethernet network with RJ-45 plug
Aggregation	Collection of several CEA-709 packets into a single CEA-852 packet
AST	Alarming, Scheduling, Trending
BACnet	Building Automation and Control Network
BBMD	BACnet Broadcast Management Device
BDT	Broadcast Distribution Table
BOOTP	Bootstrap Protocol, RFC 1497
CA	Certification Authority
CEA-709	Protocol standard for LONWORKS networks
CEA-852	Protocol standard for tunneling CEA-709 packets over IP channels
CN	Control Network
COV	change-of-value
CR	Channel Routing
CS	Configuration Server that manages CEA-852 IP devices
DA	Data Access (Web service)
DALI	Digital Addressable Lighting Interface, see IEC 62386
DHCP	Dynamic Host Configuration Protocol, RFC 2131, RFC 2132
DIF, DIFE	Data Information Field, Data Information Field Extension
DL	Data Logger (Web service)
DNS	Domain Name Server, RFC 1034
DST	Daylight Saving Time
EEP	EnOcean Equipment Profile
GMT	Greenwich Mean Time
IP	Internet Protocol
IP-852	logical IP channel that tunnels CEA-709 packets according CEA-852
LAN	Local Area Network
LSD Tool	LOYTEC System Diagnostics Tool
MAC	Media Access Control
MD5	Message Digest 5, a secure hash function, see Internet RFC 1321
M-Bus	Meter-Bus (Standards EN 13757-2, EN 13757-3)
MIB	Management Information Base
MS/TP	Master/Slave Token Passing (this is a BACnet data link layer)
NAT	Network Address Translation, see Internet RFC 1631
NV	Network Variable
OPC	Open Process Control
OPC UA	OPC Unified Architecture
PEM	Privacy Enhanced Mail
PLC	Programmable Logic Controller
RNI	Remote Network Interface
RSTP	Rapid Spanning Tree Protocol (Standard IEEE 802.1D-2004)
RTT	Round-Trip Time
RTU	Remote Terminal Unit

SCPT ..... Standard Configuration Property Type
SL ..... Send List
SMI..... Standard Motor Interface
SMTP ..... Simple Mail Transfer Protocol
SNMP ..... Simple Network Management Protocol
SNTP ..... Simple Network Time Protocol
SSH..... Secure Shell
SSL ..... Secure Socket Layer
STP ..... Spanning Tree Protocol (Standard IEEE 802.1D)
TLS..... Transport Layer Security
UCPT..... User-defined Configuration Property Type
UI..... User Interface
UNVT..... User-defined Network Variable Type
UTC..... Universal Time Coordinated
VIF, VIFE..... Value Information Field, Value Information Field Extension
WLAN..... Wireless LAN
XML ..... eXtensible Markup Language

1 Introduction

1.1 Overview

The LOYTEC product family includes high performance, reliable and secure network infrastructure components, embedded automation servers, universal agteways, touch panels, I/O modules, room controllers, and lighting controllers. The different device models contain a number of components and network technologies, such as BACnet, CEA-709, KNX, Modbus, M-Bus, MP-Bus, DALI, SMI, EnOcean.

This User Manual describes common tasks on the built-in Web server, which allows convenient device configuration through a standard Web browser. The Web interface also provides statistics information for system installation and network troubleshooting. Some devices also have an LCD display, which provides a quick way to configure basic settings of the device via a jog dial.

An embedded OPC server exposes a defined set of data points as OPC tags. It implements the OPC XML-DA standard OPC XML-DA 1.01, which lets OPC clients access the data points via Web services. For secure OPC communication some LOYTEC device models add an OPC UA server. Which native data points are exposed to OPC can also be configured by the configuration software.

LOYTEC devices permanently collect statistical information from the attached network channels (OPC connections, FT traffic, MS/TP token passing, Ethernet traffic, etc.). Using this data, the device is able to detect problems on these channels (overload, lost tokens, connection problems, etc.). An intuitive user interface allows fast and easy network troubleshooting without any additional analysis tools or deep system knowledge. For troubleshooting Ethernet protocols a local and remote Wireshark packet capture can be configured (see Section 20.2).

Some LOYTEC device models are also equipped with a 2-port Ethernet Switch/Hub. In switched mode an Ethernet daisy chain can be built, which reduces cabling effort. The two Ethernet connectors can also be configured to work as two isolated IP interfaces. This can be used to safely connect a local building network while keeping it isolated from WAN access, that exposes some aspects using secure services (see Section 3.5.4). By using the external L-WLAN adapter, the device also provides a WLAN interface, which can link to an existing access point, set up its own access point or work in a wireless mesh network (see Section 3.5.8).

1.2 CEA-709.1

LOYTEC device models that have CEA-709 are equipped with an FT port (CEA-709) and a 100Base-T Ethernet port (CEA-852). CEA-709 models come with a router option or an RNI option. Device models with the router option contain a CEA-709 router between the FT and

the IP-852 channel, which can be configured like an L-IP. It includes a configuration server (CS) to manage the IP-852 channel. Device models without the router option contain a remote network interface (RNI) instead of the router for remote network access.

A CEA-709 LOYTEC device is fully compliant with ANSI/CEA-709, ANSI/CEA-852-A, EN 14908. The CEA-709 node, that is going to be commissioned in the network, is always connected to the FT port of the device.

A LOYTEC device with the router option possesses a router between the CEA-852 interface (IP-852) and the FT interface. The CEA-852 interface can be used to connect the device to an IP-based high-speed backbone. The router can be used as a standard CEA-709 configured router or it can be used as a self-learning plug&play router based on the high-performance, well-proven routing core from our L-Switch plug&play multi-port router devices ("smart switch mode"). The self-learning router doesn't need a network management tool for configuration but is a true plug&play and easy to use IP infrastructure component. For a detailed description of the CEA-709 router's usage refer to the L-IP User Manual [2].

A LOYTEC device without the router option can be configured to run either on the CEA-852 interface (IP-852 mode) or on the FT interface (FT mode). In the FT mode, the device provides a remote network interface (RNI), which appears like a LOYTEC NIC-IP is intended to be used together with the LOYTEC NIC software [4]. The RNI can be utilized for remote access and configuration as well as trouble-shooting with the remote LPA. Please consult our product literature for the LPA-IP to learn more about this IP-based CEA-709 protocol analyzer.

1.3 BACnet

LOYTEC device models that have BACnet are BTL-certified products that implement the B-BC profile. They are equipped with an MS/TP port and a 100Base-T Ethernet port (BACnet/IP or BACnet/SC). The MS/TP port supports remote Wireshark packet capture for troubleshooting. BACnet device models with the router option also contain a BACnet router between the MS/TP and the BACnet/IP and BACnet/SC ports, which can be configured like an LIP-ME20X. The router models also include a BACnet broadcast management device (BBMD) to manage BACnet/IP internetworks, which span across IP routers. BACnet models without the router can register as a foreign device (FD) with other BBMDs. The device is fully compliant with ANSI/ASHRAE 135-2010 (1.7) and ISO 16484-5.

A BACnet device without the router option can be configured to run either on the BACnet/IP interface or on the BACnet/SC interface or on the MS/TP interface. In BACnet/IP mode, the device can be configured as a foreign device in another BBMD. The BACnet device without the router option may not provide the BBMD functionality itself. The L-GATE can also be configured to be a BBMD.

LOYTEC devices expose BACnet server objects and client mappings to data points of the automation server or the gateway. For client mappings, the BACnet address information is supplied by the configuration software by importing e.g., a CSV file or by performing an online network scan.

Some models also support the LOYTEC Alarming, Scheduling and Trending (AST) features in native BACnet objects. The device provides BACnet scheduler/calendar objects, which can directly schedule BACnet server objects, remote BACnet objects or non-BACnet registers. For alarm conditions the device supports the intrinsic reporting method of BACnet objects. Trend logs can be uploaded from the device via the native BACnet read range.

1.4 M-Bus

In addition to the basic network technologies some models support the M-Bus interface according to the standards EN 13757-2 and EN 13757-3. To get access to the M-Bus network, an external M-Bus interface such as the L-MBUS by LOYTEC must be attached to the device. On devices with a serial port, the M-Bus interface is connected to the serial connector. In this case the user needs to turn M-Bus support on and off via a DIP switch. On devices without a serial port, the L-MBUS interface must be used and is connected to the extension port (EXT).

Through the M-Bus interface the LOYTEC device can be used to scan the attached M-Bus network for devices, pull M-Bus data points into a configuration, connect those data points to other technologies and expose M-Bus data points to the automation server. All device functions can be used directly on M-Bus data points. Especially trending data and polling for data on M-Bus devices has been optimized for automatic meter reading applications.

For debugging purposes a protocol analyzer is included in the firmware and can be operated via the Web-UI and the configuration software. For more information on how to set up the device for using M-Bus, configuring and using M-Bus data points, refer to Chapter 7.

1.5 Modbus

In addition to the basic network technologies some models support the Modbus RTU and the Modbus TCP interface. To get access to the Modbus network, the appropriate interfaces have to be activated either in the Web UI or in the configuration software. Modbus RTU is operated with 8N1. A Modbus port can either be operated as Modbus master or Modbus slave.

Modbus RTU/ASCII on RS-232 requires the LRS232-802 interface. Some LOYTEC device models support this interface on the USB port which provides two RS-232 ports.

On some BACnet L-INX models, the Modbus RTU/ASCII and BACnet MS/TP protocols share the same port. On those models, Modbus RTU can only be used, if BACnet MS/TP is disabled. Please refer to the respective product manual to learn, which device models have this restriction.

Through the Modbus interface the device can be used to data points to other technologies, and expose Modbus data points to OPC tags. All device functions can be used directly on Modbus data points. Especially trending data and polling for data on Modbus devices has been optimized for automatic meter reading applications.

For debugging purposes a protocol analyzer is included in the firmware and can be operated via the Web UI and the configuration software. For more information on how to set up the device for using Modbus, configuring and using Modbus data points, refer to Chapter 8.

1.6 KNX

In addition to the basic network technologies some models can be connected to KNX networks. To get access to a KNX TP1 network, the LKNX-300 interface has to be attached to the device for TP1 networks. All KNX-capable models support KNXnet/IP directly with their Ethernet interface.

The KNX interface allows creating KNX data points which can be used with the device functions, the OPC server and also the PLC on the L-INX models. The device configuration can be imported from an ETS database export.

For more information on how to set up the device for using KNX, configuring and using KNX data points, refer to Chapter 9.

1.7 EnOcean

In addition to the basic network technologies some models can integrate EnOcean wireless devices. To get access to an EnOcean network, the LENO-800 interface has to be attached via one of the USB ports USB 1 or USB 2.

The EnOcean interface is represented in the Configurator as a technology folder. EnOcean devices are created from device templates and provide data points, which can be used with the device functions, the OPC server and also the PLC on the L-INX models.

For debugging purposes a protocol analyzer is included in the firmware and can be operated via the Web UI. For more information on how to set up the device for using EnOcean, configuring and using EnOcean data points, refer to Chapter 11.

1.8 SMI

In addition to the basic network technologies, some models can be connected to SMI networks. To get access to the SMI network, the LSMI-800 interface has to be attached to the EXT port of the device (for one SMI channel), or the LSMI-804 interface to the USB port (for four SMI channels).

The SMI interface is represented in the Configurator as a technology folder. SMI devices are created from device templates and provide data points, which can be used with the AST functions, the OPC server and also the PLC on the L-INX models.

For debugging purposes a protocol analyzer is included in the firmware and can be operated via the Web UI. For more information on how to set up the device for using SMI, configuring and using SMI data points, refer to Chapter 10.

1.9 MP-Bus

In addition to the basic network technologies, some models can be connected to MP-Bus devices through a dedicated MP-Bus port. On other models, the LMPBUS-804 interface can be attached to the USB port (for four MP-Bus channels). Some models support two LMPBUS-804 interfaces, making a total of eight MP-Bus channels. Note, that external USB hubs are not supported.

The MP-Bus interface is represented in the Configurator as a technology folder. MP-Bus devices are created from device templates and provide data points, which can be used with the AST functions, the OPC server and also the PLC on the LIOB-AIR models.

For debugging purposes a protocol analyzer is included in the firmware and can be operated via the Web UI. For more information on how to set up MP-Bus devices and configuring MP-Bus data points, refer to Chapter 12.

1.10 L-IOB

The L-INX automation server models, L-ROC room controller models allow connecting physical I/Os to the device via the L-IOB I/O modules. On some models those modules can be stacked up directly to the device using the LIOB-Connect feature. The connected I/O modules are automatically identified and coupled as data points into the automation server.

Some device models have additional L-IOB connection options, that support easy integration of L-IOB I/O modules over FT cabling using the LIOB-FT feature, or over Ethernet using the LIOB-IP feature.

L-IOB modules are available with digital inputs and outputs, analog inputs and outputs and universal inputs that are configurable. Some models are also available with a differential pressure sensor.

The I/O modules can be parameterized over the configuration software or the Web UI. All parameterization data is stored on the LOYTEC device and can be reloaded to the L-IOB modules when needed. The exchange of modules is detected automatically.

Some device models are also equipped with local I/Os, which are built into the device. Configuration of local I/Os is similar to I/O configuration of LIOB-Connect, FT or IP devices. What specific local I/Os are available is specified in the User Manual of the respective product.

1.11 LTE and SMS

The LTE-800 module provides wireless LTE connectivity to a LOYTEC device and acts as an interface to the Internet. This connectivity can be used by the device itself, for instance to synchronize to NTP or establish a VPN connection to an LWEB-900 server (or customer-based OpenVPN server) for remote access to the device and its data points.

A LOYTEC device can also be configured to provide Internet access of local devices through the LTE module. In this use case the LOYTEC device functions as a NAT router for a handful of local devices, such as L-VIS or LIOB-IP. A LOYTEC device with LTE access will not, however, replace a dedicated LTE router equipment for access to large sites with 10 and more devices.

Especially in combination with an LWEB-900 server, the VPN setup is made as simple as entering a project ID into the LOYTEC device. Using this method, the LOYTEC device will register at the corresponding LWEB-900 project and automatically integrate into the LWEB-900 VPN.

The LTE-800 interface can also be used to transmit SMS, either locally or via a remote LTE-800 connected to another LOYTEC device on the network. SMS are configured like E-Mails in the Configurator software and their transmission are triggered by data points.

1.12 Scope

This document covers common operations on LOYTEC devices with firmware version 8.2. For more information of specific usage refer to the User Manual of the respective product. The data point configuration is covered by the LINX Configurator User Manual [1].

2 LCD Display

2.1 Device Setup

Device models with an LCD display can also be configured to their basic settings through jog dial navigation on the LCD UI. The main page of the LCD UI is shown in Figure 1. It displays the device's IP address, hostname, CPU load, system temperature and supply voltage. On devices that don't have Ethernet link LEDs, the LCD display shows the link status as **Eth1+2** or a respective combination thereof.

For language selection navigate to the language icon 〓 and enter into the menu. Choose the desired display language. The display language is updated immediately without the need to restart the device. For the remainder of this Section the English language setting is used.

Below are menu icons. Turn the jog dial to navigate between menu icons and press to enter a menu or go into selection mode. When in selection mode turn the jog dial to alter the value and press again to quit the selection. The **Datapoints** menu 🗀 allows browsing through the data points on the device.



Figure 1: Main Screen of the LCD UI.

The **Device Settings** menu ✿ allows configuring basic device settings. Navigate to the **Device Management »»** sub-menu, which is displayed in Figure 2.



Figure 2: Device Management Menu on the LCD UI.

This menu gives you the following options for basic device configuration:

- **TCP/IP Setup**: This menu allows configuring the device's IP address.
- **HTTP Server**: This menu allows to enable/disable the HTTP server and to configure its TCP port.
- **HTTPS Server**: This menu allows to enable/disable the HTTP server, to configure its TCP port and to remove an installed certificate.
- **Date/Time**: This menu allows setting the system time. A time synchronization mechanism can be chosen, and the UTC offset and daylight savings can be defined.

- **Send ID messages**: When selecting this menu, the device sends out service pin, BACnet I-Am, and identification broadcasts for finding the device in the L-Config tool on all applicable ports.

- **Reload config**: By choosing this menu, the device performs a quick restart by reloading its configuration only.

- **Reboot system**: By choosing this menu, the device performs a full reboot.

- **Clear DP config**: By choosing this menu, the user can clear the device's entire data point configuration. This is equivalent to the same Web UI function. The IP address as well as other settings needed to reach the device are not deleted.

- **Reset pers.values**: By choosing this menu, the user can clear all persistent values on the device. They are reset to default values if defined.

- **Factory Defaults**: By choosing this menu, the user can reset the entire device to its factory default. Also IP addresses are cleared.

- **Remote Config**: When enabling this option, the LWEB-822/900 master device manager restores the last saved configuration to the discovered device, if it has no configuration yet. This feature is beneficial when replacing a device.

- **PIN**: Alter the default PIN to any 4-digit number to protect certain operations on the LCD UI. The user will be prompted to enter the PIN on protected areas.

- **Contrast**: This menu allows adjusting the display's contrast.

- **LCD Rotation**: By choosing this menu item, the LCD display can be rotated by 180 degrees. This can be a useful setting if the device is mounted upside down.

- **Language**: By choosing this menu, the user can switch between languages on the LCD display.

The **VPN Setup** menu allows configuring the LWEB-900 VPN connection. In the setup menu, enter the 9-digit LWEB-900 project PIN code and optional device PIN code. In order to connect this device to LWEB-900 choose **Register Device** as shown in Figure 3.



Figure 3: Device VPN enrollment in LWEB-900

Alternatively, LOYTEC devices with a USB port can be on-boarded to the VPN using a USB thumb drive. Copy a '.ovpn' file the the thumb drive and plug it into the device. On the LCD display a menu will pop up that offers different options on the USB storage. Choose **Import VPN Config** from that menu and then select the ovpn file.

2.2 BACnet Settings

The **Device Settings »»** menu also allows configuring basic BACnet settings. Navigate to the **BACnet »»** sub-menu, which is displayed in Figure 2.



Figure 4: BACnet Menu on the LCD UI.

This menu gives you the following options for basic BACnet configuration:

- **Send I-Am message**: This menu allows sending an I-Am message to the BACnet network.
- **ID**: Use this menu to enter the BACnet device ID. Choose the first four digits then move on the last three digits.
- **BAC/IP Net**: On a BACnet router use this setting to specify the BACnet network number on the BACnet/IP port.
- **MS/TP Net**: On a BACnet router use this setting to specify the BACnet network number on the MS/TP port. If the device has more than one MS/TP port this menu is available for each MS/TP port. To disable the router port, scroll down till **off** appears.

2.3 WLAN Settings

On device models with a WLAN interface, the basic WLAN settings can also be configured on the LCD display. It provides menus to display and edit settings for the WLAN client, access point and mesh point. In order to make the setup of mesh networks simple, the Quick Wireless Setup menu can be used. Alternatively, a previously created configuration can be loaded from a USB stick.

Quick Wireless Setup: In the **TCP/IP Setup** menu choose the sub-menu **Quick Wireless Setup »»** beneath the list of IP interfaces. This opens the quick wireless setup menu as shown in Figure 5. This menu determines the physical channel for both wireless interfaces and the settings for the mesh point on a wireless interface. Optionally, the settings for an access point on the other wireless interface can also be made. After saving the settings, the display automatically goes to the TCP/IP configuration menu of the mesh point interface. For configuring the mesh point, only the mesh ID, the mesh point ID for this mesh point and a PIN are required. Starting from the mesh point ID, a default whitelist is generated. A pre-shared key can be generated out of the PIN code. When configuring the optional access point, transmission of the SSID can be disabled. A default password can be used or a random password be generated. The SSID of the access point is derived from the serial number of the device.

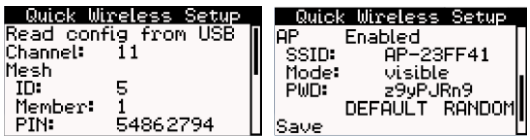


Figure 5: Quick Wireless Setup on the LCD Display.

The **TCP/IP Setup** menu of a wireless interface provides a **Wireless Setup »»** menu, which can be used to configure the WLAN modes of the interfaces separately (see Figure 6). After configuring the WLAN settings and saving them, the new WLAN mode is activated.

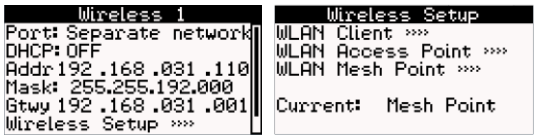


Figure 6: Wireless Setup on the LCD Display.

The following sub-menus for the different WLAN modes are available:

- **WLAN Client**: This menu displays the WLAN client settings. After saving these settings, the WLAN client mode is activated on this interface (see Figure 7).

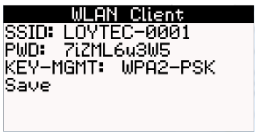


Figure 7: Wireless Setup on the LCD Display.

- **WLAN Access Point**: This menu (see Figure 8) allows displaying the SSID for this access point, which has been generated out the the serial number. Transmission of the SSID can be deactivated, the IEEE radio channel can be configured. Also a default password can be set or a random password can be generated. When saving these settings, the WLAN access point mode is activated on this wireless interface.

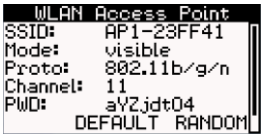


Figure 8: Access Point Setup on the LCD Display.

- **WLAN Mesh Point**: This menu allows configuring the Mesh point (see Figure 9). The Mesh ID can be chosen, a radio channel, PIN, and Mesh point ID can be selected. It is also possible to configure the whitelist entries. When choosing **GENERATE**, a default whitelist is generated depending on the Mesh point ID. When saving these settings, the WLAN Mesh point mode is activated on this wireless interface.

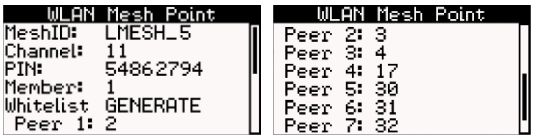


Figure 9: Mesh Point Setup on the LCD Display.

Read Config from USB. This menu in the Quick Wireless Setup menu allows reading in a previously generated Wireless configuration from a USB stick. For doing so, the USB stick needs a valid wireless configuration file and be connected to one of the USB ports. After loading the file, the configuration settings are displayed. These settings can then be accepted on one selected Wireless interface or on both interfaces, as shown in Figure 10.

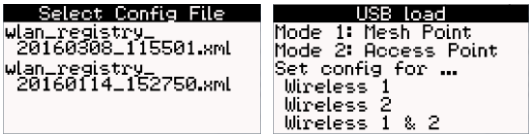


Figure 10: Loading a configuration over USB on the LCD Display.

When loading a wireless interface that has been configured in Mesh point mode, a mesh member menu is displayed (see Figure 11). In this menu the mesh point ID of this device can be chosen. This mesh point ID is used in the configuration by selecting **OK**. Additionally, the whitelist for this mesh point will be loaded from the configuration, if it contains one.

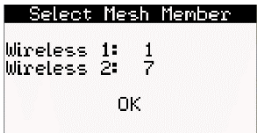


Figure 11: Mesh Member Selection on the LCD Display.

2.4 Local I/O Settings

2.4.1 I/O Page

On devices with local I/Os, the I/O page can be opened using the **I/O »»** menu from the home. The I/O page is shown in Figure 12. The top and bottom rows show the direction, state, and operating mode (without a letter = Auto, **M** = Manual, **O** = Override, **D** = Disabled, **U** = Unconfigured) of all I/Os.

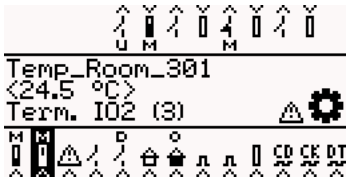


Figure 12: L-IOB LCD Display Main Page

The I/O state is shown as one of the following icons:

- **Switch Icon**: used for I/Os which generate a digital value as well as Inputs in Switch Mode,
- **Bar Icon**: used for I/Os which generate an analog value,
- **Pulse Icon**: used for pulse count inputs,
- **House Icon**: used for occupancy inputs,
- **Exclamation Mark**: shown for disconnected sensors or sensors which indicate an error,
- **Check Icon**: shown for sensors which indicate correct operation,
- **COM Icon**: used for all common terminals of relays and triacs.
- **CD Icon**: used for STId card reader code signals.
- **DT Icon**: used for STId card reader data signals.
- **CK Icon**: used for STId card reader clock signals.

When an I/O is selected, the middle of the main page shows the I/O name, current value, terminal name, and terminal number. To the right, the exit icon and I/O state icon is shown. When the exit icon is selected, the middle of the main page shows the device name. The device state icon shows an exclamation mark if at least one I/O shows an exclamation mark. Otherwise it shows the checked icon to indicate that all I/Os are operating correctly.

By turning the jog dial, the user can cycle through all I/Os. This can be used to get a quick overview of all I/O states. Observe that the common terminal icons (COM) only show the name and information of that terminal. No further configuration is possible for common terminals.

2.4.2 Unconfigured Mode

As long as a L-IOB I/O module in LIOB-Connect, LIOB-FT or LIOB-IP mode has not yet received a configuration from the L-IOB host, all relay outputs will be set into "Unconfigured" mode, indicated by the "U" icon on the I/O LCD page.

In this mode, manual control of the relay outputs is not possible.

2.4.3 Manual / Quick Edit Mode

If the jog dial is pushed shortly on an I/O in manual mode (**M**), the quick edit mode is entered, which allows changing the I/O value by turning the jog dial. By pushing the jog dial shortly again, the quick edit mode is left. When pushing the jog dial shortly on an I/O in auto mode (normal mode without special letter), one can quickly switch to both manual mode *and* quick edit mode by turning to the jog dial. The manual mode (along with the quick edit mode) can be left again by pushing the jog dial for at least one second. The manual mode can also be setup in the corresponding I/O configuration page (see Section 2.4.4).

If an input is in manual mode, the physical input from the connected sensor is ignored and the user can setup a simulated input value to be used in the logic application. This can be used e.g. to test the behavior of the application in the L-IOB device depending on certain input values. If an output is in manual mode, the value coming from the logic application is ignored and the user can set the value for the actuator connected to the physical output. This can be used to physically test the connected actuator.

It is possible that changing the manual value is restricted via a PIN code. In this case, the user will be requested to enter a pin code before the value can be changed. The pin code only needs to be entered once except when the device is not operated manually for more than 30 minutes.

2.4.4 I/O Configuration

If the jog dial is pushed for at least one second on any I/O, the configuration page for that I/O is entered, which allows viewing and changing configuration properties of the I/O. The properties which can be changed are enclosed by angle brackets ("<", ">"). By turning the jog dial, the user can cycle through the configuration properties. If the jog dial is pushed shortly on a property, the edit mode is entered, which allows changing the property by turning the jog dial. By pushing the jog dial again, the edit mode is left.

It is possible that changing properties is restricted via a PIN code. In this case, the user will be requested to enter a pin code before a value can be changed. The pin code only needs to be entered once except when the device is not operated manually for more than 30 minutes.

To leave the configuration page, the user must turn the jog dial until the title line (I/O name) is selected and then push the jog dial. Alternatively, the jog dial can also be pushed anywhere on the page for at least 1 second.

Observe that depending on the hardware type, signal type, and interpretation of an I/O, the list of configuration properties varies. Refer to the LINX Configurator User Manual [1] for detailed information on the different configuration properties. In addition to the configuration properties described there, for some I/Os, a "RawValue" property will be displayed. It shows the physical measured value for inputs (e.g. the resistance of an NTC) resp. the physical value for outputs (e.g. the actual voltage for analog outputs). Note that this information can be used for debugging sensors or actuators but is not available in the form of data points.

For counting inputs, two additional configuration options are available: ‘Pulse Count Reset’ and ‘Count Start Value’. Using ‘Pulse Count Reset’, the counter can either be reset to 0 or to the value set in ‘Count Start Value’.

2.5 LIOB-IP Page

Some LOYTEC device models can additionally host LIOB-45x/55x devices in LIOB-IP mode. This requires firmware version 4.8 or higher. The corresponding LCD page can be entered from the main page via **LIOB-IP** or **Device Settings »» LIOB-IP »»**.

Even without any configuration, the LIOB-IP bus can be scanned to check if a LIOB-45x/55x device is connected to the L-IOB host. In the **LIOB-IP** page, select the item **Scan L-IOB bus** to scan for an attached LIOB-45x/55x device. At the end of the scan process, the LCD will show the detected L-IOB device and its status resp. error state. By pushing the jog dial on the detected L-IOB device, some configuration properties of the device are displayed.

If a configuration is downloaded to the L-IOB host using the Configurator software, a configuration run is started automatically and if the configuration matches the physically attached LIOB-45x/55x device, it should go online. The configuration run can also be started manually at any time by selecting **Configure LIOBs** in the **LIOB-IP** page.

The attached LIOB-45x/55x Device can be enabled and disabled by pushing the jog dial on the device (shown in the **LIOB-IP** page) and choosing **Enable** or **Disable**. To activate the new setting, a configuration run must be started afterwards by choosing **Configure LIOBs** as described above.

The LCD Display of a connected LIOB-45x/55x device can be remotely accessed by pushing the jog dial on the device (shown in the **LIOB-IP** page) and choosing **Remote Display**. To leave the remote display mode again, either push and hold the jog dial for at least 10s and then release it or exit via the **Remote LCD Access** menu item in the device configuration page of the LIOB-45x/55x device.

2.6 Firmware Upgrade

Devices with USB connectors support firmware upgrade from a USB memory stick. Copy a firmware ‘.zip’ or ‘.dl’ file to the USB memory stick. Then plug the USB memory stick into the device. On the LCD display a menu will pop up that offers different options on the USB storage. Choose **Firmware Update** from that menu as shown in Figure 13.



Figure 13: USB pop-up menu on the LCD UI.

A list containing available firmware images is displayed. Choose the one for the update and confirm the choice (see Figure 14).



Figure 14: LCD UI firmware update chooser.

The chosen file is unzipped. Do not remove the USB memory stick while uncompressing. After the information on unzipping has disappeared, the USB memory stick can be removed. The display indicates that the firmware upgrade is in progress and the new image is being installed.

2.7 PIN Code Protection

The LCD UI can be protected by a PIN-code. If a PIN code has been set, the **Datapoint** and all device configuration menus are protected and require a login using the PIN code. When logged in, the LCD display can be used to perform configuration tasks. After being idle for 15 minutes the LCD logs off automatically. You can also use the **Logout** option in the **Device Settings** to log out immediately. A new attempt to enter a protected menu will require a PIN code again.

For certain applications it is desireable to let the operator view a selected number of data points without entering a PIN code. For setting this up, create a folder called "UnprotectedBrowse" in the "Favorites" tree. All favorites in the unprotected browse folder will be accessible without the PIN code. The folder description of the "UnprotectedBrowse" folder will be displayed to the operator for convenience. For instance, set the description to "MyRegs" and the LCD display will show "MyRegs" as the folder name when entering the **Datapoints** menu as shown in Figure 15.



Figure 15: Unprotected data point browser.

3 Web Interface

LOYTEC devices come with a built-in Web server and a Web interface to configure the device and extract statistics information. The Web interface allows configuring the IP settings, CEA-709, CEA-852, BACnet and other configuration settings.

3.1 Device Information and Account Management

3.1.1 Device Setup

The LOYTEC device is shipped with DHCP enabled and auto-configures an IP address when connected to the network. In a Web browser, enter the IP address of the device shown on the LCD display.

The login screen of the device is shown and prompts for initial administrator and operator passwords to be set. The password strength indicator will inform you about the security quality of your passwords. Enter the passwords in the screen as shown in Figure 16 and then click on **Set passwords**.

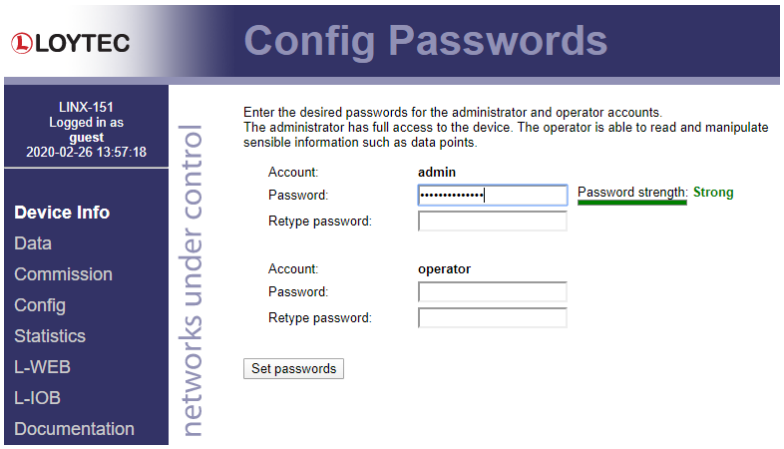


Figure 16: Configure admin and operator passwords.

The Web UI cannot be used without configuring the passwords. Note that strong passwords should be chosen (avoid ‘admin’ or ‘loytec4u’). The device information page will appear. The passwords can be changed later as described in Section 3.7.1.

3.1.2 Device Information

The device information page (Figure 17) shows some general information about the device in the **General Info** section. This includes the product model and the current firmware version. Below, it shows important operational parameters, such as free memory, CPU load, system temperature and supply voltage, time synchronization status and system uptime.

Note: *For AC powered devices the supply voltage reading is VAC * sqrt(2), e.g., 24VAC reads as 34V.*

In the upper right corner of the page header a flag symbol indicates a language selector. Choose the desired interface language and it will become effective immediately. This is the same as changing language on the LCD display.

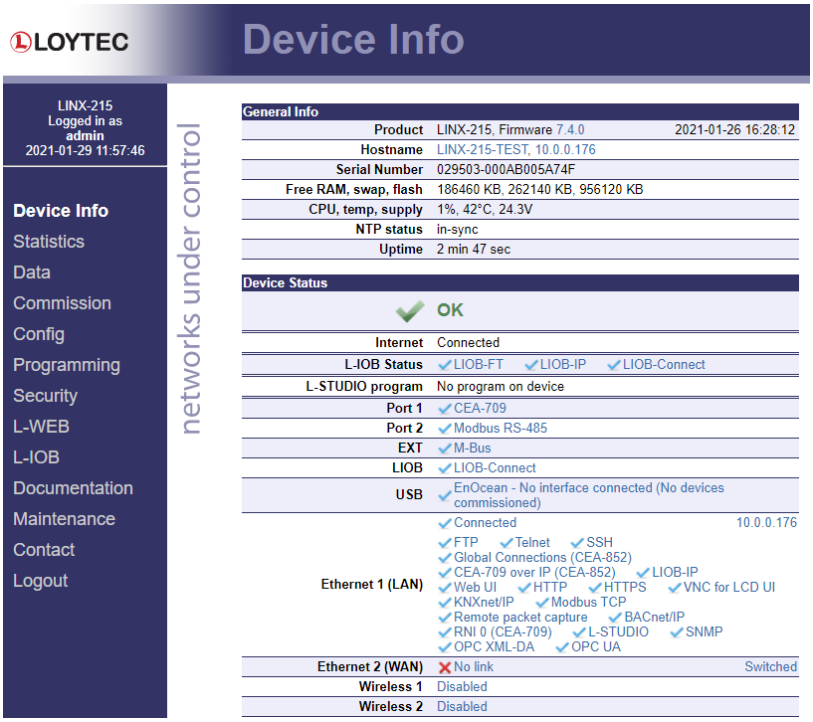


Figure 17: Device Information Page.

The **Device Status** section summarizes the status of the various ports and protocols on the device. The summary status is displayed as a green OK checkmark. If any of the interfaces, protocols or operational parameters are non-normal, a warning or error sign is shown instead. The status page also indicates, if one or more data points are overridden. L-INX devices show information on the current IEC61131 program. This includes the state of the PLC kernel, the I/O driver and the program source information. Shown below are further a summary on the enabled L-IOB I/O buses and active protocols on the respective ports. All items are links that lead directly to their configuration page.

Below the general status information more specific sections are displayed depending on the model. The **Firmware Info** provides version and build times of the primary and fallback firmware images installed on the device. The **Project Information** area shows details on the currently loaded data point configuration. The **Router Info** and **CEA-709 Application** sections include the unique node IDs ("Neuron IDs") of the CEA-709 network interfaces. This page can also be used to send the CEA-709 service pin messages. This is a useful feature when commissioning the device, since it is not necessary to be on-site to press the status button.

3.1.3 Device Login

Click through the menus on the left hand side to become familiar with the different screens. If you click on **Config** in the left menu, you will be asked to enter the administrator password in order to make changes to the settings as shown in Figure 18. Enter the administrator password and select **Login**.

If logging in using a local user having the 'admin' role, edit the user name in the Account field.

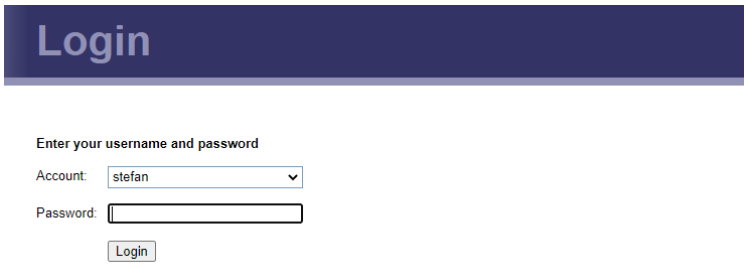


Figure 18: Enter the user name and password.

3.2 Device Statistics

The device statistics pages provide advanced statistics information about the CEA-709 device, the CEA-852 device, the BACnet device, the system log, the scheduler, the alarm log and the Ethernet interface.

3.2.1 System Log

The **System Log** page prints all messages stored in the system log of the device. An example is shown in Figure 19. This log data is important for trouble-shooting. It contains log entries for reboots and abnormal operating conditions. Errors and warnings are color-coded in red and yellow. The default log direction is newest entries on top. The direction can be edited by clicking on the arrow ⇑ in the column header.

To save the log click on the **Save System Log** button. When contacting LOYTEC support, have a copy of this log ready.

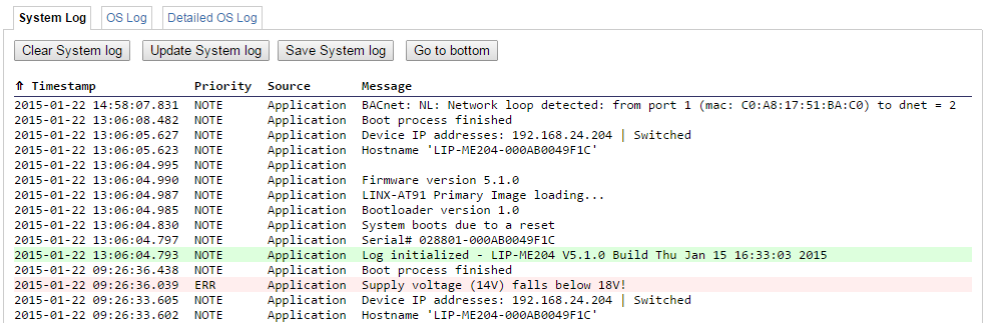


Figure 19: System Log Page.

3.2.2 IP Statistics

Figure 20 shows the IP statistics page. The **Ethernet** tab allows finding possible problems related to the IP communication. Specifically, any detected IP address conflicts are displayed (if the device's IP address conflicts with a different host on the network). It also shows the routing table, the ARP table (including IPv6 neighbours), DNS configuration, and detailed connection statistics. The **Wireless** tab contains statistics specific to the LWLAN-800 interface.

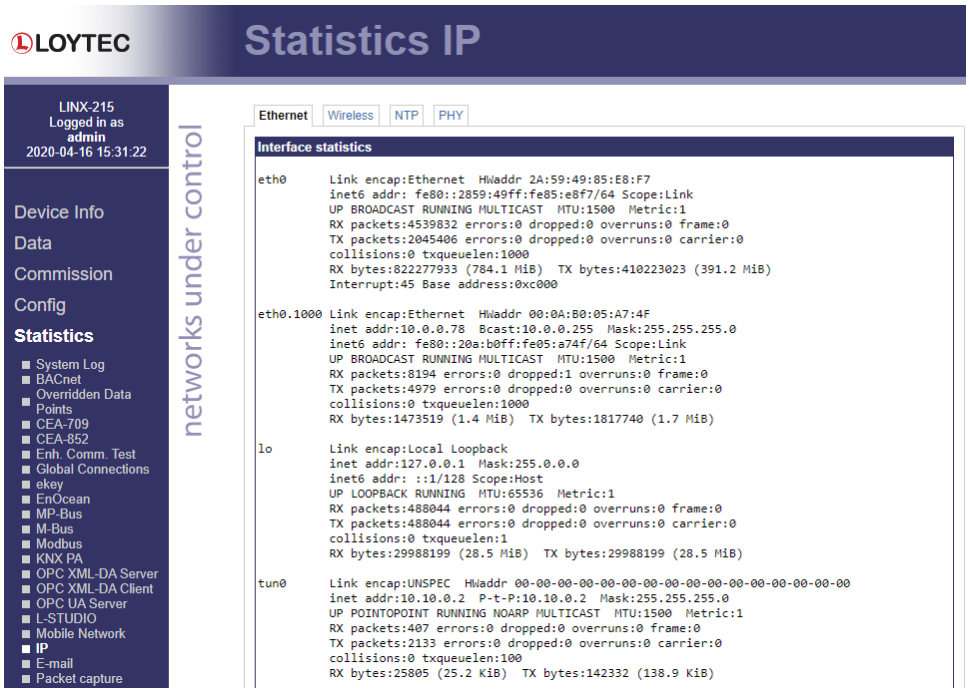


Figure 20: IP Statistics Page.

The **NTP** tab provides information on the contacted NTP servers and their synchronization status. The **PHY** tab shown information on the Ethernet link state, link speed and seen MAC addresses on either Ethernet port.

3.2.3 E-mail

The E-mail statistics page shows information regarding the devices SMTP client (e-mail transmission). This includes information regarding the number of messages queued for transmission (Queued currently/total/max), transmitted messages (delivery successful/failed/failed after retry) and dropped messages (with reason for dropping). Maximum time for gethostbyname shows needed time to resolve DNS names. If the maximum time is high, a problem with DNS servers is likely. Maximum time for SMTP transfer adds up DNS and e-mail transfer time.

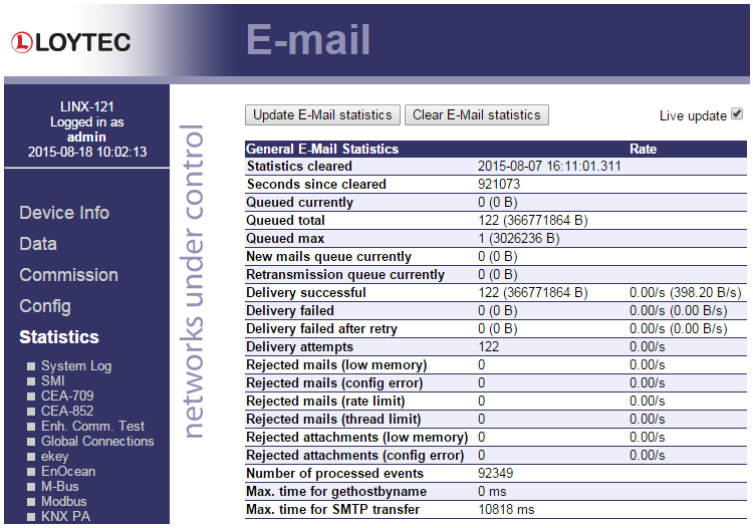


Figure 21: E-mail Statistics.

3.2.4 CEA-852 Statistics

The CEA-852 statistics page displays the statistics data of the CEA-852 device on the device. It is only displayed if the CEA-852 interface is enabled and supported by the device model. The upper part of the CEA-852 statistics page is depicted in Figure 22. To update the statistics data, press the button **Update all CEA-852 statistics**. To reset all statistics counters to zero, click on the button **Clear all CEA-852 statistics**. The field **Date/Time of clear** will reflect the time of the last counter reset.

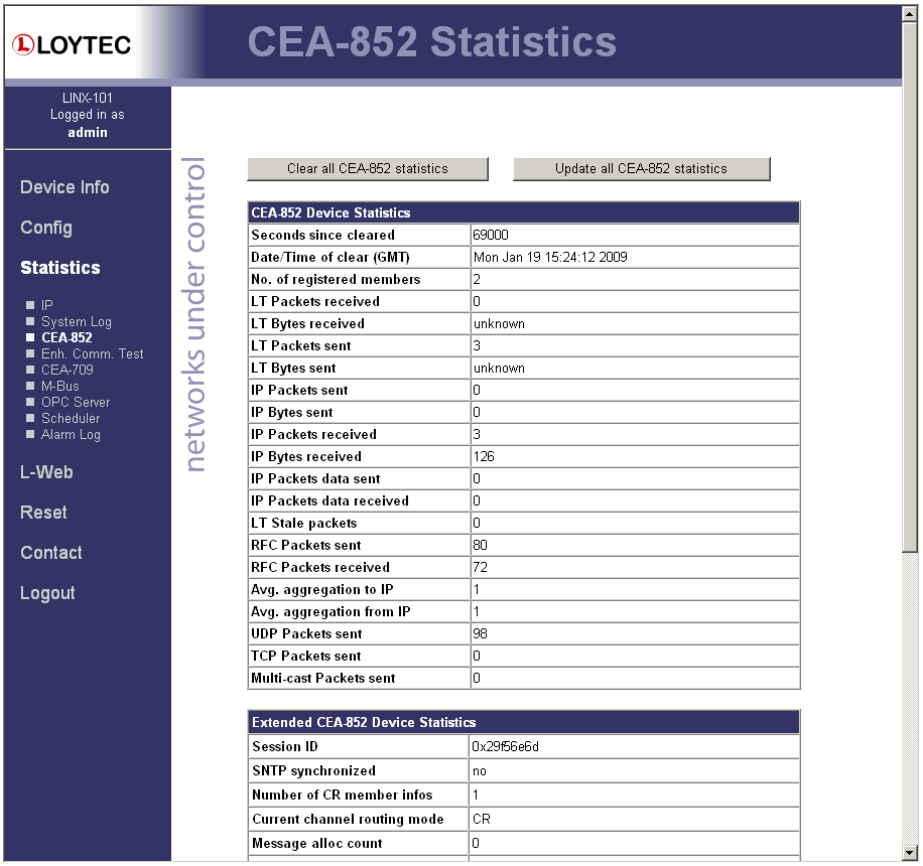


Figure 22: Part of the CEA-852 Statistics Page.

3.2.5 Enhanced Communications Test

The Enhanced Communications Test allows testing the CEA-852 communication path between the CEA-852 device on the L-INX/L-GATE and other CEA-852 devices as well as the configuration server. The test thoroughly diagnoses the paths between individual members of the IP channel and the configuration server in each direction. Port-forwarding problems are recognized. For older devices or devices by other manufacturers, which do not support the enhanced test features, the test passes as soon as a device is reachable, but adds a comment, that the return path could not be tested. A typical output is shown in Figure 23.

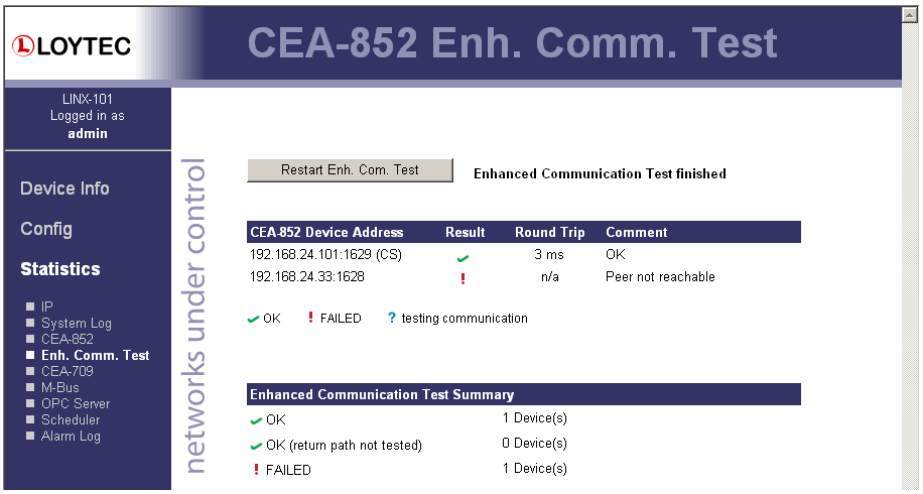


Figure 23: Enhanced Communication Test Output.

The Round Trip Time (RTT) is measured as the time a packet sent to the peer device needs to be routed back to the device. It is a measure for general network delay. If the test to a specific member fails, a text is displayed to describe the possible source of the problem. The reasons for failure are summarized in Table 1.

Text displayed (Web icon)	**Meaning**
OK, Return path not tested (green checkmark)	Displayed for a device which is reachable but which does not support the feature to test the return path (device sending to this CEA-852 device). Therefore a potential NAT router configuration error cannot be detected. If the tested device is an L-IP, it is recommended to upgrade this L-IP to 3.0 or higher.
Not reachable/not supported (red exclamation)	This is displayed for the CS if it is not reachable or the CS does not support this test. To remove this uncertainty it is recommended to upgrade the L-IP to 3.0 or higher.
Local NAT config. Error (red exclamation)	This is displayed if the CEA-852 device is located behind a NAT router or firewall, and the port-forwarding in the NAT-Router (usually 1628) or the filter table of the firewall is incorrect.
Peer not reachable (red exclamation)	Displayed for a device, if it is not reachable. No RTT is displayed. The device is either not online, not connected to the network, has no IP address, or is not reachable behind its NAT router. Execute this test on the suspicious device to determine any NAT configuration problem.

Table 1: Possible Communication Problems.

3.2.6 Global Connections Statistics

The global connections statistics page shows all currently configured communication groups. For each group the list displays name, address hash, receive, transmit, poll-on-startup status, the most recently communicated value and its timestamp. An example is shown in Figure 24. The receive/transmit/poll-on-startup status displays an ✕ if the direction is configured, but no value was communicated. A green check mark ✔ is shown as soon as a value was received or transmitted, respectively.

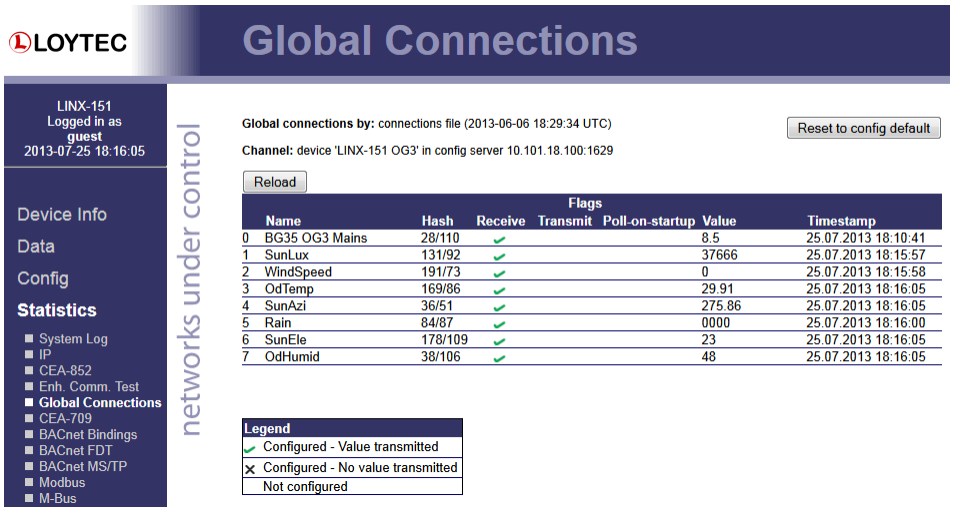


Figure 24: Global Connections Statistics

The **Reload** button refreshes the status. The button **Reset to config default** removes any global connections configured by LWEB-900 at run-time and reverts to the configuration default. A reboot is required in this case.

3.2.7 CEA-709 Statistics

The CEA-709 statistics page displays statistics data of the CEA-709 port on the device as shown in Figure 25. This data can be used to troubleshoot networking problems. To update the data, click on the button **Update CEA-709 statistics**.

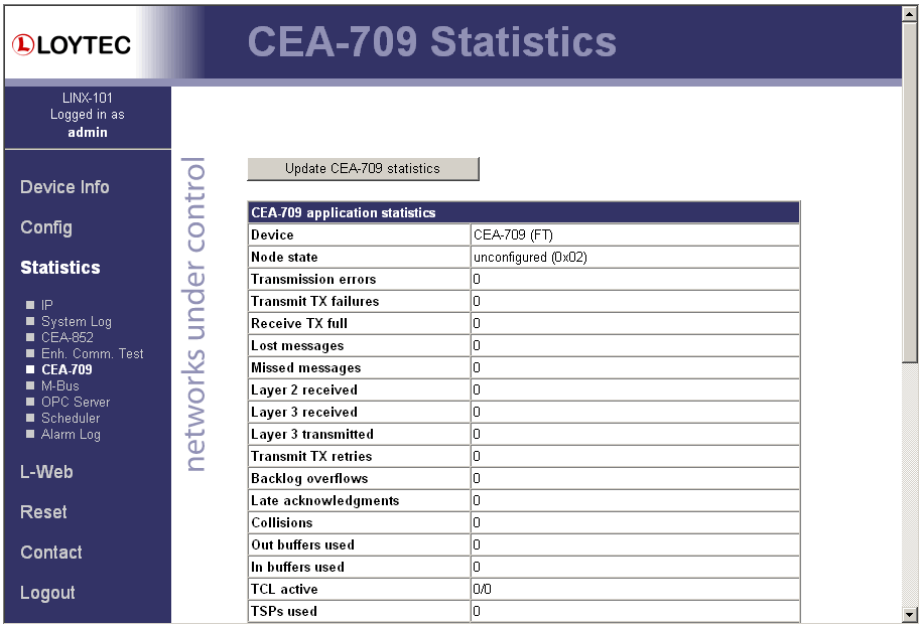


Figure 25: CEA-709 Statistics Page.

3.2.8 OPC XML-DA Server Statistics Page

The OPC XML-DA server statistics page shows statistics data, which contains information on currently and previously connected clients. An example list of OPC clients is shown in Figure 26. Clicking on the **Update OPC XML-DA statistics** button retrieves the current statistics.

The **Summary** table on the top of the page displays the number of currently connected clients. These clients occupy TCP connections. The next line specifies the total number of accepted client connections since the device is running. The figure for rejected connections can be used to detect situations, where too many clients try connecting at the same time.

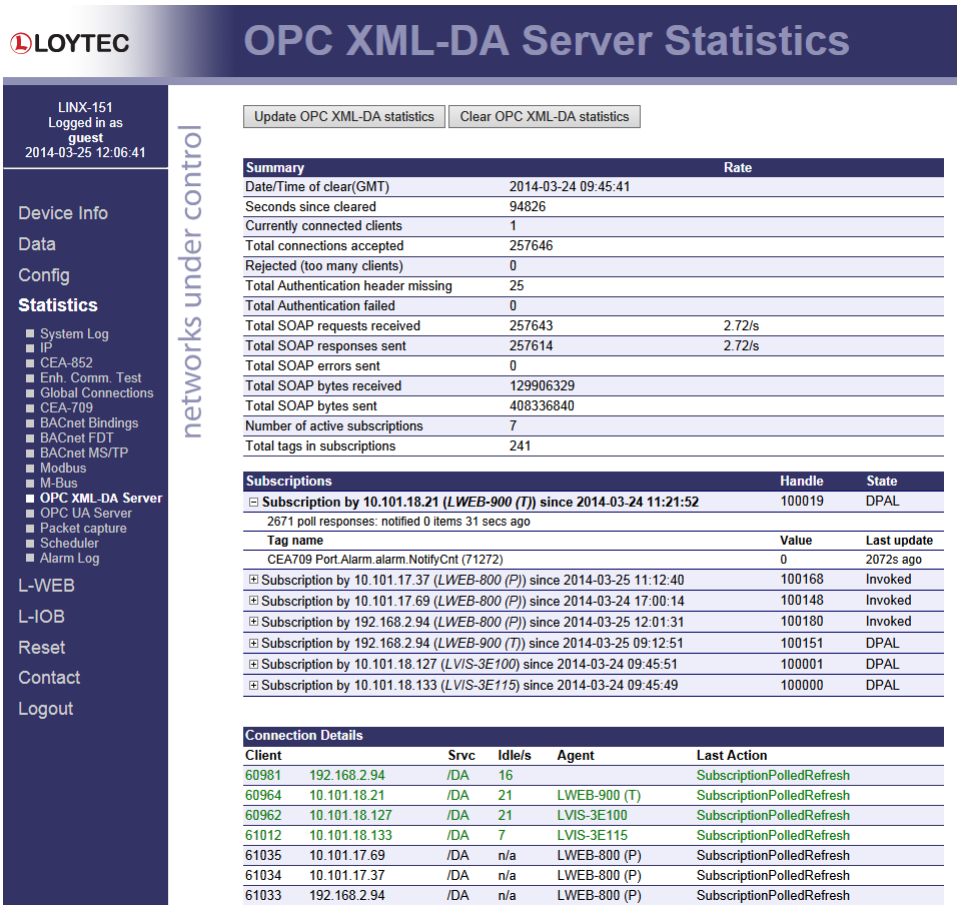


Figure 26: OPC XML-DA Server Statistics Page.

The **Subscriptions** list shows detailed information on OPC items subscribed by OPC XML-DA clients. The subscriptions are sorted by client IP address and can be expanded to show the subscribed items. The **Handle** specifies the server subscription handle and the value represents the last value notified for the respective item in this subscription.

The **Connection Details** list shows more information on the history of client connections. The green lines at the top denote currently active connections. Active connections have an idle time figure specified in seconds. The following lines in black represent a history of the most recent connections. Inactive connections read “n/a” in the **Idle** column.

All lines contain client information, which specifies the client IP address and port of the connected client. The **Srvc** column specifies the type of Web service (Web, DA, and DL). The **Agent** column contains information on the HTTP agent of the client, and the **Last Action** column contains information on the last known Web service SOAP action the client has requested.

3.2.9 BACnet MS/TP Statistics

The BACnet MS/TP statistics page is only available, when the MS/TP data link layer is enabled (see Section 3.5.21) and supported by the L-INX model. The three statistics items displayed are: Device Statistics, Bus History, and Token History.

The **MS/TP Device Statistics** (see Figure 27) is split into three major columns, **MS/TP State/RX**, **TX Port**, and **RX Port**. The MS/TP State/RX column contains information related to the status of the MS/TP machine as well as packets received and processed by the MS/TP state machine. The TX Port column counts packets sent by the device according to their types, and the RX Port column tracks packets and errors seen by the MS/TP receive state machine.

The most prominent information in the **MS/TP State/RX** column is the **status** entry which describes the current status of the MS/TP token as perceived by the device. In status **Token Ok**, the token is circulating between the masters. This is the normal state, when multiple masters are on the MS/TP network. The status **Sole Master** is the normal state when the device is the only master on the network. If there are multiple masters on the network, token passing has been interrupted and this state is a hint to a broken cable. In state **Token Lost**, the token is currently not circulating.

While **status** reflects the current state the device is in, the **lost tokens** counter is more indicative for communication problems on the MS/TP network. If it increases, there are cabling, ground, or termination issues.

Note, that the **RX Port** column monitors all packets seen on bus, not only those addressed to the device. Statistics related to received packets that are addressed to the device are tracked in the **MS/TP State/RX** column.

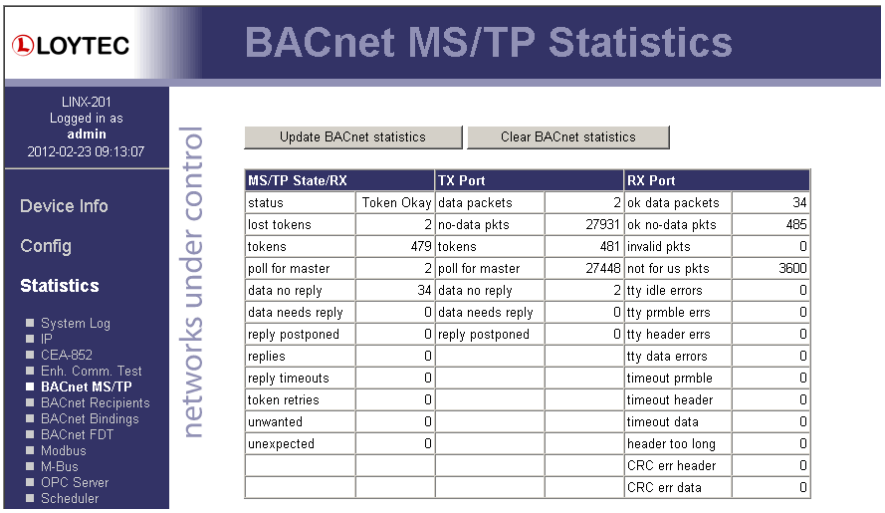


Figure 27: BACnet MS/TP Device Statistics.

The **MS/TP Bus History** (see Figure 28) presents information related to the MS/TP bus as a whole over the last minute, split into 10 second time slices.

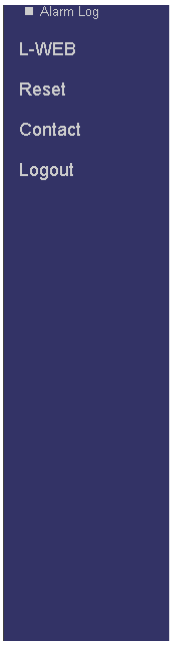
The convenient **health** indicator, a percentage in the range 0 – 100%, gives an overall impression of the communication quality on the bus: The higher the percentage, the better the MS/TP communication between devices on the bus. Reasons for **health** to be low are:

- Superfluous PollForMaster requests (because MS/TP node addresses in use contain gaps or Max_Master of the node with the largest node address is not set to the same value as the node's address),
- token losses,
- reply timeouts,
- slow token passing.

The **load** percentage simply displays how much of the available bandwidth is used for data. Note, however, that actual application data is only a subset of the amount of data taken into account here.

Statistics reflecting the average ability of devices to initiate communication are **roundtrip** and **token/dev/sec**. They give an impression on how long the token requires to circulate once (in milliseconds), and how often a device on the bus receives the token per second.

Other counters of interest are: **tk passes** (the number of times the token was passed), **tk misses** (the number of times the receiver of a token did not continue passing the token), **tk retry** (the number of times passing of token was retried), **postponed** (the number of ReplyPostPostponed packets seen), **pfm** (the number of PollForMaster packets seen), **data pkt**, **data pkt rx**, **data pkt tx** (the number of data packets seen, the number of data packets received and transmitted by the device), ***data, data rx, data tx*** (the amount of data seen, the amount of data received and transmitted by the device), **token rx** (the number of tokens received by the device).



Update BACnet statistics | Clear BACnet statistics

Bus History							
09:12:50 - 09:13:00 (0.0sec sole master, 0.0sec sole master activity)							
health	33%	load	0%	roundtrip	120ms	token/dev/sec	8.301
tk passes	753	token rx	83	data pkt	0	data	0byte
tk misses	0	postponed	0	data pkt tx	0	data tx	0byte
tk retry	0	pfm	124	data pkt rx	0	data rx	0byte
09:12:40 - 09:12:50 (0.0sec sole master, 0.0sec sole master activity)							
health	31%	load	0%	roundtrip	126ms	token/dev/sec	7.900
tk passes	707	token rx	79	data pkt	0	data	0byte
tk misses	0	postponed	0	data pkt tx	0	data tx	0byte
tk retry	0	pfm	115	data pkt rx	0	data rx	0byte
09:12:30 - 09:12:40 (1.1sec sole master, 0.0sec sole master activity)							
health	13%	load	0%	roundtrip	104ms	token/dev/sec	9.601
tk passes	554	token rx	96	data pkt	0	data	0byte
tk misses	1	postponed	0	data pkt tx	0	data tx	0byte
tk retry	1	pfm	122	data pkt rx	0	data rx	0byte
09:12:20 - 09:12:30 (10.0sec sole master, 0.0sec sole master activity)							
health	12%	load	0%	roundtrip	0ms	token/dev/sec	0.000
tk passes	38	token rx	0	data pkt	0	data	0byte
tk misses	5	postponed	0	data pkt tx	0	data tx	0byte
tk retry	0	pfm	187	data pkt rx	0	data rx	0byte
09:12:10 - 09:12:20 (10.0sec sole master, 0.0sec sole master activity)							
health	100%	load	0%	roundtrip	0ms	token/dev/sec	0.000
tk passes	0	token rx	0	data pkt	0	data	0byte
tk misses	0	postponed	0	data pkt tx	0	data tx	0byte
tk retry	0	pfm	189	data pkt rx	0	data rx	0byte

Figure 28: BACnet MS/TP Bus History.

The **MS/TP Token History** (see Figure 29) shows the most recent token passes on the bus. The syntax used is simple: '`40<15`' means that the node with address '0x15' has passed the token to the node with address '0x40'.

If token losses or token sending retries have been recorded, these are marked by substituting '**.**' for '<'. For example, '`40<15.40<15`' either means that '0x15' retried sending the token to '0x40', or that passing the token to '0x40' failed and '0x15' created a new token and sent it to '0x40'.

Transitions to or from sole master mode can be spotted by looking out for '`XX`', e.g., '`XX<15`' means that after '0x15' received the token, the device entered sole master mode. Finally, based on the recorded token passes, the MS/TP Token History also lists the node addresses of MS/TP masters detected on the bus.

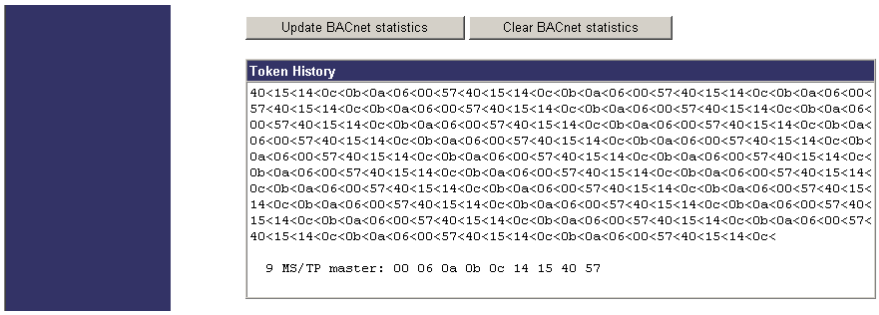


Figure 29: BACnet MS/TP Token History.

3.2.10 BACnet Bindings Statistics

The BACnet bindings statistics page displays a list of all currently active address bindings. This list can be used for troubleshooting to see, which BACnet device instance numbers could be resolved and to what BACnet network number and MAC address. See Figure 30 for an example list. In this case the device instance 224220 has been resolved to the local network and MAC address 192.168.24.220:BAC0.

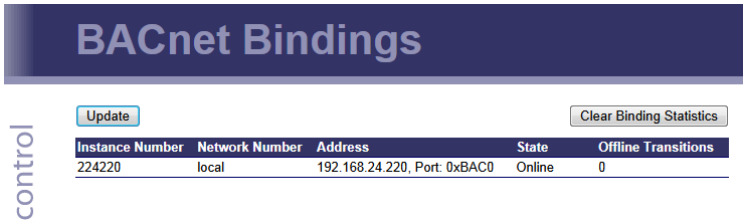


Figure 30: BACnet bindings statistics page.

3.2.11 BACnet/SC Statistics

The BACnet/SC statistics can be found on the Port tab of the BACnet Statistics page. Choose the sub-tab for the port where the BACnet/SC protocol is running on, shown in Figure 31. The **Node State** reflects the overall BACnet/SC node operation state. In an error state, look at the **Primary error reason** and **Failover error reason** to learn about the error reasons. In a regular operation state, the primary connection should be “OK” and the failover “Idle”. Otherwise, errors are reported, such as “Couldn’t resolve hostname” or “Timeout error”.

Reconnect count is increasing every time the BACnet/SC node retries a hub connection. This can be successful or result in an error. In this case **Connection errors** are counting up. When a connection was established to the hub but the node was rejected by the hub, then **Reject errors** is counting up.

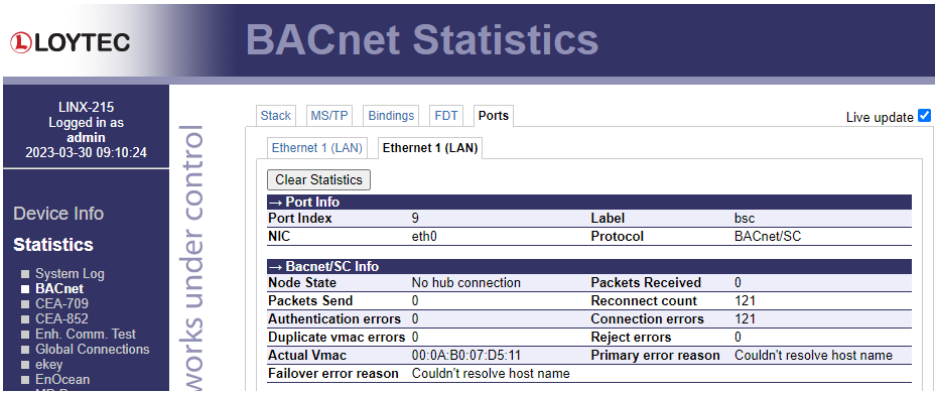


Figure 31: BACnet/SC statistics.

3.2.12 BACnet FDT Statistics

The BACnet FDT (Foreign Device Table) Statistics page displays a list of all BACnet/IP foreign devices currently registered with the device (see Figure 32). Note, that foreign devices can only register with the device if the latter is configured as BACnet **Broadcast Management Device** (see Section 3.5.18).

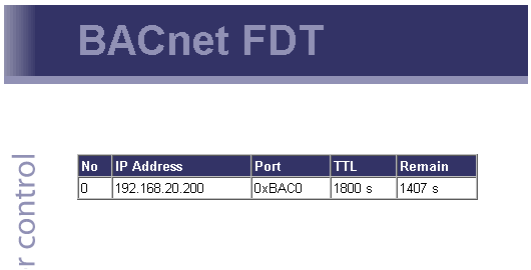


Figure 32: BACnet FDT Statistics page.

3.2.13 Scheduler Statistics Page

The scheduler statistics page provides an overview of what is scheduled at which day and which time. In the **Display Schedules** list, select a single schedule to view its scheduled values and times. Use the multi-select feature to get the overview of more schedules. An example is shown in Figure 33.

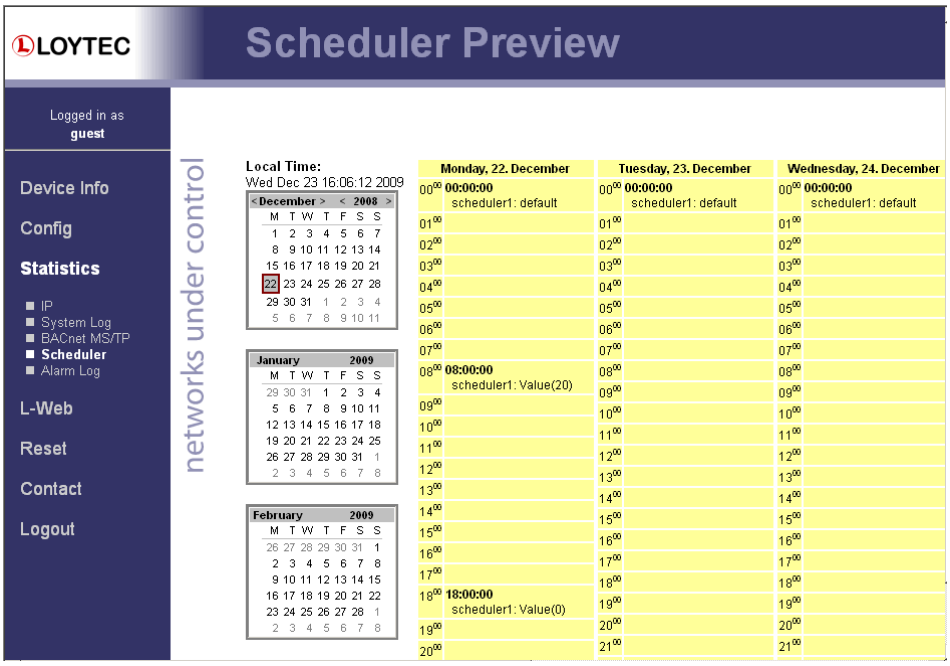


Figure 33: Scheduler Statistics Page.

3.2.14 Packet Capture

The packet capture feature allows configuring and running a local packet capture for the Ethernet and MS/TP ports. Please refer to Section 20.2 for more information on how to set up local capture and configure remote packet capture with Wireshark.

3.2.15 Mobile Network

The **Mobile Network** statistics page shows traffic statistics over the LTE-800 mobile interface as shown in Figure 34. The first table **Mobile Network Data Usage** accounts for an aggregated data and SMS transfer volume since the last data usage reset. These counters

are persistent over device reboots. By clicking on **Reset Data Usage** those counters are reset to 0.

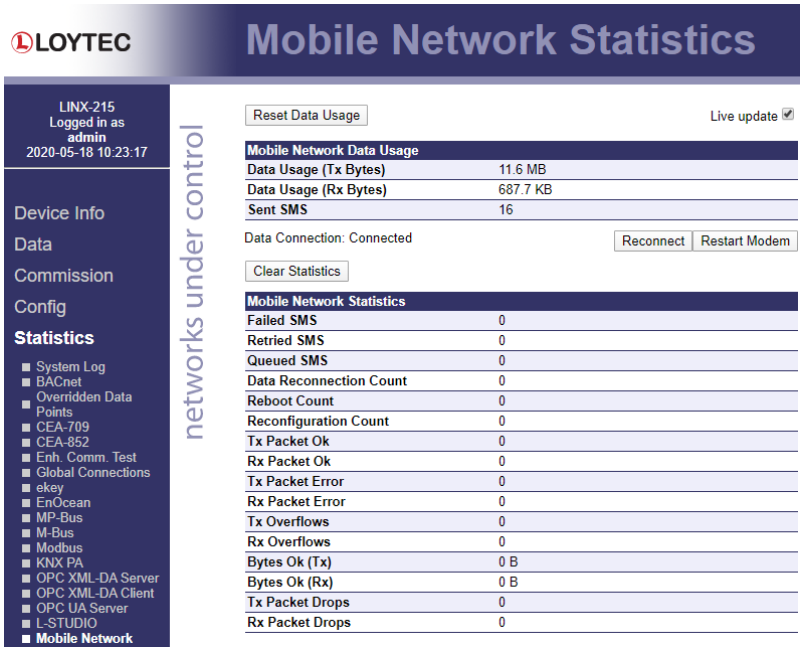


Figure 34: Mobile Network Statistics Page.

Under the first table, the **Data Connection** status is displayed. For testing purposes, the button **Reconnect** allows clearing and re-connecting the LTE data connection. The button **Restart Modem** allows restarting the LTE modem. During normal operation, these actions are not necessary. The second table **Mobile Network Statistics** provides information on data and SMS transfer volume per data connection. **The Clear Statistics** button clears the data of this table but leaves the aggregated data volume unchanged.

3.3 Data Management

3.3.1 Data Points

The device's Web interface provides a data point page, which lists all configured data points on the device. An example is shown in Figure 35. The data point page contains a tree view. Clicking on a particular tree item fills the right part of the page with a data point list of that tree level. A breadcrumb navigation header allows navigating back to an arbitrary level in the tree. The displayed items per page can be configured (including ALL) and the pagination header allows jumping to selected pages directly.

The data point list displays the data point name, direction, type, data point state, current value, engineering unit and a description. All values are updated live. Inactive points are displayed in gray. If the data point list does not fit on one page, there are page enumerator links at the bottom. Important data point states and their implications are listed in Table 2. Values can be directly edited in the list where the pencil symbol appears. Data point structures can be expanded or collapsed for better overview. For the structure top a compact list of all member values is displayed including units.

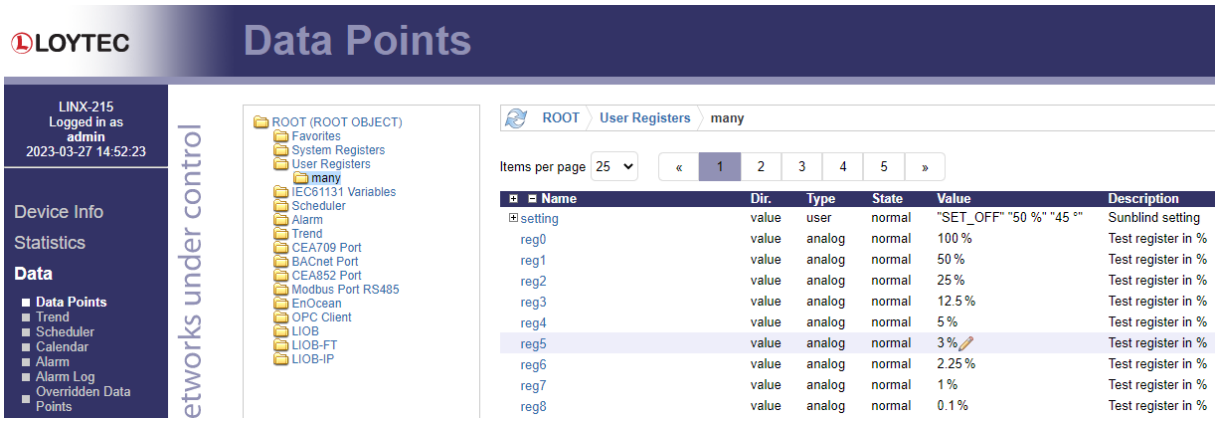


Figure 35: Data point page.

Data Point Status	Description
normal	The data point is in normal operation state and possesses a value.
invalid value	The data point has no valid value.
normal (config)	The data point has a normal value but it is not fully configured on the network (not commissioned, no binding, no client mapping, etc.)
overridden	The data point value is overridden by the user and currently is not driven by network communication or controller logic.
offline	The data point has a value but it is not reflected on the network due to a communication error (e.g., the peer node is not online).
unreliable (offline)	The data point is in normal operation. The value of it, however, is qualified as unreliable because a connected data point is offline. For an output data point it means that the value was fed from a connection, where the source is offline. For an input data point it means that the connected output data point could not send the value to the network.
unreliable (range)	The data point is in normal operation. The value of it, however, is qualified unreliable because the value is an out-of-range value for the connected data point. The value is limited to the supported range.
unreliable	The data point is in normal operation. The value of the data point or a connected data point has been tagged as unreliable over the network. This is the case when the BACnet reliability has been written.
not configured	The data point is mapped to a port, which is not configured (e.g., the port is disabled).
inactive	The data point is inactive and the line is grayed-out. Values can be written but no network communication is triggered. This can be the case, if a data point is not used in the configuration or it is connected to a BACnet server object, which is not present on the device.

Table 2: Data Point States.

The data point names are links. Clicking on such a link opens a detailed page on that data point. If the data point supports it, the user can also enter a new data point value as depicted in Figure 36. For a structured data point the member values are displayed and can be edited in a structure grid. The **Timestamp** field contains the last update time of the data point and the source of the write, e.g. written by Web UI. The **Status** field is discussed in Table 2. The field **Status Description** contains a describing text for the data point status. The **Flags**, **Poll cycle**, **Min/Max send time** and **Max age** fields are the common timing parameters for the data point. See Chapter "Concepts" of the LINX Configurator User Manual for a closer discussion on timing parameters. **UID** is the data point UID assigned by the Configurator to

this data point. The **Native Info** field displays detailed information on the underlying technology object.

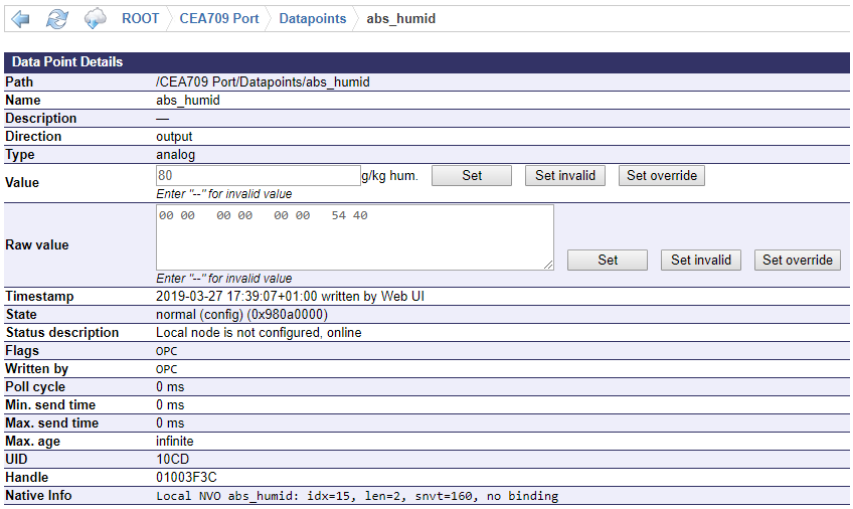


Figure 36: Data point details page.

Clicking on the **Set** button writes the new value to the device's data server, **Set invalid** writes the invalid value. When setting a value, the Web page displays the status of the action:

- **Successfully set value**: The new value has been successfully set in the data point and the update has been sent on the network, if it is a network data point.
- **Could not send value update**: The new value has been set but it has not been sent out on the network. The reason can be that the peer node is currently offline or there is a configuration error. The data point status reflects this error.
- **Could not set value (Forbidden)**: The value cannot be written over the Web interface. This can be the case if the data point is written by the L-STUDIO runtime. Check if the data point is marked PLC_OUT.
- **Could not set value (error code)**: The new value has not been set because of an internal error. Please contact LOYTEC with the error code.

3.3.2 Priority Array

For the BACnet technology, the data point details page provides an editor to manipulate the respective BACnet priority slots of the underlying BACnet object directly. For doing so, click the button **Edit Priority Array**.

An editor pop-up opens as shown in Figure 37. The editor allows editing each priority slot, including a clear option to withdraw a slot. Then click the **Save** button to exit the editor.

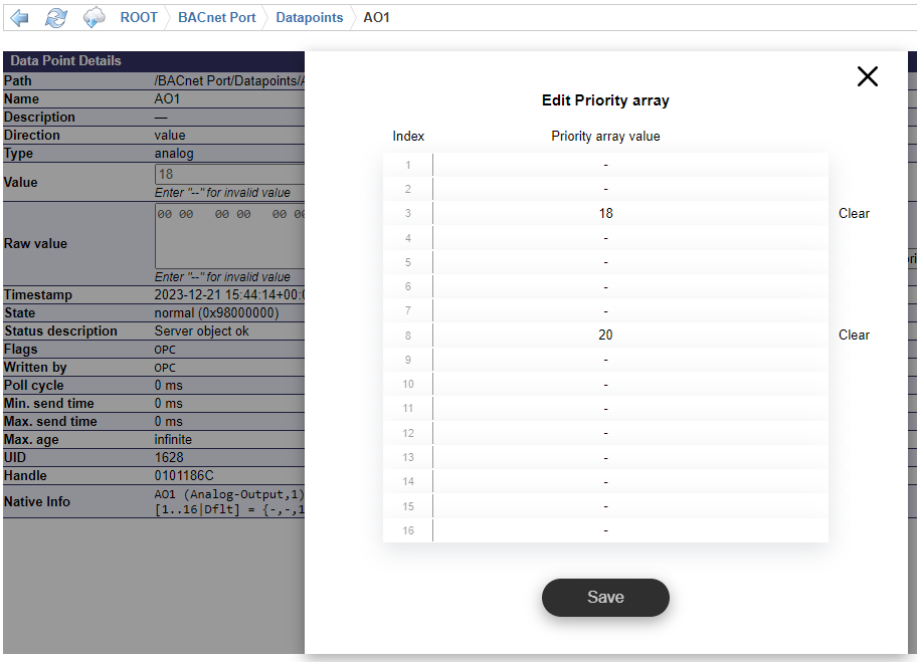


Figure 37: BACnet priority array editor on the data point Web UI.

3.3.3 Manual Override

Data point values can be manually overridden by the user. The general purpose of a manual override is to separate physical I/O values and network communication from and to application values (e.g., logiCAD programs, application-specific control algorithms). By setting an override value regular parts that drive a data point's value are overridden. For example, the valve position in a heating system may be overridden and thus decoupled from the controller algorithm.

On the device, a manual override can be set and revoked manually on the Web interface or the LCD display. If a manual override value is active:

- Output data points write the manual override value to the network or the physical output. Output values written by an application to the data points are no longer reflected in the value cache and are not written to the network. The written application value is stored in a backup cache, which is applied to the data point again, as soon as manual override is revoked.
- Input data points are decoupled from the network or physical inputs and report the manual override value to the application. They are no longer updated by values received from the network or physical inputs.
- Value data points incorporate both semantics of output and input data points.

To set an override value, go to the details page of a data point, enter the value and click the **Set Override** button. The status **overridden** is displayed for a data point in override. To revoke the override value, click the **Clear Override** button. This restores the data point value to the last regular application value.

The Web interface menu **Data** – **Overridden Data Points** displays a list of all overridden data points on the device (see Figure 38). You can navigate to the details page of an overridden data point by clicking on the link. It is also possible to remove all override values at once by clicking the button **Clear override values**.

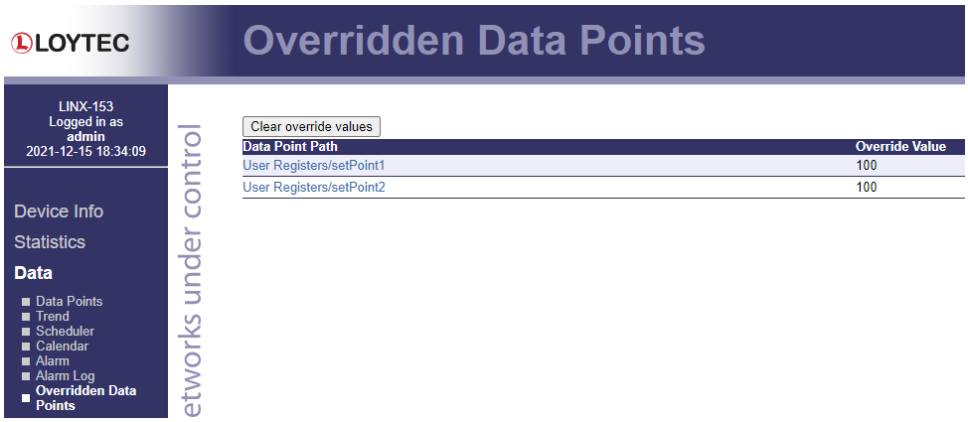


Figure 38: Overridden Data Point page.

3.3.4 Trend

The Web interface provides a trend log overview page to see all available trend logs and their current state (active, first available date/time, last date/time, number of records). An example is shown in Figure 39. This list allows a convenient upload of single trend data in CSV format by clicking on the respective icons. To upload an archive of all trend data, click on the **all** link in the **Download** column heading. It is also possible to purge single or all trend logs directly from that list.

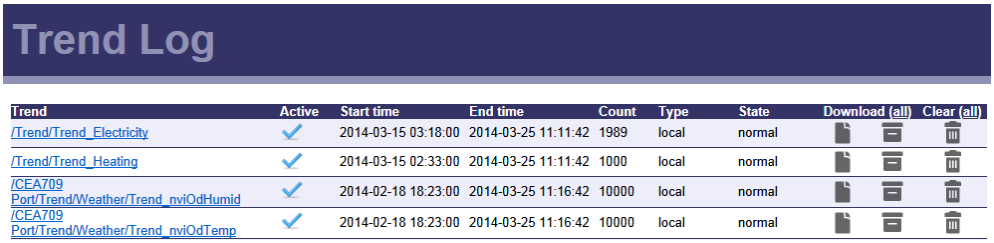


Figure 39: Trend log overview on Web UI.

Click on a trend log and re-configure local trend logs at run-time. The changes made to the trend logs take effect immediately without the needs for a reboot of the device. Allocating new trend logs can only be done in the configuration software. The trend log main page displays all available trend logs. Click on the trend log to be edited. This opens the trend log configuration page. An example is shown in Figure 40.

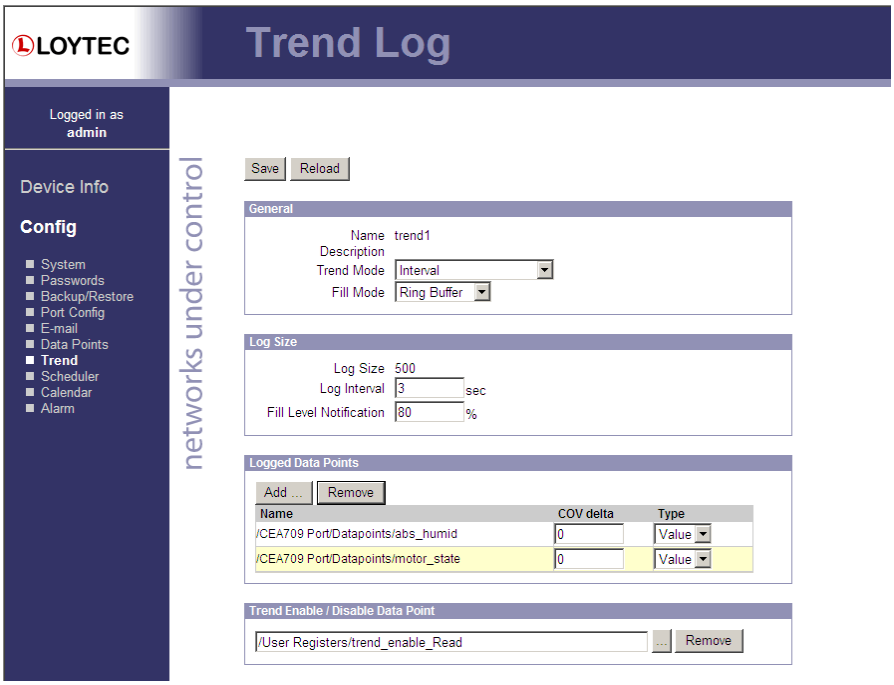


Figure 40: Trend log configuration page.

The user can change the **Trend Mode**, the **Fill Mode**, the **Log Interval** and the **Fill Level Notification**. Furthermore, data points can be added to the trend log by clicking the **Add…** button. A data point selector dialog opens. Click on a data point for adding it. For removing a data point from the trend log, click on it in the **Logged Data Points** list and hit the **Remove** button. Save the changes made by clicking the **Save** button. For more information on how a trend log can be configured please refer to the LINX Configurator User Manual [1].

To look at the historical trend data in a chart view select the **Preview** tab as shown in Figure 41. Trend logs with multiple data points are shown with multiple color-coded curves. A legend at the bottom of the page identifies the trended data points. Moving the mouse over the trend chart shows a data curser displaying time stamp and actual value.

Using the chart slider below the trend chart, one can zoom in and out in time as well as shift the time axis. Click into the slider and drag the mouse while keeping the button pressed in order to span a sub-interval, which is displayed in the chart view. Alternatively, select one of the pre-defined sub-intervals (week, day, etc.) and drag the sub-interval along the time axis.

Data points can be deselected in the legend at the bottom of the window. This hides the respective curves in the chart view and may improve visibility for certain detail. Enable the data points again and the curves will re-appear.

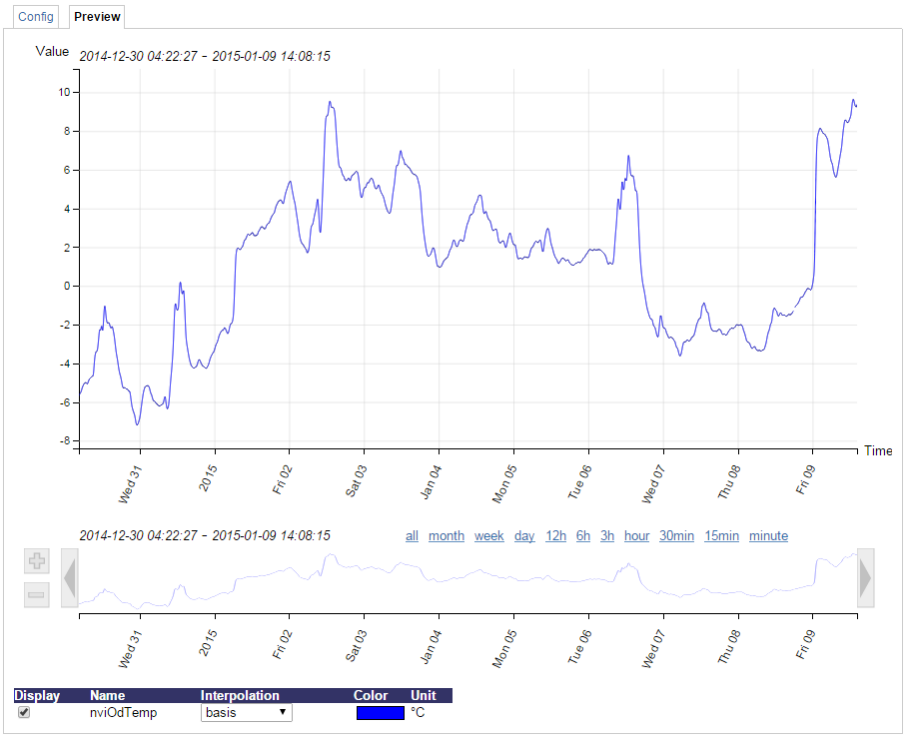


Figure 41: Web UI trend chart preview

3.3.5 Scheduler

The Web interface provides the scheduler page to edit its schedules at run-time, i.e., change the times and values that shall be scheduled. Allocating new schedules and attaching data points to those schedules can only be done in the configuration software. The scheduler main page displays all available schedules. Click on the schedule to be edited. This opens the scheduler page. An example is shown in Figure 42.

The **effective period** defines when this schedule shall be in effect. Leave **From** and **To** at '*.*.*' to make this schedule always in-effect. Otherwise select the desired start and/or end dates by clicking the calendar icons. To entirely disable a scheduler de-select the **Enable Schedule** check box.

Schedules are defined per day. On the left-hand side, the weekdays **Monday** through **Sunday** can be selected, or exception days from the calendar, e.g., Holidays. Once a day is selected, the times and values can be defined in the daily planner on the right-hand side. In the example shown in Figure 42, on Monday the value **Occupied** is scheduled at **8:00am**. The same principle applies to **exception days**. **Exception days** override the settings of the normal weekday. Put a check mark on those exception days from the calendar, which shall be used in the schedule. To edit the date ranges of exception days click on the links to the used calendars, e.g., 'calendar' or 'Scheduler_1'. The 'Scheduler_1' is a calendar, which is embedded into the schedule and not accessible by other schedulers. For more information on how to set up schedules and calendars refer to the LINX Configurator User Manual [1].

To define actual values for the names such as **Occupied** click on the tab **Presets** as shown in Figure 43. To define a new value, click on the button **Add Preset**. This adds a new column. Enter a new preset name (e.g., 'Occupied'). Then enter values for the data points in the **preset** column. The **data point description** column displays the short-hand name defined in the configuration software. This description can also be changed on the Web UI. Optionally, click on the color button in the **Preset Colors** line to select a color for that preset. This color is used on calendar views such as LWEB-802 or on the L-VIS.

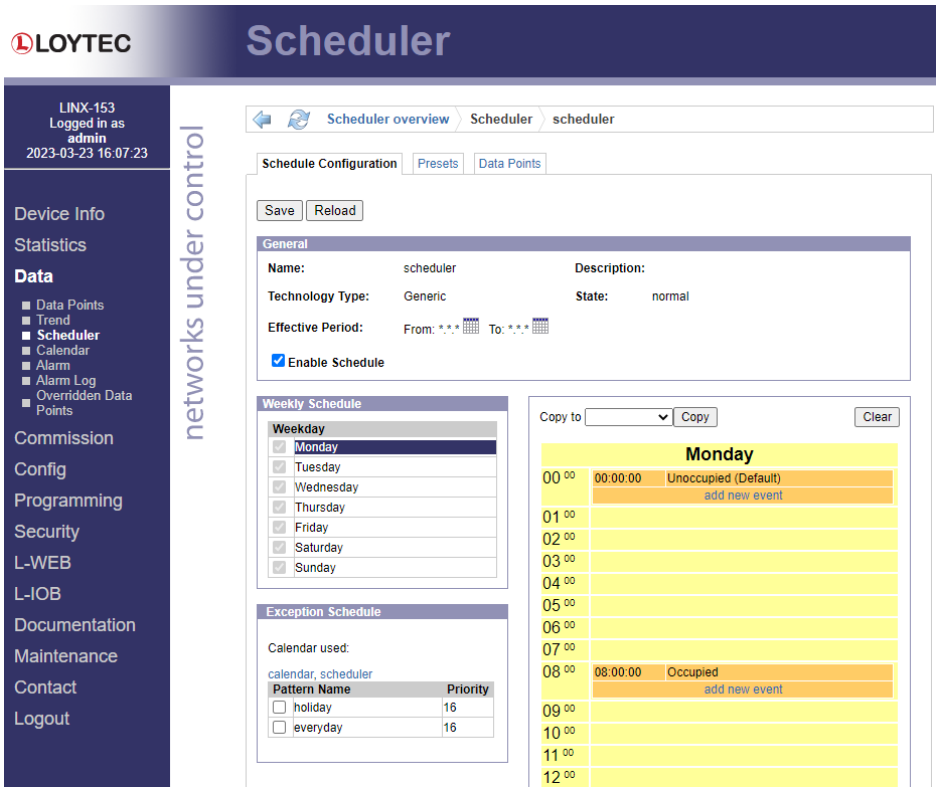


Figure 42: Schedule Configuration Page.

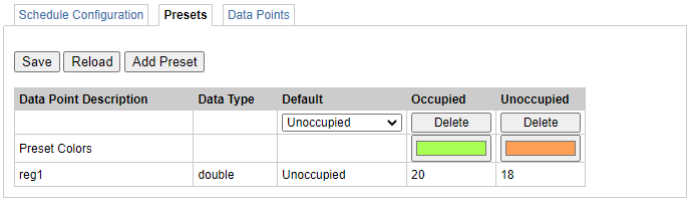


Figure 43: Scheduled Presets Configuration Page.

You can switch back and forth between the two tabs. Once the configuration is complete, click on the **Save** button. This updates the schedule in the device. Any changes made become effective immediately.

Note: *Clicking **Save** may remove any presets which are currently not used in any of the daily schedules. This happens for example in native BACnet schedules, where the underlying network technology cannot store presets individually. Therefore always complete the daily schedules first and then press save as the last step.*

For local schedulers using the CEA-709 network technology or generic schedulers, the Web UI also allows to reconfigure the scheduled data points. This change takes effect immediately without a reboot of the device. To add and remove data points to the scheduler, go to the **Data Points** tab. The configuration page is depicted in Figure 44. To add a new data point, click the **Add…** button. To remove a data point, select the data point in the list **Scheduled Data Points** by clicking on it and then press the **Remove** button. Finally, store the changes by clicking the **Save** button. After modifying the scheduled data points, go back to the Presets tab and enter descriptive value label names. For more information on how to configure a scheduler please refer to the LINX Configurator User Manual [1]. The **Revert** button rolls back any changes made locally to the data point configuration.

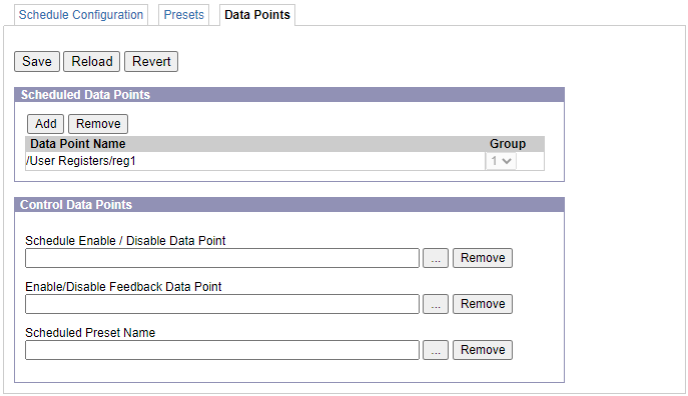


Figure 44: Re-configure scheduled data points on the Web UI.

3.3.6 Calendar

The Web interface provides the calendar page to edit its calendars at run-time, i.e. change the exception days. The calendar main page displays all available calendars. Click on the calendar to be edited. This opens the calendar configuration page. An example is shown in Figure 45.

The **effective period** defines when this calendar shall be in effect. Leave **From** and **To** at '*.*.*' to make this calendar always in-effect. Otherwise enter dates, such as '30.1.2000'.

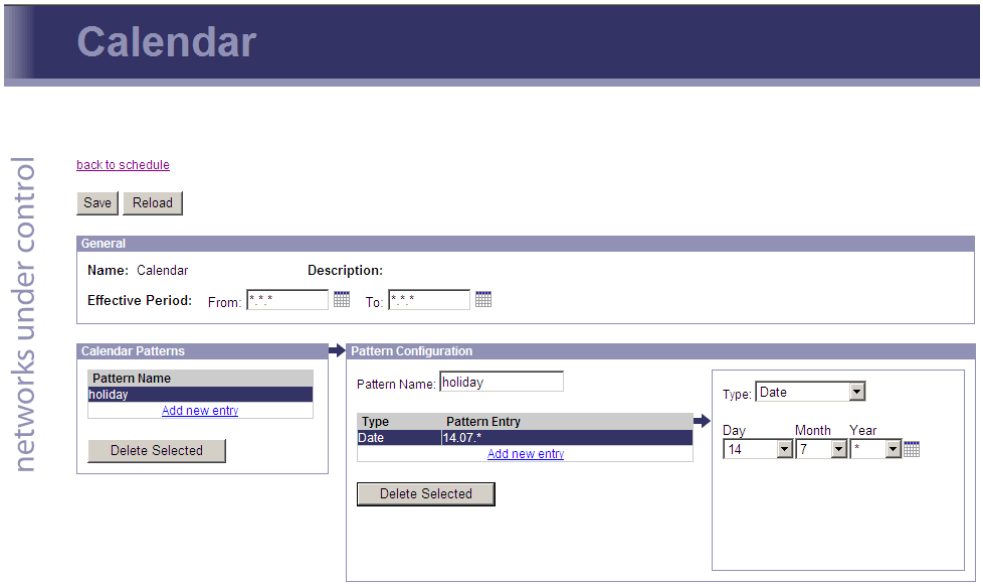


Figure 45: Calendar Configuration Page.

On the remainder of this page, work from left to right. Click on a calendar pattern or create a new calendar pattern by clicking **Add new entry**. A calendar pattern defines a set of pattern entries, which defines the actual dates or date ranges. In the example in Figure 45, the calendar pattern **Holidays** is selected.

In the **Pattern Configuration** box, the calendar pattern's name can be edited if supported by the underlying network technology. Otherwise, an auto-generated name will be assigned and the pattern name box is not shown. Below the pattern name is a list of the individual pattern entries. New entries can be added by clicking **Add new entry**.

Note:	*Embedded calendar patterns can only have exactly one entry to define the dates at which the pattern should be in effect. Only calendar patterns in global calendars may consist of multiple entries.*

Existing entries can be selected and edited in the box on the right-hand side. In the example in Figure 45, the date **14.7.*** is selected, which means “The 14.7. of every year”. Other entry types such as **Date Range** and **Week-and-Day** can be selected.

3.3.7 iCalendar Scheduler

Another type of scheduler is the iCalendar scheduler. This scheduler type is configured using calendar data in iCalendar format (ICS data) and is strictly event-based. The Web interface provides a typical calendar view known from Google or Outlook calendars and allows planning events to be scheduled.

The events can be single events or have a recurrence, such as “Weekly on Monday, every two weeks”. Each event is associated with a value preset that defines the scheduled value during that event. The event priority will resolve conflicts, if two or more events should overlap. Smaller numbers mean higher priority. For example: if two events overlap, tha have priorities 2 and 3, then the event with priority 2 will have precedence.

There are different views, including monthly, weekly, and daily as well as an event list view (see Figure 46). The list view shows all events in the underlying iCalendar data.

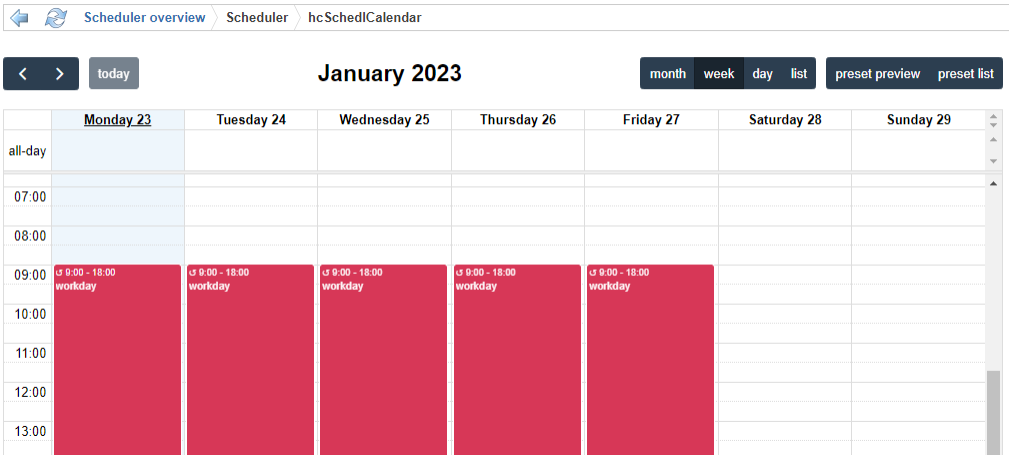


Figure 46: iCalendar configuration of events.

New events can be added by clicking the Create a new event button on the right-hand side of the calendar or by drag-and-drop one of the listed presets as shown in Figure 47. These events are added to the default local calendar. Click on the **Configure Presets** button to open the presets configuration tab as described in Section 3.3.5.

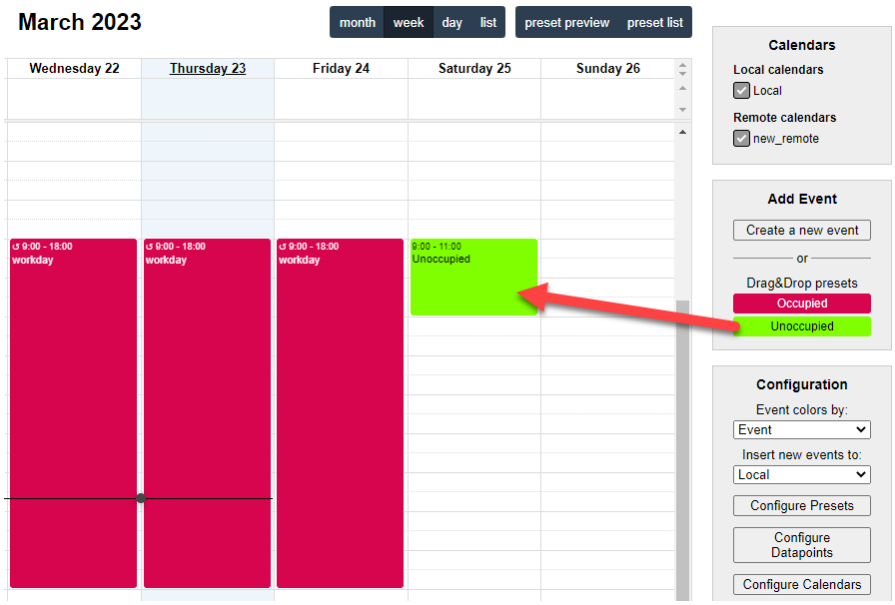


Figure 47: Creating a new event in an iCalendar scheduler.

There can be more than one iCalendar in the scheduler. The available calendars are listed in the upper right corner. Events of *local* calendars are created and stored on the device. In addition, *remote* calendars can be added by clicking on the **Configure Calendars** button. This opens the **iCalendar** configuration tab as shown in Figure 48.

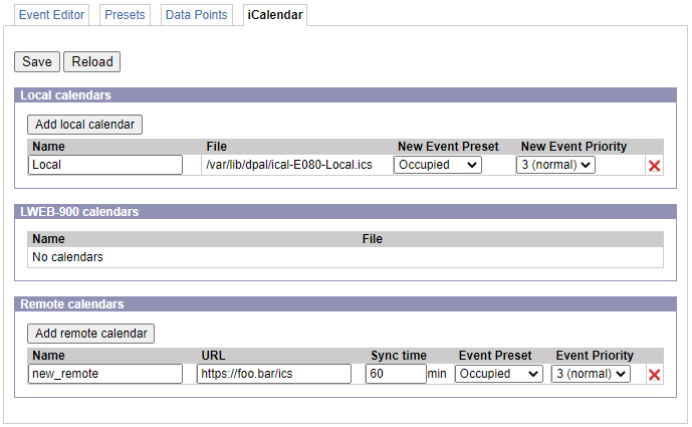


Figure 48: Create a new remote iCalendar.

Click on **Add remote calendar** to add a new remote calendar. A remote calendar fetches its ICS data from an external URL in a periodic fashion. Enter a **sync time** in minutes and select an **Event Preset** to be scheduled at the **Event Priority** for the events in the remote iCalendar. Examples for remote calendar URLs are Google calendar or Outlook 365 URLs.

3.3.8 Alarm

The Web interface provides the alarm page to view the currently pending alarms of its alarm data points. The alarm main page displays all available alarm data points. Alarm objects which have active alarms are displayed in red. Click on the alarm object to be viewed. This opens the alarm summary page. An example is shown in Figure 49.

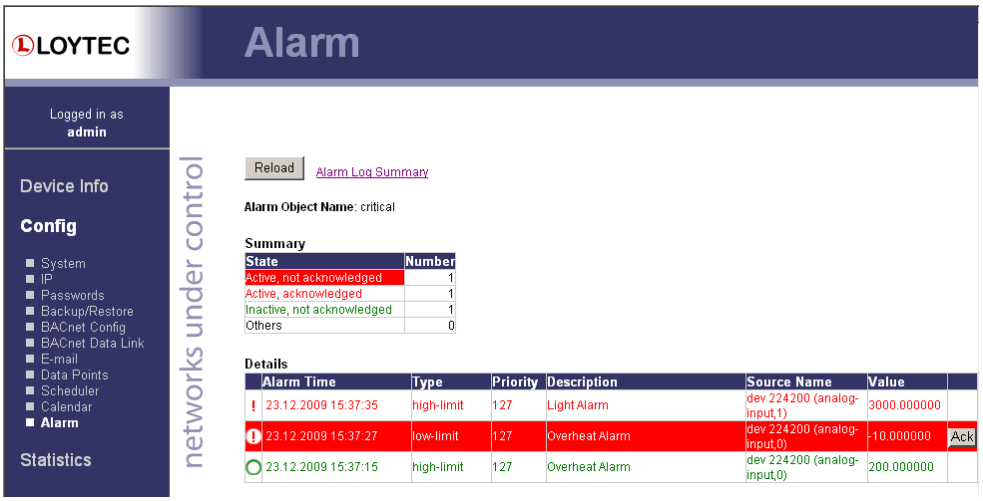


Figure 49: Alarm Summary Page.

Active alarms are highlighted red. Inactive alarms which have not been acknowledged are rendered in green. Alarms that can be acknowledged have an **Ack** button. Press on the **Ack** button to acknowledge the alarm. Depending on the technology, this and older alarm records will be acknowledged. Acknowledged, active alarms are rendered in red. Click on **Reload** to refresh your alarm list.

Inactive alarms that have been acknowledged disappear from the list. To record historical information about those alarms, the alarm log must be used. See Section 3.3.9 for the alarm log Web interface.

3.3.9 Alarm Log Page

The alarm log page provides an overview of all alarm logs on the system. Click on one of the links to view a specific alarm log. Each alarm log contains a historical log of alarm transitions. When an inactive and acknowledged alarm disappears from the alarm summary page (live list), the alarm log contains this last transition and maintains it over a reboot. An example is shown in Figure 50.

To refresh the alarm log contents click on the **Reload** button. Currently active alarms cannot be acknowledged in this historical view. Follow the link to the attached alarm objects to get to the respective live lists, where alarms can be acknowledged on the Web interface (see Section 3.3.8).

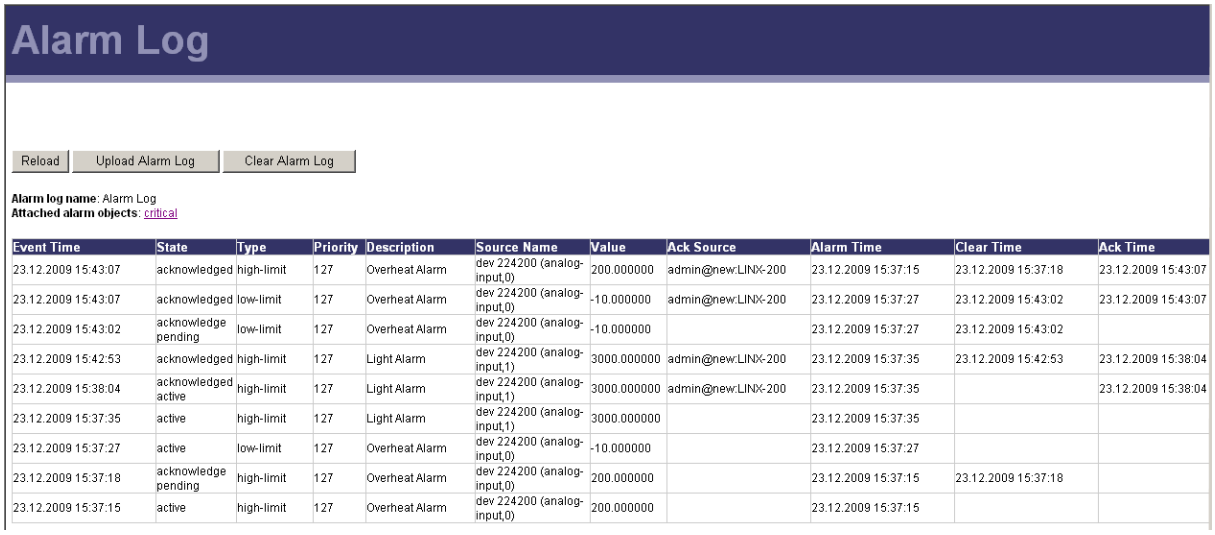


Figure 50: Alarm Log Page.

The alarm log contents can be uploaded from the device in a CSV formatted file. Click on the button **Upload Alarm Log** to upload the current log. To clear the log, press the button **Clear Alarm Log**. Please note, that this permanently purges all historical alarm log data of this alarm log.

3.4 Commission

3.4.1 BACnet

The commissioning Web UI allows assignment of physical devices to existing devices in the data point configuration, that have been created with the commission later option. Under the **Commission** menu choose the BACnet technology to open the BACnet commissioning interface.

The Web page shows a list of all **Devices in configuration**. An example is shown in Figure 51. Each line represents a device and shows the device name, the device **Instance** and the optional BACnet **Address**. The **Static Binding** checkbox defines, whether static device binding is configured for this device and requires a BACnet address. The **Status** column shows their current status. It can be one of the following:

- OK: The device is configured for communication.
- Offline: The device is configured for communication but appears offline.
- Uncommissioned: The device is not yet commissioned.
- Disabled: The device is disabled.

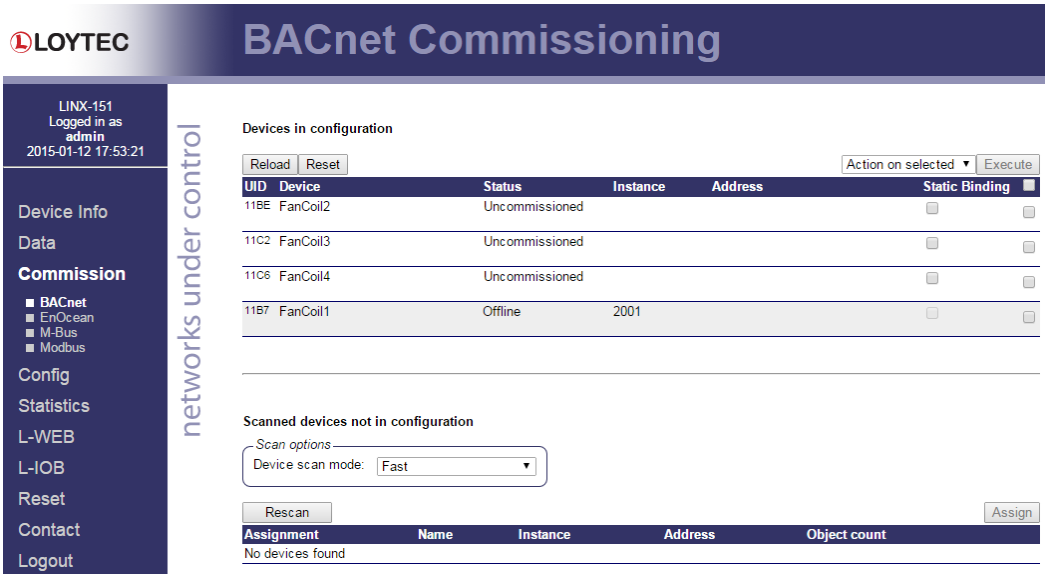


Figure 51: BACnet commissioning Web interface.

In order to execute an action on devices, select the checkbox at the end of the respective lines. Then choose an action in the drop-down **Action on selected** and click the **Execute** button. Actions that can be executed on all devices are enable and disable. A disabled device will stop communication on the network until it is enabled again.

Those devices created as commission later can be assigned to physical devices on the network. The device description displayed beneath the device name can be edited, where the edit symbol appears. The assignment can be done manually by editing the fields in the **Instance** column and **Address** column (for static device binding). It can also be done by

executing a network scan. Edit the scan options as appropriate for your BACnet network and click on **Rescan**. The scan progress will be displayed and fill the list for **Scanned devices not in configuration**. An example is shown in Figure 52.

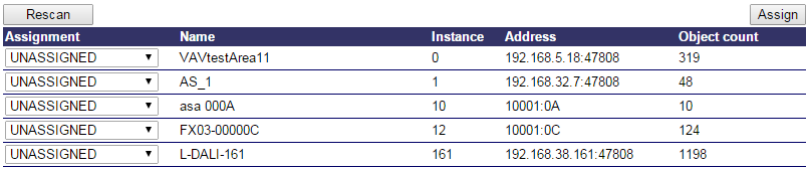


Figure 52: Result of a BACnet scan on the Web interface

To assign a scanned device to an uncommissioned device in the configuration, select the corresponding device name from the drop-down box in the **Assignment** column. Repeat that for all other devices and then click the button **Assign**.

3.5 Device Configuration

3.5.1 System Configuration

The system configuration page is shown in Figure 53. This page allows configuring the device's system time and other system settings. The **TCP/IP Configuration** link is a shortcut to the Ethernet port configuration. Follow that link to change the IP settings of the device.

The time sync source can be set to **auto**, **manual**, **NTP**, **BACnet**, or **LonMark**. In the auto mode, the device switches to the first external time source that is discovered. Possible external time sources are NTP, BACnet, LonMark. The option **manual** allows setting the time manually in the fields **Local Time** and **Local Date**. In **manual** mode, the device does not switch to an external time source. Note, that if **NTP** is selected, the NTP servers have to be configured on the IP Configuration page (see Section 3.11.1).

In order to use BACnet as the time source, a BACnet device (time master) must be configured to distribute time synchronization. For doing so, the BACnet address of the devices, which shall be synchronized, must be added to the device object of the BACnet time master (see Section 17.3.8). The device synchronizes automatically as soon as it is contacted by the BACnet time master.

The time zone must be defined independently of the time source. It can be chosen from the drop-down menu **Time Zone** or by typing a text, e.g., "Vienna", which refines the drop-down selection to those entries containing the text. Delete any entered characters to expand the drop-down selection to its full range again. The chosen time zone information automatically configures time zone offset and DST start/end. If the desired time zone information is not available, choose "manual". Then **Time Zone Offset** needs to be explicitly configured. It is specified as the offset to GMT in hours and minutes (e.g., Vienna/Austria is +01:00, New York/USA is -06:00). For setting the daylight saving time (DST) predefined choices are offered for Europe and USA/Canada. DST can be switched off completely by choosing **none** or set manually for other regions. In that case, start and end date of DST must be entered in the fields below. It is also possible to automatically configure timezone and DST for a specific region by the system settings in the Configurator (see the **Enable automatic Time Zone and DST** check box). In this case, the settings cannot be edited on this page.

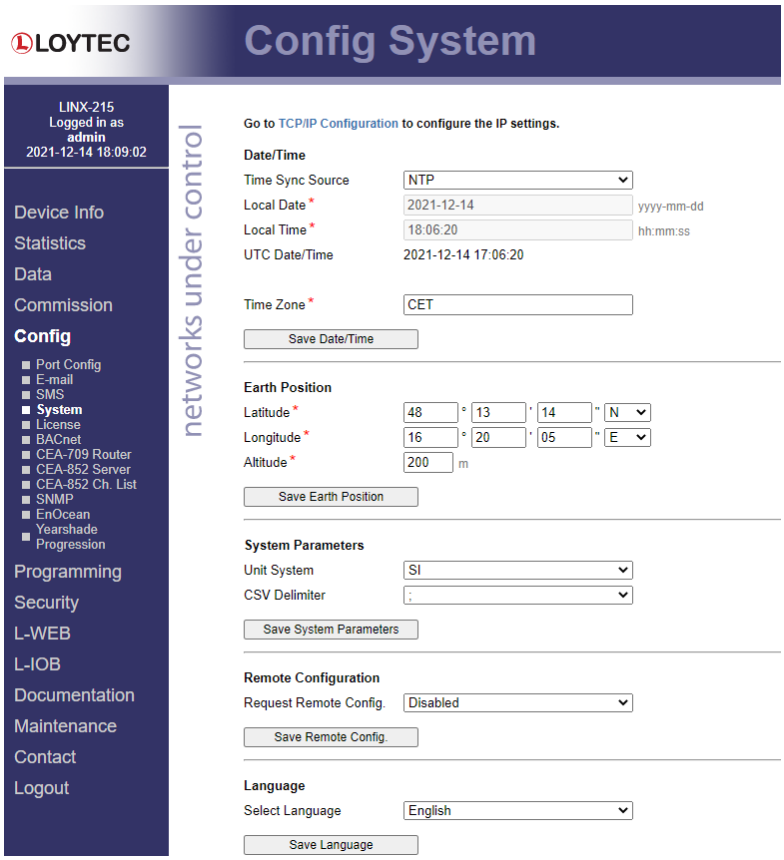


Figure 53: System Configuration Page, e.g., for Vienna, Austria.

The next section on the page allows configuring the device's earth position. This setting defines the longitude, latitude and elevation of the device. The latitude and longitude are entered as degrees, minutes, and seconds. The altitude is entered in meters height above sea level. This setting is used for an astronomical clock. For fixed locations such as a building, the position can be entered on this page. For moving locations, this setting can be updated over the network using the network variable nciEarthPos (see Section 17.2.1) or by writing to the corresponding system register.

The section **System Parameters** allows defining the displayed units and CSV delimiter. The unit system can be either SI or U.S. Depending on the chosen unit system, data point values will be presented in either SI or U.S. units.

Important! ***When changing the unit system, the device needs to be rebooted and will reset all persistent values to their default values converted to the chosen unit system.***

For generating CSV files for trend logs, alarm logs, etc., the delimiter for those CSV files can be configured. This setting can be changed between a comma ',' and a semi-colon ';'. The change takes effect immediately for all files generated by the device.

In **Remote Configuration** it can be configured, whether a replaced device shall automatically request its configuration from an LWEB-900 server. This remote configuration request is sent only, if the device does not have a data point configuration.

The **Language** setting allows changing the language of the Web interface. When changing the language setting it becomes effective immediately. Changing this setting is the same as changing language on the LCD display.

3.5.2 Port Configuration

This menu allows configuring the device's communications ports. For each communication port, which is available on the device and shown on the label (e.g., Port 1, Port 2 Ethernet), a corresponding configuration tab is provided by the Web UI. An example is shown in Figure 54. Each port tab contains a selection of available communication protocols. By selecting a checkbox or radio button the various protocols can be enabled or disabled on the communication port. Some ports allow exclusive protocol activation only, other ports (e.g., the Ethernet port) allow multiple protocols bound to that port.

When using L-STUDIO, some settings in the port configuration are set by deployment. A local edit is possible for experimenting but will be overwritten by the next deploy. A pop-up dialog warns about this fact when applicable.

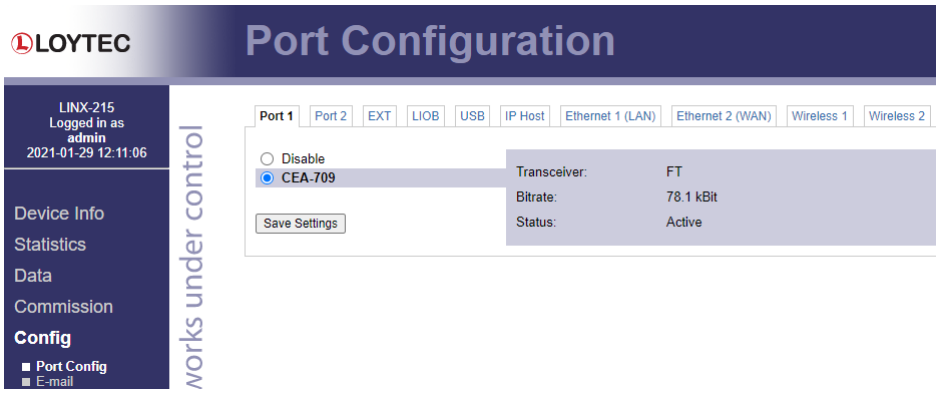


Figure 54: Port Configuration Page.

When selecting a protocol on a communication port, the protocol's communication parameters are displayed in a box on the right-hand side. To save the settings of the currently opened protocol, click the **Save Settings** button.

3.5.3 IP Configuration

The TCP/IP configuration is done under the Ethernet port tab as shown in Figure 55. The mandatory IP settings, which are needed to operate an IP interface the device, are marked with a red asterisk (IP address, netmask, gateway). The **Enable DHCP** checkbox switches between manual entry of the IP address, netmask, and gateway address, and automatic configuration from a DHCP server.

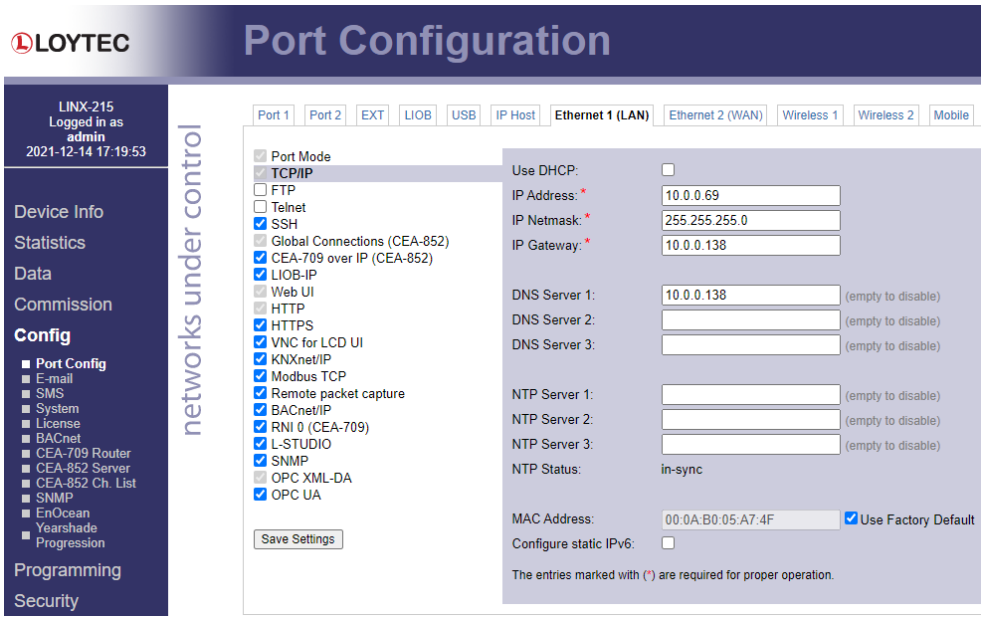


Figure 55: TCP/IP Configuration Page.

The device comes configured with a unique MAC address. This address can be changed in order to clone the MAC address of another device. Please contact your system administrator to avoid MAC address conflicts.

If the device is operated with a 10 Mbit/s-only hub, the link speed should be switched from **Auto Detect** to **10Mbps/Half-Duplex**. With modern 100/10 Mbit/s switches, this setting can be left at its default.

LOYTEC devices support IPv6 static configuration as of firmware 7.2.0. Normally, IPv6 uses auto-config that does not require a static setting (SLAAC or DHCPv6). If the network requires it, however, a static IPv6 address can be set at shown in Figure 56. Enable Configure Static IPv6 and enter the IPv6 address, e.g. “2001:0db8:0:f101::2”. Also define an IPv6 gateway. Note that only 64-bit subnets are allowed for static configuration.

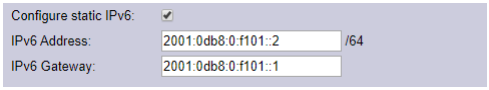


Figure 56: Static IPv6 Configuration.

The settings for DNS and NTP servers should be made in the IP host settings (see Section 3.5.6). In case an IP interface runs DHCP, the DNS and NTP addresses supplied by DHCP can be seen here. Models with one Ethernet port only do not have these settings here.

Other standard protocols that are bound to an Ethernet interface are SSH and HTTP (Web server). By deselecting the checkbox, those protocols can be individually disabled. The standard UDP/TCP ports can be changed in the respective protocol settings. An example for the SSH server is shown in Figure 57. The SSH server is used for instance to update the firmware (see Section 19.1) or to upload a new data point configuration. Note that HTTP for the Web server can only be disabled when using the Web interface over HTTPS or by using the device configuration of the Configurator.

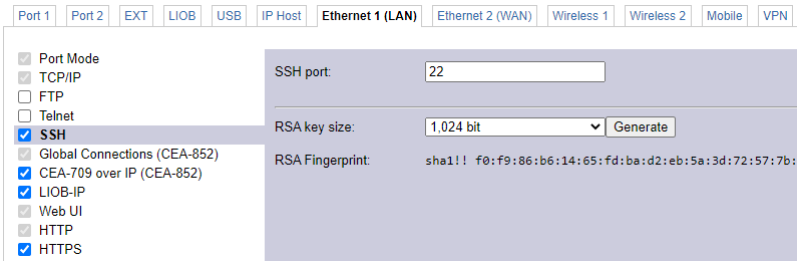


Figure 57: SSH server configuration on the Ethernet port.

3.5.4 Using Multiple IP Ports

On models with multiple IP interfaces, the port configuration provides a separate port tab for each IP port, e.g., **Ethernet 1 (LAN)** and **Ethernet 2 (WAN)**. In the port mode setting these interfaces can be enabled to operate as a separate IP network. As a default only **Ethernet 1 (LAN)** is enabled and configured to be switched with the Ethernet 2 port. To enable **Ethernet 2 (WAN)** as a separate, isolated IP network, choose **Separate network** in the port mode setting as shown in Figure 58 and save settings. A reboot is required to make this change effective.

For each IP interface configured as a separate network, the various standard protocols can be enabled separately. As a default, the secure protocols HTTPS, SSH and OPC UA are enabled on a new separate IP interface. Some protocols can be enabled on multiple interfaces at the same time, others on one interface only. If one of the latter is enabled on a new separate IP interface, a warning will be displayed, stating on which other interface the protocol will now be disabled (e.g., CEA-709 over IP, BACnet/IP, KNXnet/IP).

The separate network mode can be used, if you want to operate an isolated building network on the LAN and expose some aspects outside the building network (denoted as WAN). This configuration can also be used to operate a gateway between two otherwise entirely separate building network domains, e.g. BACnet/IP on the Ethernet 1 port and KNXnet/IP on the Ethernet 2 port. Physically, the two Ethernet ports will be plugged into different Ethernet switches.

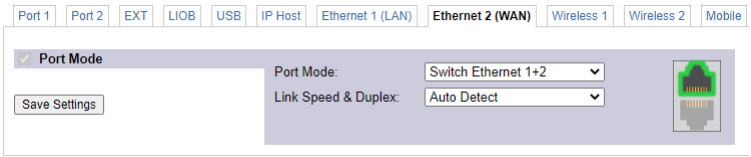


Figure 58: Enable the Ethernet 2 (WAN) interface.

To disable a separate IP interface, choose **Disable** in the port mode setting. This change is effective immediately without a reboot. To configure switch mode again, choose **Switch Ethernet 1+2** in the port mode setting.

3.5.5 802.1X Port Authentication

To further increase security in a network installation, IT departments support the 802.1X port authentication method. This standard requires a device to authenticate its port on the network switch, before traffic into the network is allowed.

LOYTEC devices can enable 802.1X port authentication in the **Port Mode** settings on the **Ethernet** tabs of the port configuration (see Figure 59). Set the checkbox **Enable 802.1X**. Then choose an authentication **EAP Type** required by your IT department. The following EAP types are supported:

- **Protected EAP (PEAP)**: For this type define an inner **Authentication** method (e.g., MSCHAPv2) and **Username** and **Password**. Anonymous identity and CA certificate of

the Radius server are optional. The latter is needed if the Radius server shall be authorized.

- **Tunneled TLS (TTLS)**: For this type define an inner **Authentication** method (e.g. PAP) and **Username** and **Password**. Anonymous identity and CA certificate of the Radius server are optional. The latter is needed if the Radius server shall be authorized.

- **EAP-TLS**: This type is fully certificate-based. It is required to define the **Identity** (cleartext name of the client) and a matching **User certificate** needs to be installed. This certificate is typically issued by the Radius server and is password-protected. To upload the user certificate, click on the **Choose File** button next to **User Certificate** and select the certificate file. Both certificate formats, PEM and PFX are supported. The name is then printed out and the **Key Password** is prompted. Enter the password and click **Save Settings** to store the certificate on the device.

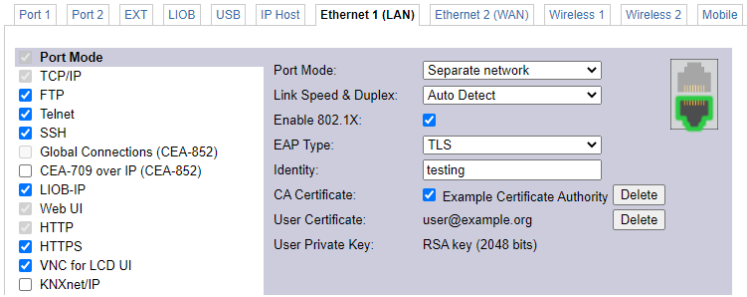


Figure 59: Configure 802.1X port authentication.

To delete any of the installed certificates, click on the **Delete** button next to it. Then another certificate may be installed by clicking the **Choose file** button. The selected file is noted next to the button. Click **Save Settings** to store the selected certificates.

3.5.6 IP Host Configuration

The L-INX models, which provide a built-in Ethernet switch/hub possess a separate **IP Host** tab for editing all common host settings as shown in Figure 60. These settings affect all IP interfaces on the entire device. On models with a single Ethernet port, the IP Host settings appear directly on the Ethernet tab.

Hostname and **Domainname** are optional entries and can be left empty. For some DHCP configurations it may be necessary to enter a hostname. Please contact your system administrator on how to configure DHCP to acquire an IP address.

If the device possesses more than one IP interface the **Default Gateway** setting defines the gateway of a given IP interface, which is going to route all non-local network traffic. One of the existing IP interfaces with a separate network must be selected here.

If the option **Internet connection sharing** is enabled, the device serves as a NAT router to the Internet. This enables devices on the LAN to access the Internet over this NAT router. In this case, the **Default Gateway** needs to point at the IP interface that is connected to the Internet. For example, set the default gateway to **Mobile**, if the Internet connection runs over an LTE-800. On the LAN devices, however, the gateway IP needs to point at the LAN IP address of this NAT router device. Those LAN devices will then be able to establish connections to the Internet over this NAT router.

Up to three **DNS Servers** can be defined on this page. These DNS servers will be contacted by all services on any of the IP interfaces for name resolution. In case the DNS servers are supplied by DHCP running one of the IP interfaces, change the setting **Use DNS servers from** to point to that interface.

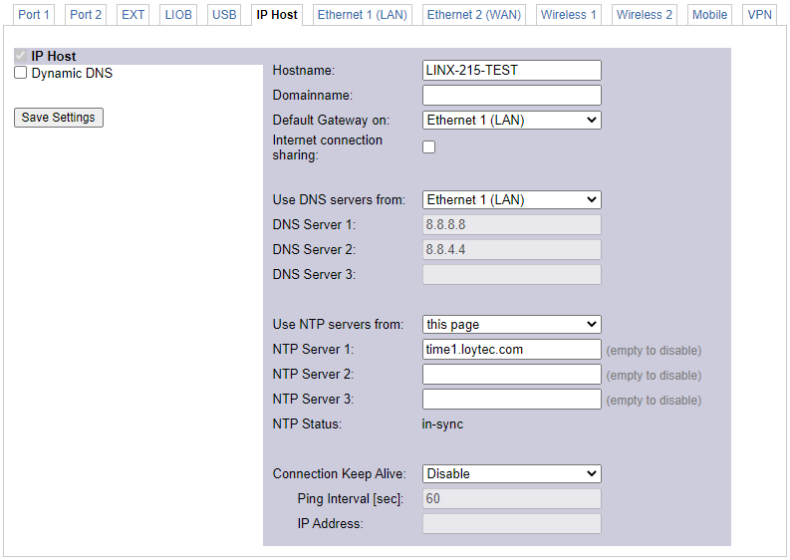


Figure 60: Setting on the IP Host tab.

The device can be configured to synchronize its clock with NTP time. Enter the IP address of a primary and, optionally, a secondary and tertiary NTP server (the address can also be an IPv6 address). The device will use NTP as a time source if the time sync source in the system configuration page is set to **NTP** (see Section 3.5.1). Note, that if using more than one NTP server, it is recommended to specify three NTP servers. The field **NTP status** below the NTP server settings displays the current NTP synchronization status (**out-of-sync**, or **in-sync**). The settings made here apply to all IP interfaces. In case the NTP servers are supplied by DHCP running one of the IP interfaces, change the setting **Use NTP servers from** to point to that interface.

The **Connection Keep Alive** feature allows the device to automatically ping other devices on the IP network in order to maintain an IP connection that might be automatically disconnected after a specific period of time (e.g., DSL routers automatically disconnect if no activity is detected). When enabled choose one of the options Auto IP or Custom IP.

If auto IP mode is selected and the device has a CEA-852 configuration server, a ping message is sent to all CEA-852 devices in the channel list of the configuration server. If the configuration server is disabled on this device a ping message is sent to the configuration server for the IP-852 channel, if one is known. If custom IP is selected, one specific IP address can be configured as the ping destination.

3.5.7 Dynamic DNS Configuration

LOYTEC devices can be configured to register for a dynamic DNS service. The settings are made in the **Dynamic DNS** protocol details field on the **IP Host** tab of the port configuration as shown in Figure 61. Select the **Provider** your domain name has been registered with and fill in the provider-specific details in the fields below. Typically, this will include the registered **Domainname** or URL and a password or security token.

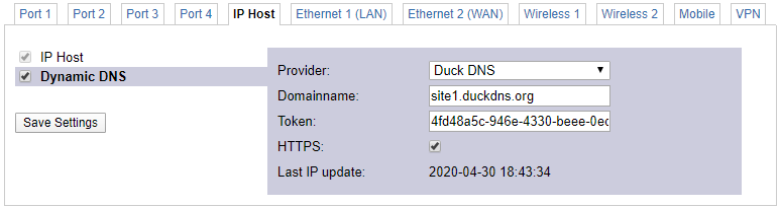


Figure 61: Dynamic DNS Settings

The interval of the dynamic DNS address check is 300 seconds. If an address change is detected, then the IP address is updated with the dynamic DNS provider. That time is reflected in **Last IP udate**.

3.5.8 WLAN Configuration

Devices supporting the LWLAN-800 wireless adapter can be connected to IEEE 802.11 wireless networks. The basic functions available in WLAN operation are described in Section 18.8. Depending on the required wireless modes, select the **WLAN Client** or the W**LAN Access Point** tab. The first configuration step is to enable the **Wireless** protocol on the respective tab of the port configuration, as shown in Figure 62.

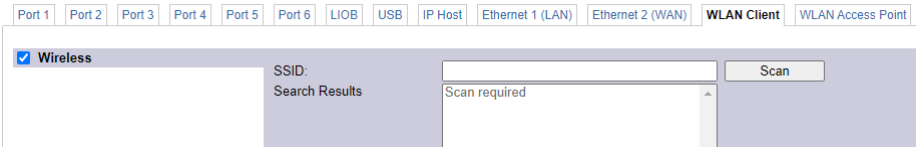


Figure 62: Enable Wireless protocol

WLAN Client tab: This tab allows configuring the WLAN interface in client mode. In this mode the WLAN client connects to an existing access point. A wireless interface in client mode has the settings shown in Figure 63.

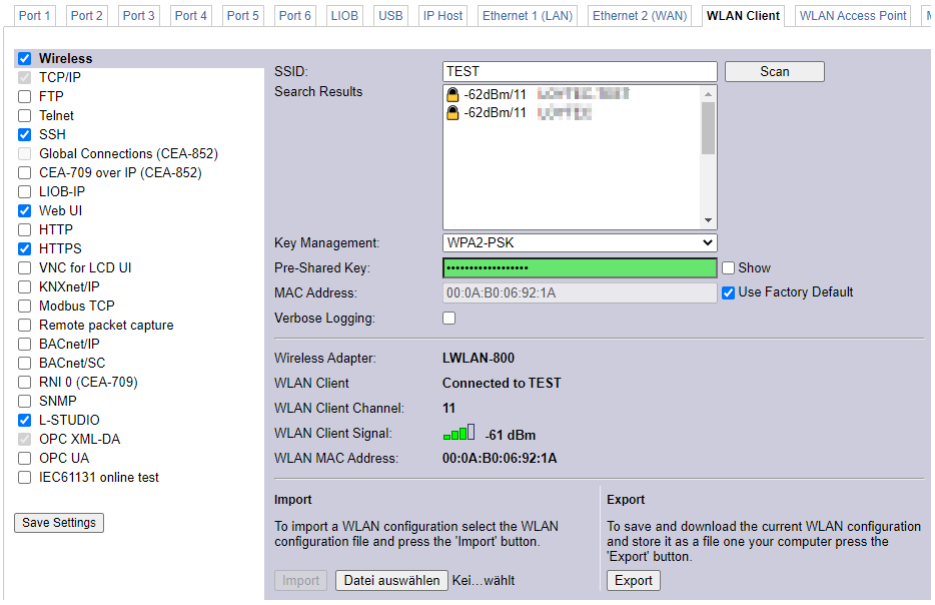


Figure 63: WLAN Client Settings

The following settings are used to configure the wireless client mode:

- **SSID**: This is the service set ID identifying the wireless network to connect to. It can be entered manually, e.g. if the network is hidden, or scanned using the **scan** button. Note that scanning interrupts an active wireless connection, so use this button only when setting up the wireless connection.

- **Search Results**: The search results list contains the discovered SSIDs and signal strenghts. Selecting one of the items copies it into the SSID field.

- **Key Management**: This list selects between NONE (no encryption), WEP, WPA and WPA2 encryption. The recommended setting is WPA2, as WPA and WEP are not considered secure anymore and are provided for backwards compatibility.

- **Pre-Shared Key**: The preshared key is the encryption key for the wireless network. The **show** checkbox shows the PSK in clear text.

- **Verbose Logging**: In case of connection problems, this checkbox can be activated to store wireless connection information in the OS log. It is not recommended to leave this option activated during normal operation.

The page displays the following information:

- **Wireless Adapter**: The type of the connected wireless adapter.

- **WLAN Client**: Displays whether the interface is connected to a wireless network.

- **WLAN Client Channel**: Displays the wireless channel.

- **WLAN Client Signal**: Displays the signal strength.

- **WLAN MAC-Address**: Displays the MAC address of the wireless adapter

WLAN Access Point tab: This tab allows configuraing a WLAN access point or a mesh point by choosing from the **Wireless Mode** drop-down:

- Access Point: The device provides a WLAN access point where a client can connect to the wireless network created by the device.

- Mesh Point: This mode is used to create an IEEE 802.11s mesh network (see Section 3.5.9).

An access point has the settings shown in Figure 64.

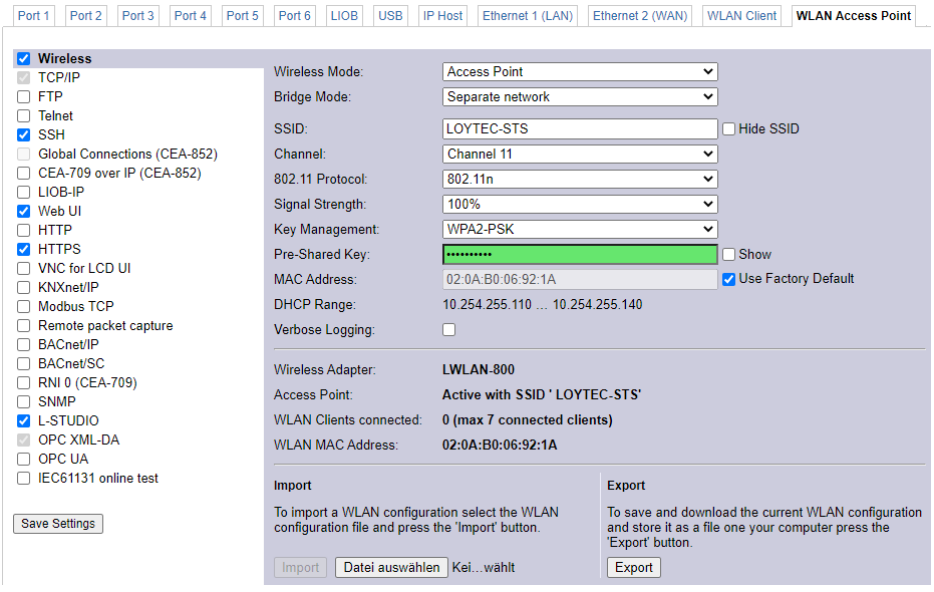


Figure 64: WLAN Access Point Settings

The following settings are used to configure the access point mode:

- **Bridge Mode**: The access point can be operated ether as a separate network or bridged to Ethernet 1. After having configured the access point, the IP settings have to be set, if the wireless port is configured as a separate network in a similar way as for Ethernet interfaces described in Section 3.5.4. For an access point in separate network mode, the IP address and netmask are used to define the network in which

client get an IP address from the built-in DHCP server. DNS and NTP settings are not needed in this mode.

- **SSID**: This is the service set ID identifying the wireless network provided by this access point. The **hide SSID** checkbox hides the SSID, so that it cannot be scanned. Not that hiding an SSID has more security drawbacks than advantages, so that this setting should be left deactivated.

- **Channel**: This field selects an available channel. The 2.4 GHz Band provides 11 channels. However these channels overlap and cannot be used without interference. When possible, use channels 1, 6 or 11 to avoid overlapping networks.

- **802.11 Protocol**: This field selects the wireless protocol to use. The default and recommended setting is 802.11b/g/n, which provides all protocols. If there are compatibility issues with some clients, the access point can be restricted to 802.11b/g or 802.11b.

- **Signal Strength**: This list selects the transmission signal strength between 5 to 100%. It can be used to reduce the signal strengh, if interference with nodes farther away shall be minimized. Ususally, it will be left at the default 100%.

- **Key Management**: This list selects between NONE (no encryption), WEP, WPA and WPA2 encryption. The recommended setting is WPA2, as WPA and WEP are not considered secure anymore and are provided for backwards compatibility.

- **Pre-Shared Key**: The preshared key is the encryption key for the wireless network. The **show** checkbox shows the PSK in clear text. For a secure network, please use WPA2, AES encryption and a PSK with at least 16 characters.

- **Verbose Logging**: In case of connection problems, this checkbox can be activated to store wireless connection information in the OS log. It is not recommended to leave this option activated during normal operation.

The page displays the following information:

- **Wireless Adapter**: The type of the connected wireless adapter.

- **WLAN Access-Point**: Displays status of the access point.

- **WLAN Clients connected**: Displays the number of connected WLAN Clients.

- **WLAN MAC-Address**: Displays the MAC address of the wireless adapter.

The buttons in the bottom area allow to export and import the wireless configuration. This allows to configure a device and to easily transfer the wireless settings to other devices. The **Export** button allows to save a file containing the wireless settings. The **Import** button imports a wireless configuration which has been selected by the **Browse** button. After changing the wireless settings, you need to click on **Save Settings** and reset the device for applying the settings.

Important! ***The LWLAN-800 supports a combined maximum of 7 connected clients.***

3.5.9 Mesh Configuration

Devices that support the LWLAN-800 adapter over USB or have a built-in WLAN interface can be configured to build a Mesh network following the IEEE 802.11s standard. The basic functions for operating a Mesh network are described in Section 18.8.2 in more detail. The

mesh network can be configured on the **WLAN Access Point** tab. The **Bridge Mode** and **TCP/IP** settings in the port configuration for a Mesh network are configured the same way as described for the access point configuration in Section 3.5.8. The configuration settings for the Mesh Point or Mesh Portal mode are shown in Figure 65.

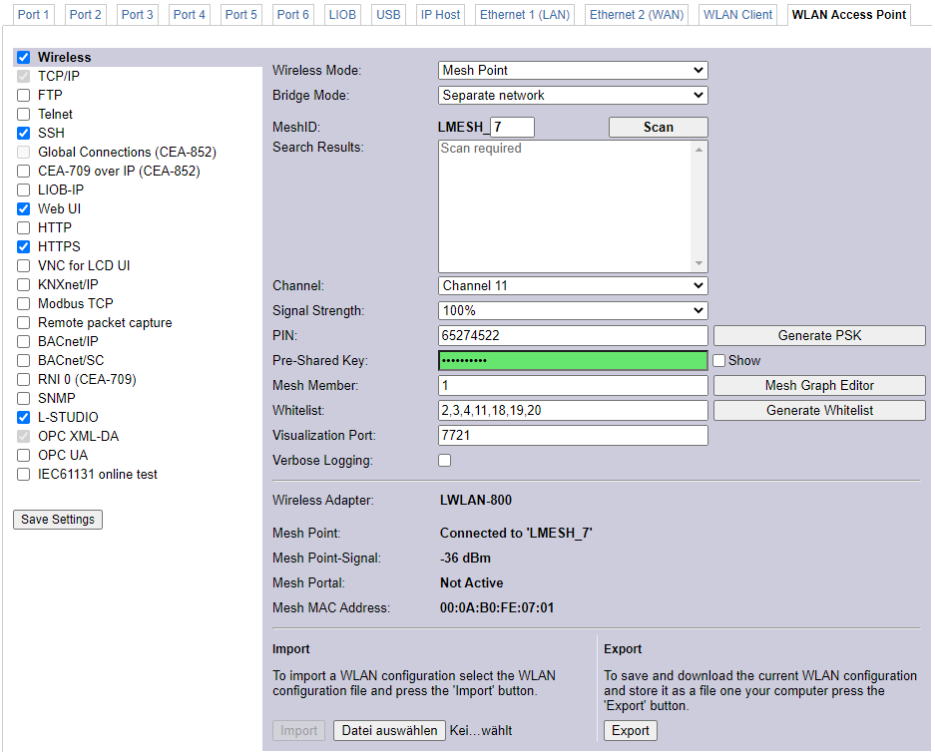


Figure 65: WLAN Mesh Network Settings

The following settings are required to configure a Mesh Point:

- **Wireless Mode**: Select **Mesh point** to configure the interface as a Mesh point.
- **Bridge Mode**: The Mesh point can be operated ether as a separate network or bridged to Ethernet 1. After having configured the Mesh point, the IP settings have to be set, if the wireless port is configured as a separate network in a similar way as for Ethernet interfaces described in Section 3.5.4.
- **MeshID**: The Mesh ID identifies the wireless network, which the device shall connect to. It can be entered manually or scanned by clicking the Scan button, which searches for available Mesh networks. Please note that a scan interferes with the normal operation of an existing connection. Therefore a scan should only be started in the setup phase of the network. Valid IDs are in the range between 1 and 255.
- **Search Results**: This list shows the scanned Mesh networks, the radio channels in use and their signal strength. By selecting an entry in this list, the respective settings are accepted.
- **Channel**: This field selects a radio channel. The 2.4 GHz band has 11 channels. These channels, however, may overlap. Therefore not all of tem can be used without interference. When possible, choose the channels 1, 6, and 11 in order to avoid overlaps. All Mesh nodes in the network must use the same channel.
- **Signal Strength**: This field allows setting the transmission signal strength between 5 and 100%. It can be used to reduce the signal strengh, if interference with nodes farther away shall be minimized. Ususally, it will be left at the default 100%.

- **PIN**: This field is used to choose an 8-digit PIN code. The **Generate PSK** button generates a 64-digit pre-shard key from this PIN code. The PIN code also makes Mesh setup easier on the LCD display.

- **Pre-Shared Key**: This field defines the password for the Mesh network. By selecting the check box **show** the password is shown as clear text.

- **Mesh Member**: This field configures the Mesh Point ID. This ID must be unique for each Mesh ID domain. The button **Generate Whitelist** can be used to generate a default whitelist. Valid Mesh Point IDs are in the range between 1 and 20.

- **Whitelist**: This field allows configuration of up to 7 mesh point IDs, which are allowed to communicate with this Mesh Point. The button **Mesh Graph Editor** opens a graphical editor for a simplified configuration of whitelists in the Mesh network.

Important! ***The LWLAN-800 supports a combined maximum of 7 connected Mesh points.***

- **Visualization Port**: This field configures the UDP port used for the Mesh network visualization. Entering '0' in this field deactivates the visualization traffic.

- **Verbose Logging**: In case of connection problems, this checkbox can be activated to store wireless connection information in the OS log. It is not recommended to leave this option activated during normal operation.

Following the settings the following information is displayed:

- **Wireless Adapter**: The type of the connected wireless adapter.

- **Mesh Point**: Displays whether the interface is connected to a mesh network..

- **Mesh Point Signal**: Displays the signal strength.

- **Mesh Portal**: Indicates whether this is a mesh point or portal.

- **Mesh MAC-Address**: Displays the MAC address of the wireless adapter.

The buttons in the bottom area allow to export and import the wireless configuration. This allows to configure a device and to easily transfer the wireless settings to other devices. The **Export** button allows to save a file containing the wireless settings. The **Import** button imports a wireless configuration which has been selected by the **Browse** button. After changing the wireless settings, you need to click on **Save Settings** and reset the device for applying the settings.

Mesh Graph Editor. This is a visual editor to assist a simple configuration of whitelists in the Mesh network as shown in Figure 66 and Figure 67. Depending on the configuration of Mesh points and connections between them in the Mesh graph, the resulting whitelist for this Mesh network graph is displayed. When changing the Mesh graph this list is updated. The following operations are available:

- Add a Mesh-Point: Clicking on the unused space of the graph editor creates a new Mesh Point. A new Mesh Point ID is assigned using the lowest available ID. Up to 20 Mesh Points can be added to the graph editor.

- Add a connection: A new connection is created by dragging a Mesh Point and dropping it onto another Mesh Point. This connection is represented by the Mesh Point ID in the respective whitelists of the affected Mesh Points. The limit of 7 connections of a Mesh Point is enforced by the editor.

- Delete a Mesh Point/connection: Select a Mesh Point or a connection by clicking on it. Then press the DEL key. By pressing the ESC key the selection is removed.
- Change a Mesh Point ID: Double-click on a Mesh Point and enter a new Mesh Point ID.
- Change the graph layout: By holding the CTRL key Mesh Point can be moved around in the graph in order to adapt the graph to the actual layout on site.
- Add a floorplan: By clicking the button **Load Floorplan** graphics can be loaded from a .jpg or .png file as a floorplan. By holding the CTRL key and clicking on the background the floorplan can be adapted to your needs.
- Scaling the floorplan: The drop-down box beneath the floorplan allows selecting a scale factor.

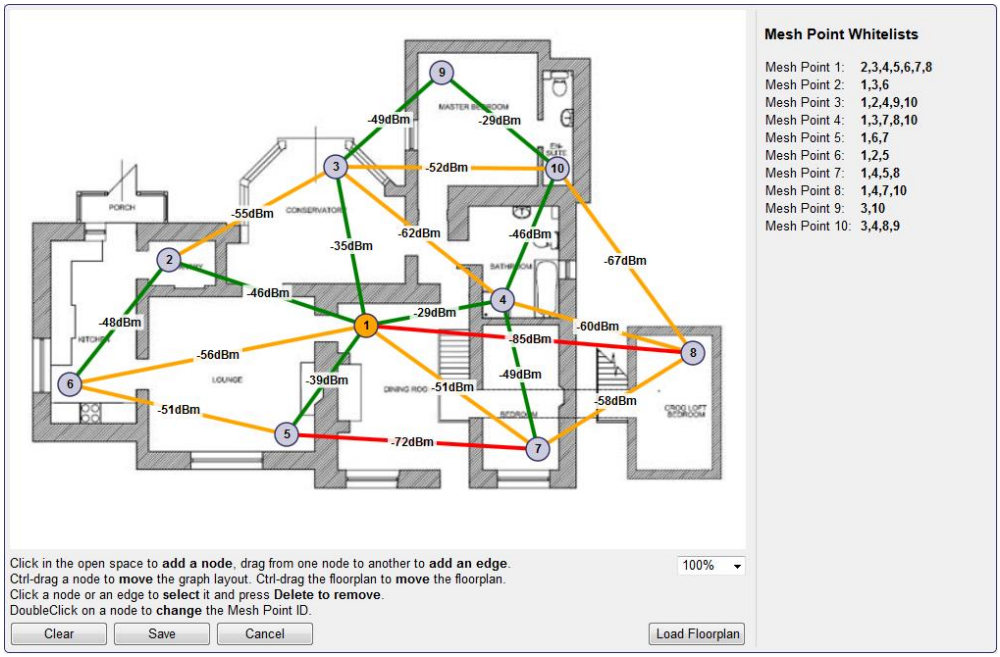


Figure 66: Mesh floorplan and online link monitor.

By using a floorplan in the Mesh graph the local layout of the building can be considered when configuring the Mesh network. Figure 66 shows the Mesh network visualization using a floorplan from the top view of the building. In contrast Figure 67 shows an overview plan of a building with five floors from the side view. If Mesh network visualization over UDP has been activated, the current signal strength between the Mesh points is added to the view. The connections are colored depending on the signal strength. Green stands for a good connection over -50 dBm, orange stands for a medium connection of about -50 dBm to -70 dBm and red stands for a weak connection under -70 dBm. By looking at the color-coded connection it is fairly easy to identify weak connections and go forward to troubleshoot weak spots in the configuration.

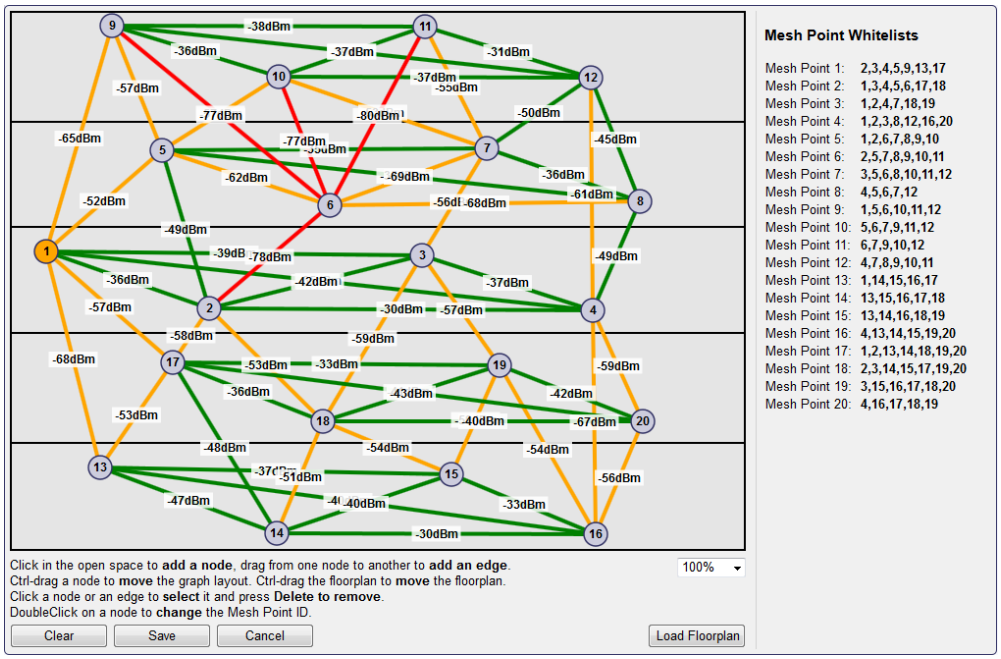


Figure 67: Mesh floorplan from side view and online monitor

Mesh Point Statistics. Weak performance or bad reliability in a Mesh network can have several reasons. One of them is a badly integrated Mesh point in the Mesh network. Such a weak point is revealed by bad connections to other Mesh points. Figure 68 shows Mesh point statistics of directly connected Mesh points. The statistics data provides information on Mesh point ID, MAC address, received and transmitted data, the signal strength, authentication status and time of inactivity.

wlan0 statistics

Stat	ID	MAC Address	rx packets	tx packets	signal	auth	inactive
OK	2	00:0a:b0:fe:01:02	10435681	5091712	-41 dBm	yes	50 ms
OK	3	00:0a:b0:fe:01:03	13903907	4988993	-34 dBm	yes	0 ms
OK	4	00:0a:b0:fe:01:04	9985008	1168027	-35 dBm	yes	52 ms
OK	5	00:0a:b0:fe:01:05	17549885	3258223	-46 dBm	yes	115 ms
OK	9	00:0a:b0:fe:01:09	13153658	3565334	-66 dBm	yes	56 ms
OK	13	00:0a:b0:fe:01:0d	13119289	2789844	-68 dBm	yes	46 ms
OK	17	00:0a:b0:fe:01:11	16381305	4039893	-65 dBm	yes	57 ms

Figure 68: Mesh Point Statistics

One of the most important values are the signal strength and the authentication status. The authentication status should always indicate successful authentication under normal operation and the signal strength should be no less than -70 dBm for a reasonable connection.

Mesh Path Statistics. The Mesh path statistics shown in Figure 69 provide information on the Mesh paths to all Mesh points in the Mesh network. Each line shows a Mesh path with the receiver Mesh point ID. Additionally, the Mesh point ID of the neighboring node is given for the respective path, to which packets are forwarded in order to reach the addressed receiver Mesh point. More statistics information are the Mesh path metric, the sequence number, the expiration period, the buffered packets and the state of the Mesh path.

Mesh Path wlan0

Stat	Dest	Next	Metric	Seq-Nr.	EXPTIME	QLEN	State
OK	2	2	127	121732	6129	0	active sn_valid resolved
OK	3	3	114	136167	6140	0	active sn_valid resolved
OK	4	2	241	134656	6129	0	active sn_valid resolved
OK	5	5	152	209313	6130	0	active sn_valid resolved
OK	6	5	266	194005	6130	0	active sn_valid resolved
OK	7	5	304	194300	6091	0	active sn_valid resolved
OK	8	5	266	159739	6116	0	active sn_valid resolved
OK	9	9	114	212555	1224	0	active sn_valid resolved
OK	10	9	228	171918	1127	0	active sn_valid resolved
OK	11	5	456	205989	6106	0	active sn_valid resolved
OK	12	5	456	181552	6099	0	active sn_valid resolved
OK	13	13	114	201133	6138	0	active sn_valid resolved
OK	14	13	228	186150	6096	0	active sn_valid resolved
OK	15	13	380	202138	6128	0	active sn_valid resolved
OK	16	13	266	183393	6112	0	active sn_valid resolved
OK	17	17	114	200096	6142	0	active sn_valid resolved
OK	18	13	342	179770	6118	0	active sn_valid resolved
OK	19	3	266	195569	6140	0	active sn_valid resolved
OK	20	13	456	178536	6138	0	active sn_valid resolved

Figure 69: Mesh Path Statistics.

The most important figures are the Mesh path metric and the state of the Mesh path. The Mesh path metric reflects the path quality from the Mesh point to the receiver Mesh point. The smaller the path metric the better the connection quality to the receiver Mesh point. A value larger than 500, however, should not be reached. In this case the Mesh point whitelist should be optimized for this Mesh path. For normal operation the Mesh path state should always read ‘active’, ‘sn_valid’ or ‘resolved’. This indicates an active and resolved Mesh path with a valid sequence number.

3.5.10 VNC Configuration

LOYTEC devices equipped with an LCD display also provide remote access over Ethernet to the LCD display. The VNC protocol is used for this purpose and the device implements a VNC server for exposing the display. The VNC server is by default disabled on the device. On the PC a VNC client needs to be installed. Using the default settings, the VNC client connects to port 5900 of the device. The password is ‘loytec4u’.

The VNC server can be configured on the **Ethernet** tab of the port configuration. To turn on the VNC server, enable the **VNC for LCD UI** checkbox. The VNC protocol settings are displayed in the settings box on the right-hand side as shown in Figure 70. The **VNC port** and **VNC password** can be changed. As a default, only one VNC client may connect. This limit may be increased in **Max VNC clients**. In order to protect changes made on the LCD UI over VNC with a PIN code, the **Admin PIN code** can be configured. To disable PIN protection, enter ‘0000’.

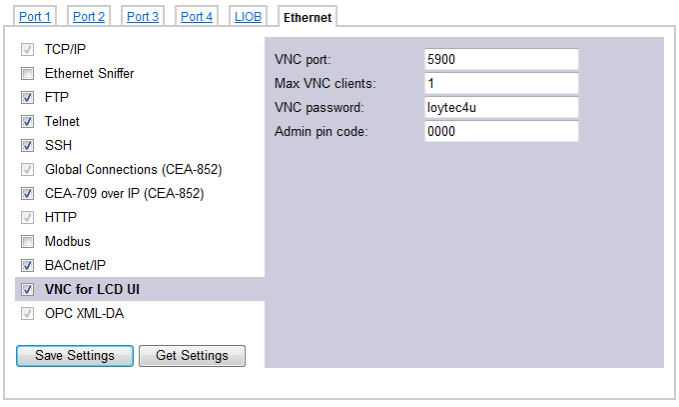


Figure 70: VNC Configuration.

3.5.11 CEA-709 Configuration

The CEA-709 protocol can be enabled on the device’s ports Port1, Port2, etc. if available. To enable it, click the **CEA-709** radio button as shown in Figure 71. Note, that depending on the device model, other protocols on the same port will be disabled in this case. The protocol settings box on the right-hand side displays the current transceiver settings.

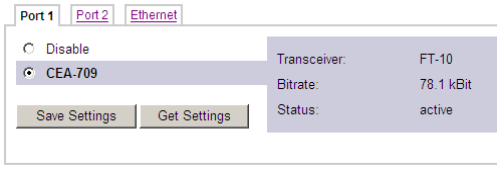


Figure 71: CEA-709 Configuration Page.

3.5.12 CEA-852 Device Configuration

The CEA-852 protocol is only available on the Ethernet port. To enable CEA-852 on the device, select the **CEA-709 over IP (CEA-852)** checkbox on the **Ethernet** tab of the port configuration page. Please note that on device models without a router or a proxy, the CEA-709 protocol on other ports will be disabled (e.g., LINX-100, L-GATE). On devices with multiple IP interfaces, the CEA-852 protocol can be activated only on one of them.

The CEA-852 protocol settings are displayed in the settings box on the right-hand side as shown in Figure 72. Typically, the device is added to an IP channel by entering the relevant information on a configuration server. The configuration server then contacts the CEA-852 device of the L-INX and sends its configuration.

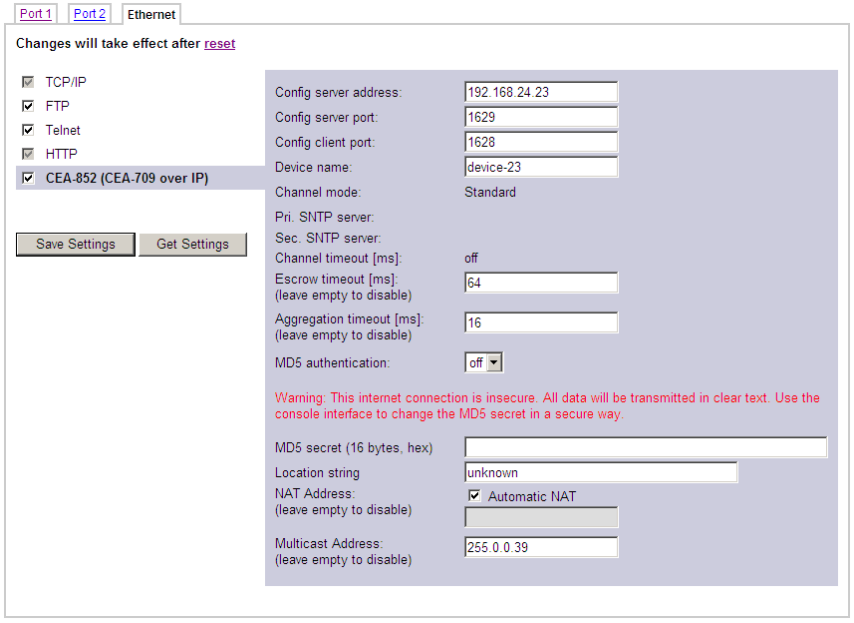


Figure 72: CEA-852 Device Configuration Page.

The field **Config server address** and **Config server port** display the IP address and port of the configuration server, which manages the L-INX and the IP channel. The field **Config client port** represents the IP port of the L-INX's CEA-852 device. This setting should be left at its default (1628) unless there are more than one CEA-852 devices operating behind a single NAT router. Please refer to the L-IP User Manual [2] to learn more about NAT configuration.

In the field **Device name** the user can enter a descriptive name for the L-INX, which will appear in the IP channel to identify this device. You can enter a device name with up to 15 characters. It is recommended to use unique device names throughout the IP channel.

The **Channel mode** field reflects the current channel mode of the CEA-852 device. It is configured by the configuration server. If there are any two devices in the channel which use the same IP address but different ports (e.g., multiple devices behind one NAT router) the

channel switches to **Extended NAT mode**. Please refer to the L-IP User Manual [2] to learn more about configuring the Extended NAT mode in the configuration server.

The configuration server sets the **SNTP server** addresses and the **Channel timeout**.

The filed **Escrow timeout** defines how long the CEA-852 device on the L-INX waits for out-of-sequence CEA-852 data packets before they are discarded. Please enter the time in ms or '0' to disable escrowing. The maximum time is 255 ms.

The field **Aggregation timeout** defines the time interval in which multiple CEA-709 packets are combined into a single CEA-852 data packet. Please enter the time in ms or '0' to disable aggregation. The maximum time is 255 ms. Note that disabling aggregation will negatively affect the performance of the CEA-852 device of the LINX.

The field **MD5 authentication** enables or disables MD5 authentication. Note that MD5 authentication cannot be used together with the Echelon's *i*.LON 1000 since the *i*.LON 1000 is not fully compliant with the CEA-852 authentication method. MD5 can be used with the *i*.LON 600. In the following field **MD5 secret** enter the 16-byte MD5 secret. Note that for security purposes the active MD5 secret is not displayed. You may enter the 16 bytes as one string or with spaces between each byte, e.g., 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.

Also note that entering the MD5 secret on the Web interface may pose a security risk. Since the information is transmitted over the network it can be subject for eavesdroppers on the line. It is recommended to use a cross-over cable.

In the field **Location string** the user can enter a descriptive test which identifies the physical location of the device. A location string can have a maximum length of 255 characters. This is optional and for informational purposes only.

If the CEA-852 device on the L-INX is used behind a NAT router, the public IP address of the NAT router or firewall must be known. To automatically detect the NAT address leave the **Auto-NAT** checkmark enabled.

The **Multicast Address** field allows the user to add the CEA-852 device of the L-INX into a multi-cast group for the CEA-852 IP channel. Enter the channel's IP multi-cast address here. Please contact your system administrator on how to obtain a valid multi-cast address. To learn when it is beneficial to use multi-cast addresses in your channel please refer to the L-IP User Manual [2].

3.5.13 Global Connections Configuration

The CEA-852 device used for global connections can be configured on the Ethernet port. The global connections function is always enabled on the CEA-852 device. This is indicated by the checkbox **Global Connections (CEA-852)** on the **Ethernet** tab of the port configuration page as shown in Figure 73. The settings are shared with the **CEA-709 over IP** settings, if that protocol is enabled. Otherwise, the CEA-852 device is configured on this tab as described in Section 3.5.12.

If the user does not want to share the CEA-709 over IP channel with his global connections, the checkbox **Use separate IP channel for global connections** can be activated. In this case, a separate CEA-852 device is configured on this tab as described in Section 3.5.12. Note, that this CEA-852 device will need a different port number, e.g. 1630. The separate CEA-852 device for global connections cannot be added to the local configuration server. In this case, also a separate configuration server (e.g. a LOYTEC L-IP) must be used.

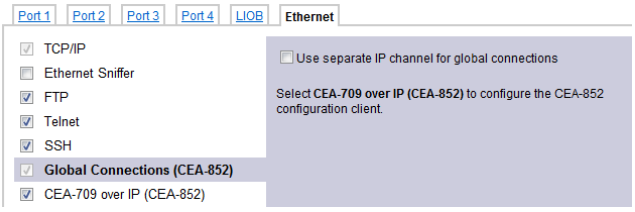


Figure 73: Global Connections Configuration Page.

3.5.14 CEA-709 Router Configuration

This page is only available on CEA-709 L-INX models with the router option (101, 111, 121, 151). The CEA-709 router configuration page allows configuring the built-in router mode. Available modes are **Configured Router** and **Smart Switch**. The L-INX must be rebooted to let the changes on this page take effect.

The configured router mode is the default setting. Choose this setting if you want to use the L-INX as a standard configured CEA-709 router that can be configured in a network management tool such as NL-200 or LonMaker.

The Smart Switch mode lets the device act as a self-learning router like the L-Switch. In this configuration the LINX's router doesn't need to be configured with a network management tool but is completely transparent in the network. Use this operating mode in a plug&play networking environment. The switch mode should only be used in LAN networks. In Smart Switch mode, this page has two more configuration fields: **Subnet/node learning** and **Group learning**.

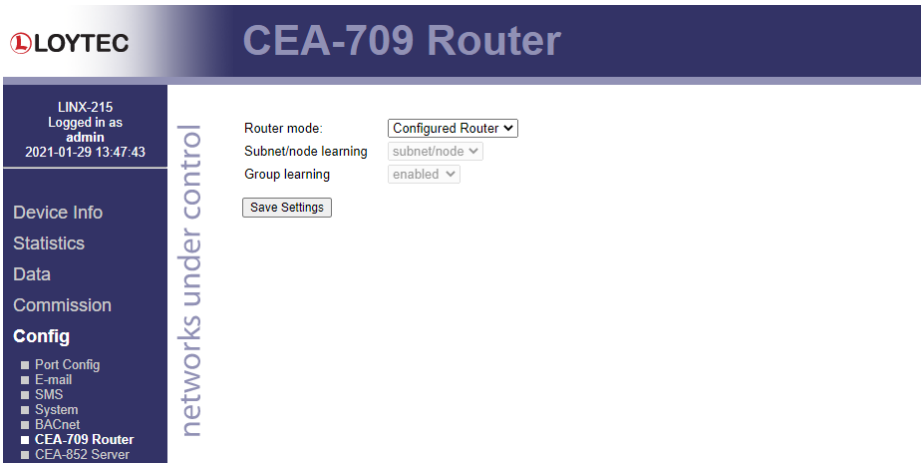


Figure 74: CEA-709 Router Configuration Page.

3.5.15 CEA-852 Server Configuration

This page is available on all L-INX and L-GATE models. On this configuration page the configuration server on the device can be enabled or disabled. In the drop-down box **Config server status** select **enabled** and click on **Save Settings** to activate the configuration server. On devices with multiple IP interfaces choose an IP interface on which the configuration server shall be running. Then the configuration server settings page appears as shown in Figure 75. If the configuration server is enabled the green configuration server LED labeled **CS** will be on, otherwise it will be off.

The configuration server port can be changed in the **Config server port** field. It is recommended to keep the default port setting of 1629. The field **Channel name** is informational only and can consist of up to 15 characters.

The field **Channel members** displays the current number of members on the IP-852 channel. The field **Channel mode** reflects the current channel mode. The L-INX configuration server automatically determines this mode. Depending on if there are any two devices in the channel which use the same IP address but different ports (e.g., multiple CEA-852 devices behind one NAT router). If all IP addresses are unique, the mode is **Standard**, if some are not unique the mode is **Extended NAT mode**. Please refer to Section 4.4.2 to learn more about the implications of this mode.

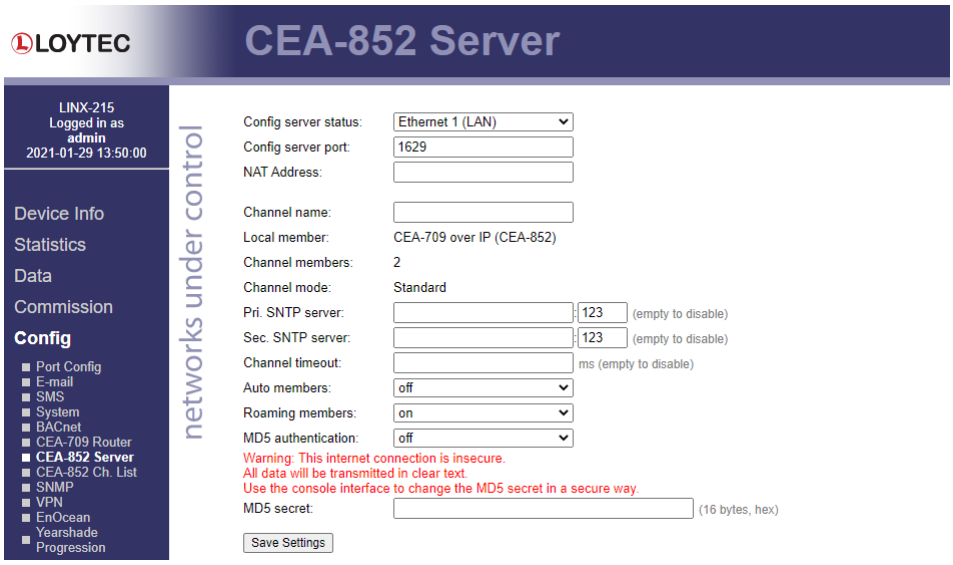


Figure 75: Configuration server settings.

Enter NTP timer server address and ports in the fields **Primary SNTP** and **Secondary SNTP**. The L-INX will synchronize to NTP time if primary or primary and secondary NTP servers are specified. A list of available timeservers can be found at www.ntp.org.

The **Channel timeout** is an IP-852 channel property and indicates how old a packet can be before it is discarded. The channel timeout is set in ms. To disable the channel timeout enter a value of 0. To select the proper value please consult Section 4.7.1. Setting a channel timeout other than 0 requires a valid SNTP server entry on the configuration server.

The **Auto members** option allows members to be automatically added to the channel. If turned on, CEA-852 devices can register on the IP-852 channel without the device being explicitly added on the configuration server. This special feature is useful in combination with the LPA-IP since it can add itself to the configuration server during the debug session. Non-responding auto members are automatically removed from the channel. This feature is turned off by default and must be explicitly turned on. Use this option with care because new CEA-852 devices can add themselves to the channel without knowledge of the system operator. This could cause a potential security hole.

The **Roaming members** option allows tracking CEA-852 devices when their IP address changes. This feature must be turned on if DHCP is used and the DHCP server can assign different IP addresses to the same device (same Neuron-ID). In combination with Auto-NAT the L-INX's router can also be operated behind NAT routers, which change their IP address between connection setups. For more information on this topic refer to Section 4.4.1. The roaming member feature is turned on by default. It is recommended to turn off this feature if DHCP is not used or if the DHCP server always assigns the same IP address to a given MAC address.

Use the drop-down box **MD5 authentication** to enable and disable MD5 authentication. If MD5 authentication is enabled, all devices on the IP-852 channel must have MD5 enabled and must use the same MD5 secret. Note that MD5 authentication cannot be used together with the Echelon's *i*.LON 1000 since the *i*.LON 1000 is not fully compliant with the

CEA-852 authentication method. MD5 can be used with the *i*.LON 600. The MD5 secret can be entered over the Web interface. You may enter the 16 bytes as one string or with spaces between each byte, e.g., 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.

It is recommended, however, to enter the secret locally and not over an Internet connection. It is best to use a cross-over Ethernet cable connected to the PC.

3.5.16 CEA-852 Channel List

This page is available on all L-INX and L-GATE models. If the configuration server is enabled on the L-INX, the CEA-852 device list can be seen in the CEA-852 channel list menu. An example is given in Figure 71.

The **Add Device** button is used to add another CEA-852 device to the IP-852 channel. The **Reload** button updates the Web page and the **Recontact** button contacts all devices to update their status. The **Execute** button executes the option selected in the adjacent drop-down box on the checked members. Each member can be selected for that action in an individual check-box in the **Sel** column. Actions available are: **disable**, **enable**, **delete**, **assign to NAT**, and **remove from NAT**. For more information on the actions on NAT routers refer to Section 4.4.2.

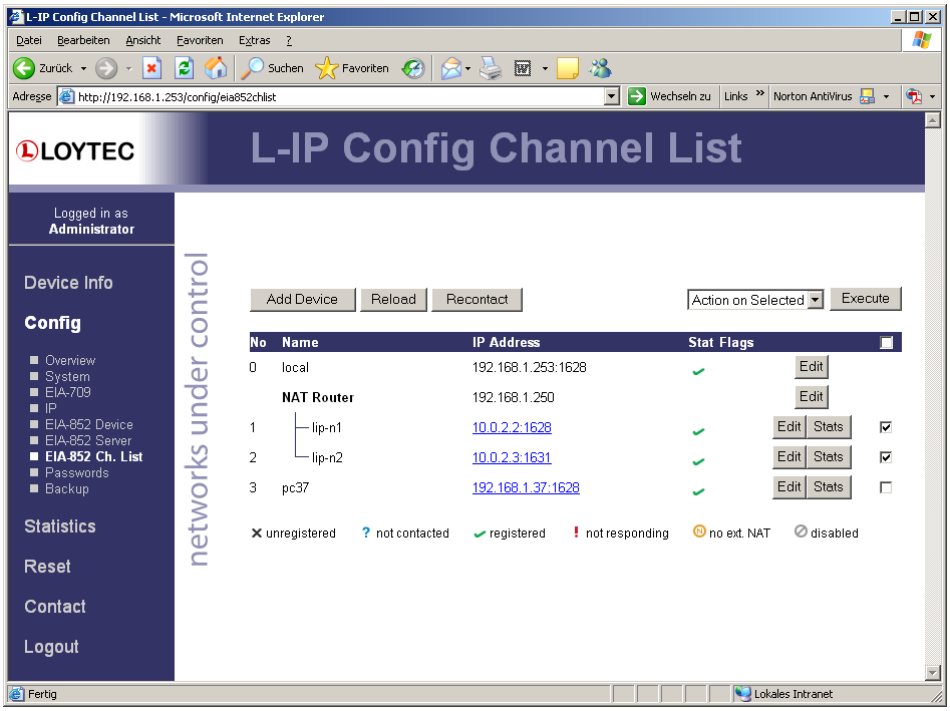


Figure 76: CEA-852 channel membership list.

The device status information is indicated with descriptive icons of different colors. The description for the different status indicators is shown in Table 3. The **Flags** column indicates with an **A** that the device is an auto member.

Click on the **Edit** button to change the device name, IP address, and port number for this device. Click **Edit** on a NAT router to change the NAT router address. The **Stats** button retrieves the statistics summary page from the client device.

Icon	Status	Description
✔	registered	The CEA-852 device has been successfully registered with the IP-852 channel and is fully functional.
✖	unregistered	The CEA-852 device has never been registered with the IP-852 channel.
?	not contacted	The CEA-852 device has not been contacted since the configuration server has started.
!	not responding	The CEA-852 device has been registered but is not responding at the moment.
⊘	disabled	The CEA-852 device has been disabled on the channel (or rejected).
Ⓝ	No extended NAT	The CEA-852 device does not support the extended NAT mode. This device is disabled.

Table 3: Possible Communication Problems in the Configuration Server.

3.5.17 BACnet Configuration

Figure 77 shows the BACnet device configuration page. This configuration page allows setting the **Device ID**, which is the instance part of the Object_Identifier property of the BACnet Device object. The field **Device name** holds the name of the BACnet device object (property Object_Name).

Important! ***The device ID and device name must be unique within the BACnet internetwork.***

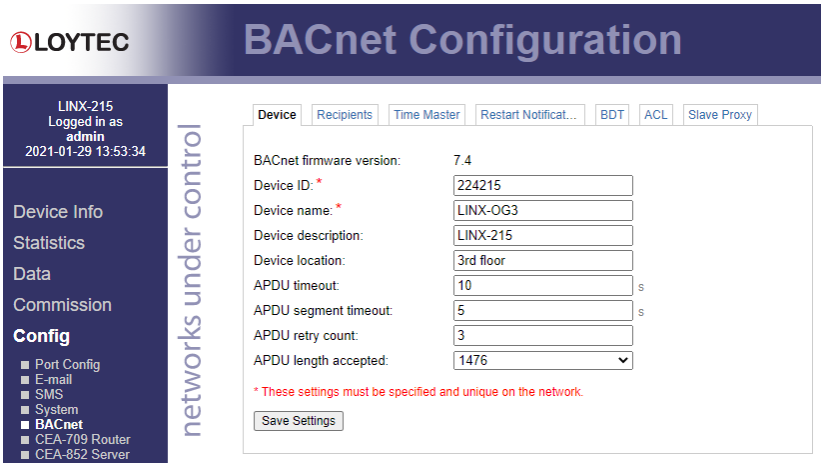


Figure 77: BACnet Device Configuration.

Further, the description and location can be configured. These configuration items correspond to the properties Description, and Location respectively of the BACnet Device object. For tuning BACnet application timing parameters, set **APDU timeout**, **APDU segment timeout**, and **APDU retry count**. The timeout values are entered in seconds allowing decimal notation, e.g. "7.5".

On the settings for BACnet/IP refer to Section 3.5.18. For configuring the MS/TP data link refer to Section 3.5.21.

Note: *If this page displays the message "Device communication is disabled via BACnet network!" the device has been externally disabled. Reboot the device to activate communication again.*

3.5.18 BACnet/IP Configuration

The BACnet/IP protocol is available on the Ethernet port. To enable BACnet/IP on the device, select the BACnet/IP checkbox on the Ethernet tab of the port configuration page. Please note that on device models without a router, the BACnet MS/TP protocol on other ports will be disabled (e.g., LINX-202, L-GATE). On devices with multiple IP interfaces, the BACnet/IP protocol can be activated only on one of them.

The BACnet/IP protocol settings are displayed in the settings box on the right-hand side as shown in Figure 78. On devices with a router (e.g., LINX-203) the **Network Number** of the BACnet/IP port must be configured to operate the built-in router. If the BACnet/IP network uses a non-default UDP port number other than 47808/0xBAC0, enter this port in the **BACnet/IP port** field. Enter '0' in this field for switching back to the default setting.

Important! ***For operating the LINX-151,153,203,213,215,221 as a BACnet router between BACnet/IP and MS/TP, the BACnet network numbers for the BACnet/IP and MS/TP ports must be set.***

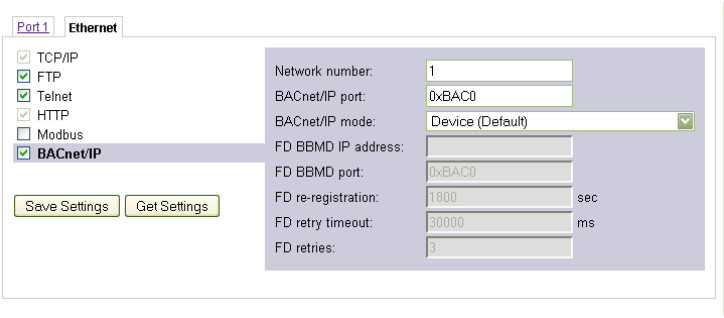


Figure 78: BACnet/IP Configuration.

In the field **BACnet/IP mode** the operation mode of the device is selected:

- **Device** (Default): In this mode the device operates as a regular BACnet/IP device on the local network without other advanced features.

- **Foreign Device** (FD): In this mode, the device registers at an existing BBMD in the BACnet/IP network as a foreign device. It is used, if the device is located as a single BACnet/IP device on a remote IP subnet or behind a NAT router. If operated as a foreign device behind a NAT router, port forwarding to the BACnet/IP port (UDP, default port 0xBAC0) and optionally to the Web server and FTP server port (TCP, default port 80 and 21) must be setup in the NAT router. If foreign device is selected, the following, additional settings must be made:

    - **FD BBMD IP address** and **FD BBMD port**: IP address and port of the remote BBMD the device registers at as a foreign device.

    - **FD re-registration**: A foreign device must periodically re-register at a BBMD. Here you can setup the corresponding interval. The default is 1800 seconds.

    - **FD retry timeout** and **FD retries**: Here you can specify the behavior, if registration does not work instantly. These values should be left at default: 30000ms / 3 retries.

- **Broadcast Management Device** (BBMD): This option is available on the L-INX models with the router (151, 201, 211, 221) and on all L-GATE models. Same as 'Device' but the BBMD function is enabled (see Section 3.5.25). For BBMD-only function, MS/TP can also be disabled (see Section 3.5.21).

On L-INX models with a BACnet router, the BACnet/IP port can be disabled while having MS/TP still enabled. This effectively disables the router, which can be useful for debugging purposes.

3.5.19 BACnet/IPv6 Configuration

On IPv6 networks the BACnet/IP protocol can be configured as BACnet/IPv6 by choosing the according setting in the **BACnet data link** drop-down box as shown in Figure 79. A reboot of the device is required to let the change take effect.

After the device has rebooted, check again on the BACnet/IP protocol tab. The field **BACnet/IPv6 Address** shows the IPv6 address currently in use. This is a link-local address if no other IPv6 address has been assigned. BACnet/IPv6 communicates via a pre-assigned IPv6 multi-cast address (ff02::bac0). Note, that in BACnet/IPv6 mode, the BACnet device will not be able to see any IPv4 devices. If your environment requires a different multi-cast address, it can be configured in the **BACnet/IPv6 Multi-Cast** field.

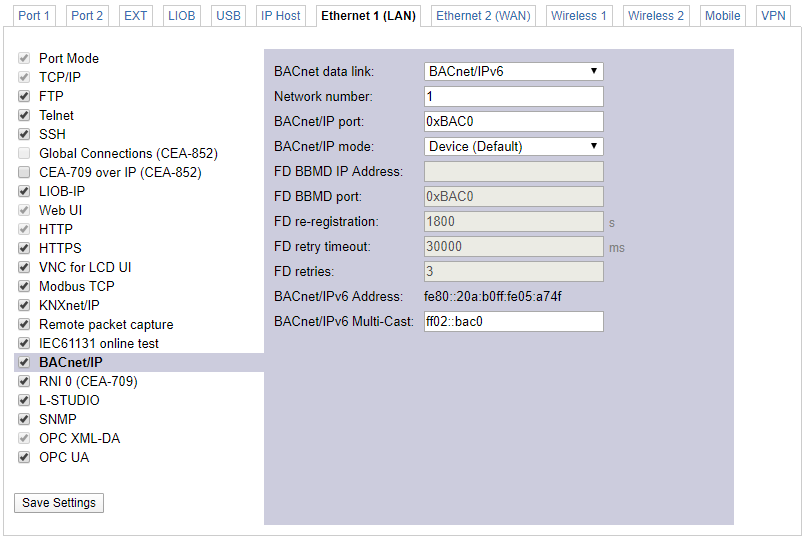


Figure 79: BACnet/IPv6 Configuration.

3.5.20 BACnet/SC Configuration

The BACnet/SC protocol is available on the Ethernet, WLAN or VPN port. To enable BACnet/SC on the device, select the BACnet/SC checkbox on the Ethernet tab of the port configuration page. Please note that on device models without a router, the BACnet MS/TP and BACnet/IP protocols on other ports will be disabled (e.g., LINX-202, L-GATE). On devices with multiple IP interfaces, the BACnet/SC protocol can be activated only on one of them.

The BACnet/SC protocol settings are displayed in the settings box on the right-hand side as shown in Figure 80. On devices with a router (e.g., LINX-203) the **Network Number** of the BACnet/SC port must be configured to operate the built-in router. The BACnet/SC node will connect to a BACnet/SC **Hub** or **Failover** hub. These must be configured by entering their web socket URLs in the format of 'wss://testhub:8443'. To establish trust with the hubs, the **CA Certificate** of the hubs must be installed by clicking on the **Choose File** button.

The BACnet/SC node certificate uses the installed Web server device certificate. If the device certificate has been deployed by LWEB-900 you can establish trust on the BACnet/SC hub by importing the LWEB-900's CA certificate on the hub. If another node certificate is required, click on the **Delete** button on the **Device Certificate** line and then **Choose File** and install the appropriate BACnet/SC node certificate.

Important!	***For operating the BACnet/SC node as a BACnet router between SC and IP, the BACnet network numbers on ALL BACnet/IP devices that route between IP and SC must be set to distinct numbers.***

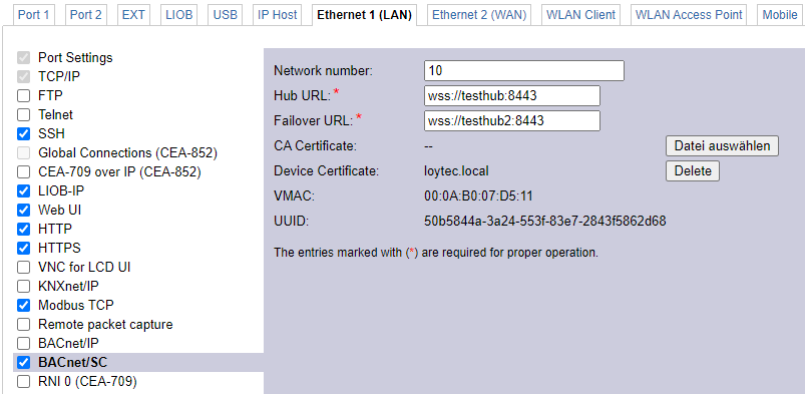


Figure 80: BACnet/SC configuration.

The device info page will show the BACnet/SC hub connection state. For more information on the connection status, go to the Statistics → BACnet page and select the BACnet/SC tab (see Section 3.2.11).

3.5.21 MS/TP Configuration

The BACnet MS/TP protocol can be enabled on one of the device's Port tabs, if MS/TP is available on the device model. To enable it, click the BACnet MS/TP radio button as shown in Figure 81. Note, that depending on the device model, other protocols on the same port will be disabled in this case

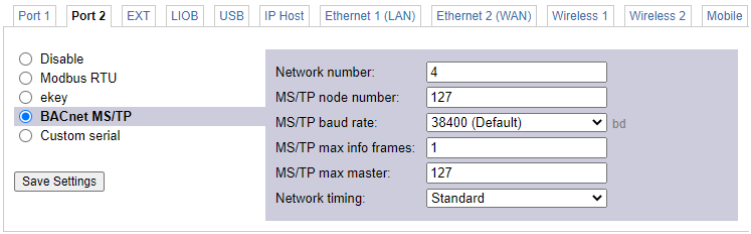


Figure 81: MS/TP Configuration.

The MS/TP protocol settings are displayed in the settings box on the right-hand side as shown in Figure 81. Mandatory settings are the **MS/TP node number** and the **MS/TP baud rate.** The MS/TP node number determines the physical address of the device on the MS/TP channel and must be in the range from '0' to the number configured with the **MS/TP max master** configuration option. It must be unique within the MS/TP channel. The Baud rate on the MS/TP channel can be set to 9600, 19200, 38400, 76800 and 115200 Baud.

Important:	***All masters on the MS/TP channel must have the same setting for MS/TP max master. Decreasing the default value 127 of MS/TP max master may reduce latency on the MS/TP bus.***

It is strongly recommended to leave the **MS/TP max info frames** and the **MS/TP max master** configuration options at their default settings. In any case the **MS/TP max master** number must be high enough to include the highest MS/TP node number of all masters on the channel. Slave devices may have a higher MS/TP node number than **MS/TP max master**.

To operate with slow devices on the MS/TP network set the **Network Timing** option to slow. This increases a number of timeouts, which is needed by some devices, but slows down

network communication. If communication problems occur in standard mode, try setting the slow mode. For fine-tuning other parameters please refer to Section 18.4.

On LOYTEC device models with a BACnet router (e.g., LINX-215), the **Network Number** of the MS/TP port must be configured to operate the built-in router. On those device models the MS/TP port can also be disabled independently of the BACnet/IP port. The MS/TP slave proxy function can be enabled and disabled in the BACnet configuration as described in Section 3.5.27.

3.5.22 BACnet Recipients

BACnet notification class (NC) objects have a recipient list. Other BACnet devices, that shall act as alarm recipients and receive alarm notifications need to be added to the recipient list of the respective notification class. The **Recipients** tab of the **BACnet Config** menu can be used to view currently subscribed recipients as shown in Figure 82. Recipient entries can be modified and deleted from the list. It is also possible to add new recipients to the list with the **Add Recipient** button. This way it is possible to integrate third-party devices as alarm recipients without an OWS.

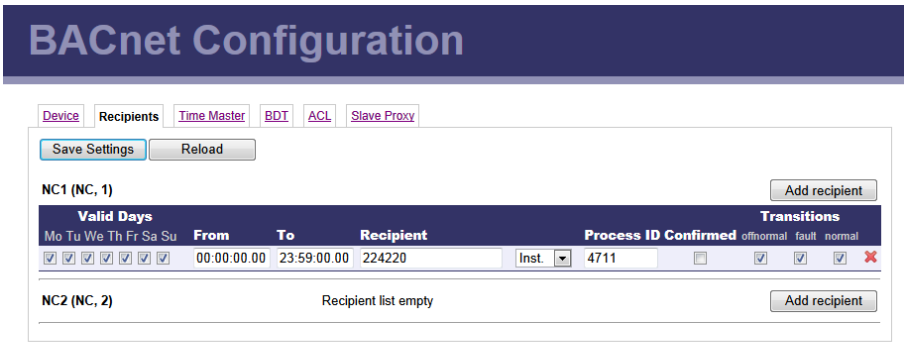


Figure 82: BACnet Recipients Configuration.

3.5.23 BACnet Time Master

The BACnet time master function relies on a list of time recipients. The **Time Master** tab of the **BACnet Config** Web page (see Figure 83) allows adding and removing time recipients of two classes: UTC time sync recipients, and time sync recipients (receiving local time). The time sync interval can also be configured on this tab. See Section 17.3.8 for more information on the settings for time sync interval, interval offset and align intervals.

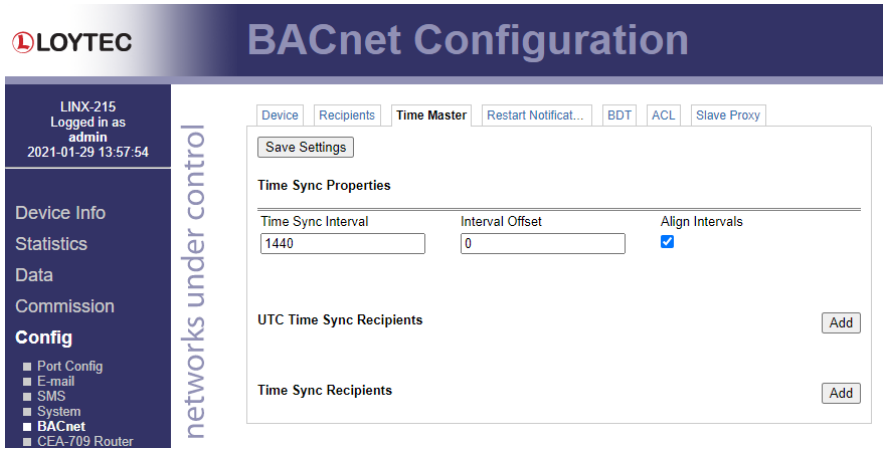


Figure 83: BACnet Time Master Configuration.

3.5.24 BACnet Restart Notifications

The device can be configured to send out a BACnet restart notification every time the device is starting. The list of recipients for this notification can be configured on the **BACnet Restart Notifications** tab. Click the **Add** button for adding a new line to the list. Then choose the recipient type from the drop-down box; it can be etiher a device instance number or a BACnet address. For broadcasting the restart notification, choose **Addr** and type in an asterisk '*' for a global broadcast or prefix it with a destination subnet, e.g. '12:*' as shown in Figure 84. Then click **Save Settings** to store the new recipient.

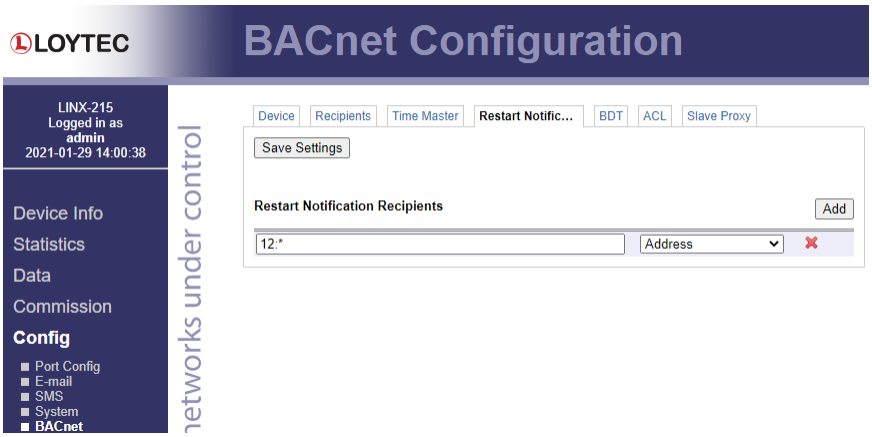


Figure 84: Broadcast BACnet restart notifications to a subnet.

3.5.25 BACnet BDT (Broadcast Distribution Table)

The BBMD function is only available on L-INX models with the BACnet router option (151, 201, 211, 221) and on all L-GATE models. The BBMD function is needed when a BACnet/IP network spans over several IP subnets separated by IP routers. If the device is configured as a BBMD, i.e. the BACnet/IP mode is set to Broadcast Management Device, see Section 3.5.17, the BDT (Broadcast Distribution Table) specifies all other BBMDs of the BACnet/IP network. The BDT is shown in Figure 85.

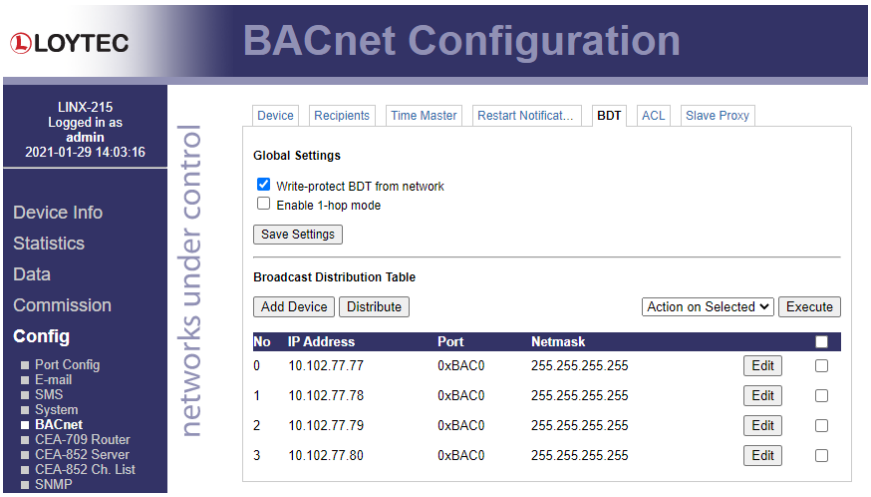


Figure 85: BACnet Broadcast Distribution Table.

By clicking **Add Device** new BBMDs (IP address and port) can be added. With **Action on Selected** and selecting existing entries, certain BBMDs can be deleted again from the table. It is not necessary to reboot the device when changing the table. However, you may want to click **Distribute** in order to propagate the table to all BBMDs in the list.

Note:	*The recommended maximum are 100 BBMD entries in the BDT.*

In the **Global Settings** section of this configuration page the behavior of the BDT can be modified:

- **Write-protect BDT from network**: If this option is enabled, the BBMD will reject any Write-BDT requests from the BACnet network. This option may be useful to protect your BDT tables from malicious access from the network.
- **Enable 1-hop mode**: Normally, the BBMD forwards broadcasts to the designated IP addresses of other BBMDs. This mode is called 2-hop mode. If the IP infrastructure allows sending directed broadcasts to other subnets, the BBMD can be switched to 1-hop mode. In this case, the subnet masks of the destination networks must be configured in the BDT entries.

3.5.26 BACnet ACL (Access Control List)

The device provides a feature in BACnet/IP to filter packets from certain sources on the BACnet/IP network. This feature is based on an access control list (ACL). An example of the ACL configuration is shown in Figure 86.

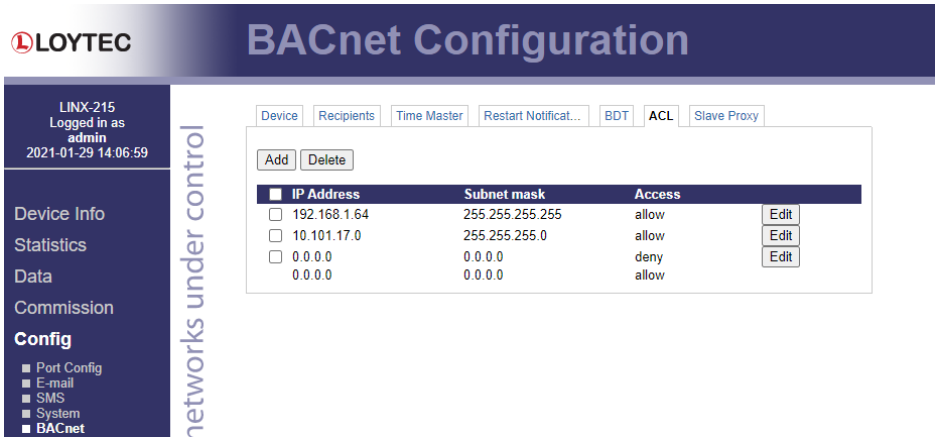


Figure 86: BACnet Access Control List (ACL).

The user can add and delete entries to the ACL. Each entry contains a source specification, which consists of an IP address and an IP mask, and an action (allow or deny). For specifying single hosts use the IP address and the mask '255.255.255.255'. For an address range specify an appropriate mask. For example use '10.101.17.0' and the mask '255.255.255.0' to specify all hosts with IP addresses '10.101.17.xxx'. To specify all IP addresses use '0.0.0.0' and the mask '0.0.0.0'.

The ACL is evaluated from specific host entries down to wider ranges. When adding new entries the ACL is automatically sorted, having the most precise definition at the top and the most general one at the bottom. The default behavior is to allow packets from all IP addresses. This is also the default entry in the ACL.

The example shown in Figure 86 specifies the following behavior for BACnet/IP:

1. Allow packets from the device 192.168.1.64
2. Otherwise allow packets from devices in the network 10.101.17.xxx
3. Otherwise deny packets from all (other) IP addresses. Note, that a "deny" overrules an "allow".

3.5.27 BACnet Slave Proxy

On LOYTEC device models with a BACnet router (e.g., LINX-215), the MS/TP slave proxy function is available. It can be enabled for each of the MS/TP ports on the **Slave Proxy** tab of the **BACnet Config** page. In auto-discovery mode the slave proxy permanently scans the MS/TP channel and automatically detects MS/TP slave devices. The **Slave Address Bindings** list shows all detected slave devices and displays their device instance number and BACnet address (DNET:MAC address) information as shown in Figure 87.

It is also possible to manually add slave address bindings in case MS/TP devices are not detected automatically. For doing so click the **Add** button indicated by the plus sign and enter the device instance number and BACnet address. If not known, leave the DNET part empty and press *Enter*. The DNET assigned to the port is automatically added. After adding all manual entries click on **Save Settings**. This also updates the current MS/TP DNET number for the manual slave address bindings. Note, when entering a DNET that is not valid for this port, the entry will appear under **Other**.

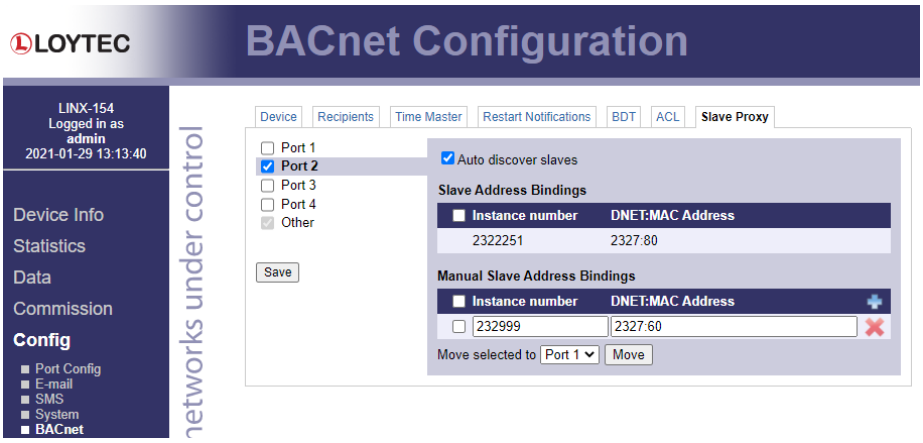


Figure 87: BACnet MS/TP slave proxy address bindings.

On device models with multiple MS/TP ports, manual slave proxy entries can be moved to other ports. For doing so, select the items using the check boxes, then select the target port from the **Move selected to** dropdown box and click **Move**. The DNET part of the manual entry is automatically adapted to match the targeted port.

3.5.28 E-mail Configuration

The Web interface provides the e-mail configuration page to set up an e-mail account, which is used to send e-mails. The content and time when e-mails are sent is configured through the Configurator software (see the LINX Configurator User Manual). The e-mail configuration page is shown in Figure 88.

In the field for the outgoing e-mail server, enter the SMTP server of your Internet provider. Typically, the SMTP server port can be left at 25. In the field **Source E-mail Address**, enter the e-mail address of the device's e-mail account. In the field **Source E-mail Sender Name** enter a name that the e-mail will display as the source name. Note, that only ASCII characters are allowed in the name. If replies shall be sent to another e-mail address, specify this in the **Reply E-mail Address**.

If the provider's SMTP server requires authentication, enter the required user name and password. Note, that username/password is supported as well as SSL/TLS authentication (e.g., for using Hotmail, gmail, or Yahoo!). For older versions of secure connection check the SMTPS check box.

To verify the e-mail configuration, reboot the device to let the changes take effect and return to the e-mail configuration page. Then press one of the **Send Test E-mail** buttons. Note, that

a DNS server must be configured in the IP settings (see Section 3.5.3) to resolve the e-mail server host name. The Web UI displays a warning message at the top of the page, if the DNS configuration is missing.

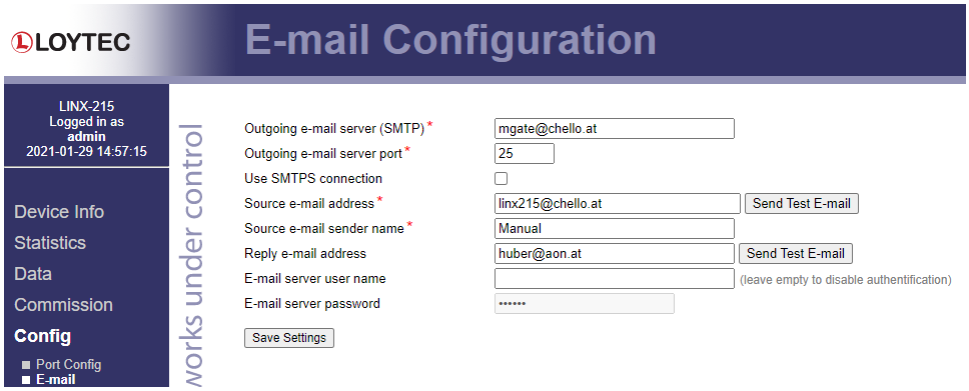


Figure 88: E-mail Configuration Page.

3.5.29 SSH Server Configuration

Some device models provide an SSH server. SSH allows encryption and authentication. The SSH server settings can be configured in the Ethernet port configuration page as shown in Figure 89.

It is possible to enable or disable the SSH server and to change the TCP port of the SSH server. The default SSH server port is 22. These settings will be active after rebooting.

The SSH configuration page displays the fingerprint of the RSA host key. A random RSA key (1024 bits) is generated per default. New keys can be created by selecting the required **RSA key size** (1024 or 2048 bits), and clicking the **Generate** button. In addition, EC keys can be generated. Select the EC key size in the drop-down box and click on the **Generate** button. The SSH server will load the new key after rebooting.

Note that recreating the SSH host keys can take up to a minute to complete. SSH clients which have already accepted the previous host key will refuse to connect to the SSH server until the host key change is confirmed in the client.

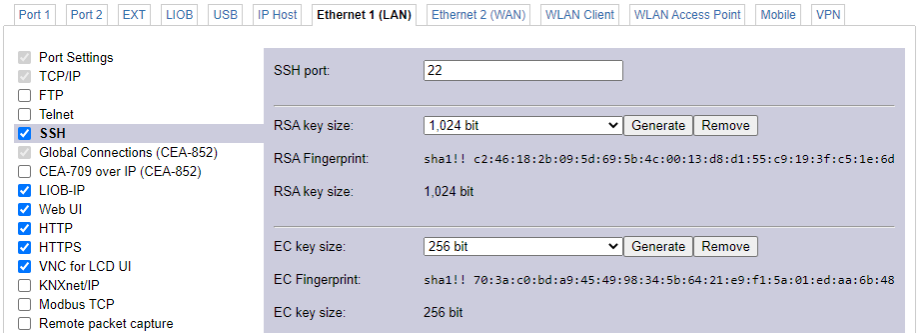


Figure 89: SSH Configuration.

3.5.30 SNMP

The device has a built-in SNMP server. All system registers and OPC-exposed data points are available as variables in the SNMP management information base (MIB). The MIB definition can be downloaded from the Web interface as shown in Figure 90. One can choose between a text and an XML format, depending on the SNMP tool in use. For more information on SNMP on the device please refer to Section 17.4.

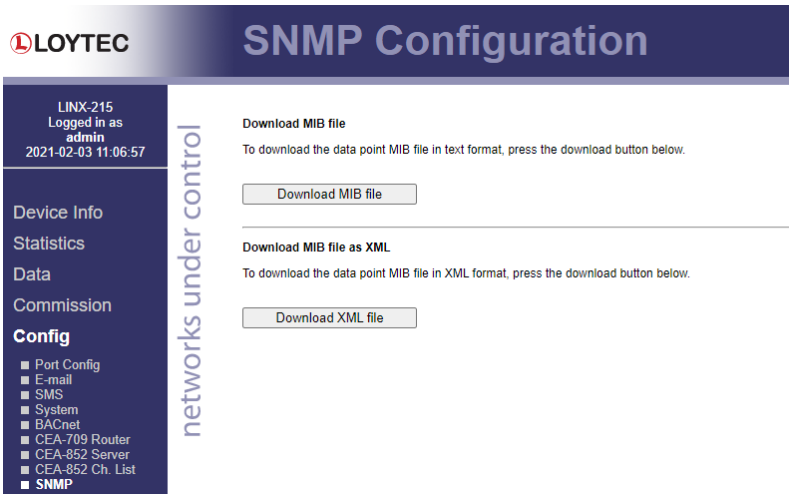


Figure 90: Get the SNMP MIB from the Web interface

3.5.31 VPN Configuration

To enable the virtual private network (VPN) interface on the LOYTEC device go to the **VPN** tab of the port configuration. The VPN is based on the OpenVPN technology and can be configured in one of two modes: 1) VPN client mode connects to a VPN server to join the VPN, 2) VPN simple server mode sets up its own VPN server on the LOYTEC device and offers an OpenVPN configuration for download that can be used to connect a VPN client to the LOYTEC device. This basic setting is made in the **OpenVPN mode** as shown in Figure 91.

Choose **Client connection** and click on **Save Settings** to activate VPN client mode. Optionally select the checkbox **Route local subnet** to enable the LOYTEC device route VPN traffic to and from the local IP subnet. This effectively makes devices on the local IP network available over the VPN, if the IP subnet address is unique on the entire VPN (i.e. each site has its own unique IP subnet that can be routed).

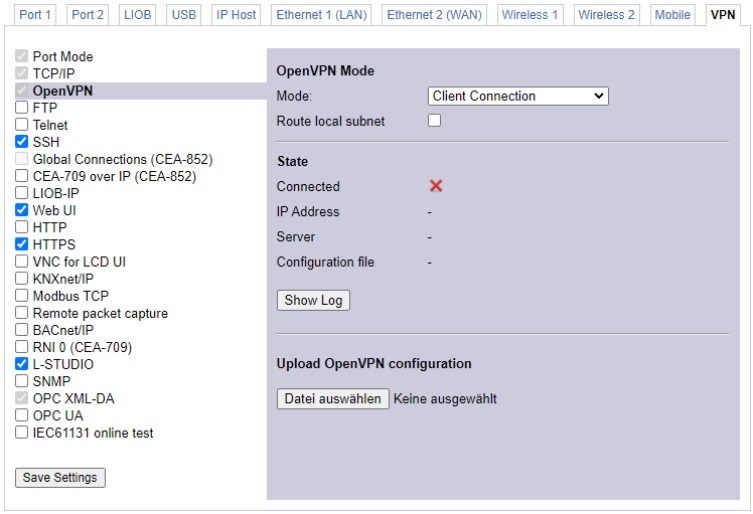


Figure 91: OpenVPN client configuration.

Under **Upload OpenVPN configuration** click **Choose File** button and choose an OpenVPN (.ovpn) configuration file provided by your OpenVPN server. Then click **Upload** to transfer the ovpn file onto the LOYTEC device. Typical OpenVPN servers such as OpenVPN Access Server or Synology OpenVPN server are supported.

Note: *OpenVPN config files must use embedded certificates and be auto-login, i.e., have no password protection to be entered before connecting to the OpenVPN server.*

When connecting to the OpenVPN server the **State** information is updated. Eventually, it should display connected state and the assigned IP address in the VPN as shown in Figure 92. To get more detailed information or troubleshoot the connection process, click on the button **Show Log** to read out and display the VPN connection log.

On the VPN tab of the port configuration Web UI, certain protocols can be configured to run on the VPN instead of the local Ethernet. This secures otherwise non-secure protocols such as CEA-852, BACnet/IP or Modbus TCP. For doing so, enable the VPN port in separate network mode. Note, that for CEA-852 all clients and the configuration server must be configured to run on the VPN interface. When running BACnet/IP on the VPN, it shall be noted that a BBMD needs to be configued on the OpenVPN server with all BACnet VPN client addresses. The LWEB-900 VPN server integrates a self-configured BBMD and thus provides a plug-and-play solution for BACnet/IP on VPN.

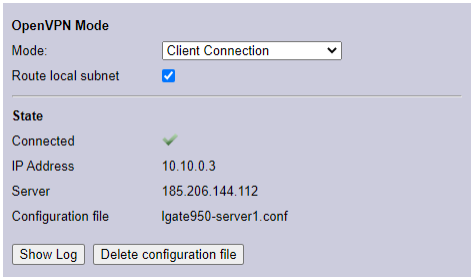


Figure 92: VPN client connection state.

Select **LWEB-900 Registration** to register with an LWEB-900 VPN and click **Save Settings**. Instead of uploading a configuration file, enter the LWEB-900 VPN Project PIN Code and optionally the Device PIN Code. The click **Start** to discover the LWEB-900 VPN and register the device in it.

Select **Simple Server** mode to enable the OpenVPN server on the LOYTEC device. Enter the IP address/hostname and port over which the LOYTEC device is externally reachable (see Figure 93). The port is shared with the local HTTPS port of the device. Optionally, edit the server's **VPN address**, which is useful when a client wants to connect to multiple VPN servers at the same time. Then click **Save Settings** and reboot the device to start the VPN server. Note, that it may be required to configure a port forwarding of HTTPS on the NAT router to reach the LOYTEC device.

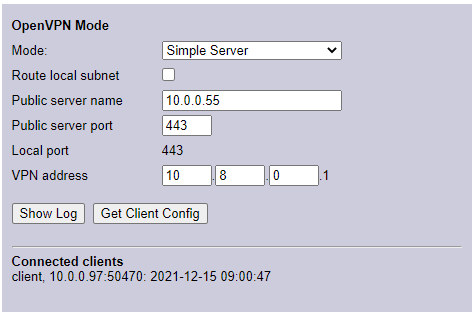


Figure 93: Configure OpenVPN simple server mode.

After the reboot has finished, the OpenVPN server on the device is active. Download the client configuration by clicking the button **Get Client Config**. Import this configuration file into an OpenVPN client (e.g. OpenVPN app on the mobile device or OpenVPN GUI on the

PC). The VPN simple server Web interface displays information on **Connected clients**. Currently, only one client is allowed to connect at a time.

3.5.32 LTE Configuration

LOYTEC devices supporting the LTE-800 adapter can be used to logging into a mobile LTE network. To enable the LTE-800 adapter on the LOYTEC device, the first configuration step is to select the port mode "Separate network" on the **Mobile** tab of the port configuration, as shown in Figure 94 and click **Save Settings**.

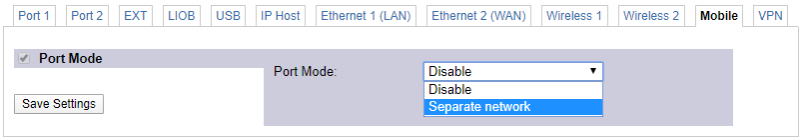


Figure 94: Enable LTE via port mode

This enables the LTE interface and jumps to the **Mobile network** settings section as shown in Figure 95. Depending on the information provided by your mobile carrier, enter the APN information under **Access Point Name** and additionally **Username** and **Password** if required by your carrier. Then enter the **PIN Code** of the SIM card. If the PIN function is disabled on the SIM card leave this field blank. Activate **Roaming** if your carrier requires roaming on the home network. Then click **Save Settings**. Whether the SIM lock has been successfully removed is indicated by the status text next to the PIN Code field.

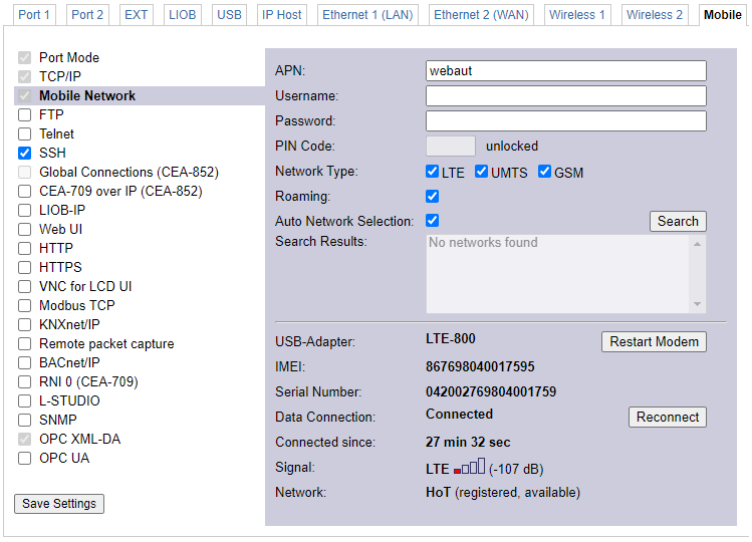


Figure 95: Mobile network settings for LTE

The LTE interface now attempts to establish a data connection to its home network. The status information of the LTE interface is displayed in the bottom part of the **Mobile Network** section. The field **Data Connection** will eventually display "Connected". Other information on signal quality and carrier information is also displayed. For information on consumed data volume refer to the mobile network statistics (Section 3.2.15).

For test purposes, the **Reconnect** button can be used to reset and reconnect the LTE data connection. With the **Restart modem** button you can completely restart the LTE modem. These actions are not required during normal operation.

If a different carrier than the home network shall be used, deactivate the checkbox **Auto Network Selection** and click on the **Search** button to find other mobile networks. The **Search Results** list is filled with the found networks as shown in Figure 96.

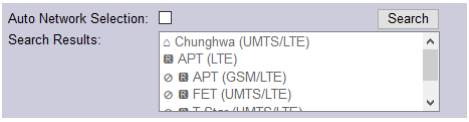


Figure 96: Scan result of mobile networks

The icons in the result list have the following meaning:

- ⌂ Home network
- ⊘ Not allowed (foreign network)
- Ⓡ Roaming: To use this network also select the Roaming checkbox.

Select the desired network and save settings. The modem will connect using the new mobile network.

3.5.33 SMS Gateway

The LOYTEC device has a built-in SMS gateway that allows transmitting SMS. The SMS gateway can be configured to transmit over a locally connected LTE-800 interface or a remote LTE-800 interface connected to a LOYTEC device on the network. This settings are made on the **SMS** configuration page as shown in Figure 97.



Figure 97: SMS gateway settings.

In the drop-down box **SMS gateway is** choose a locally connected or a remote LTE-800. If remote LTE-800 is selected, then enter the IP address or DNS name of the **SMS gateway** and the HTTPS port below. Then select the **Username** to connect and enter the **Password**.

You can use the Test button next to the gateway address to verify, if the supplied settings are correct to connect to the SMS gateway. In order to test actual SMS delivery, click on the button **Send Test SMS**. This opens a pop-up window that prompts for a mobile phone number. Finally, click **Save Settings** to make the settings effective. A reboot is not required.

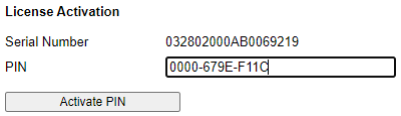
3.5.34 License

On the LOYTEC devices certain features may be activated by entering a license PIN code on the Web interface or the LCD UI. This license PIN code is entered only once and remains on the device for its lifetime.

To Activate a License on the Web UI

1. Go to the menu **Config → License**.

2. Enter the 12-digit license PIN code and click on **Activate PIN**.



3. The list of activated features now lists the PIN code and activated license.

4. Finally, reboot the device to start the activated feature.

The license activation page shows all active licenses as depicted in Figure 98. Licenses can be deactivated by deselecting the check box in front of them. Then click **Update Features** to activate the change. A reboot is required after that.

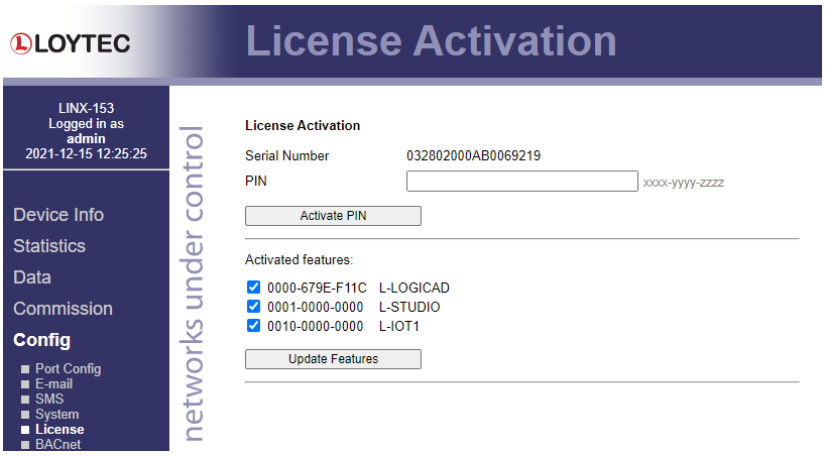


Figure 98: License activation page

3.6 Programming

3.6.1 L-STUDIO Configuration

On the **L-STUDIO** configuration page under the **Programming** menu the user can view the state of the program as well as controlling the behavior of the I/O driver, see Figure 99. After deployment of the program by L-STUDIO the PLC kernel is restarted with the new program.

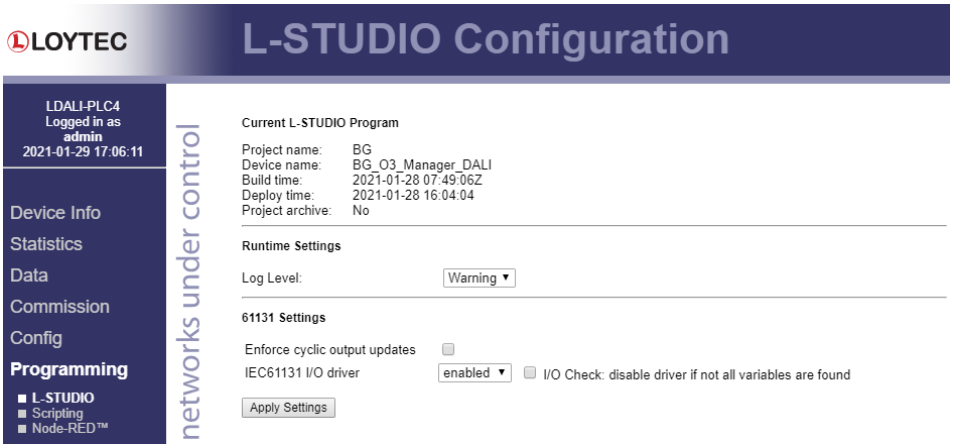


Figure 99: L-STUDIO Configuration Page.

The information about the running program is displayed, containing the project name, the device name (assigned by the L-STUDIO project), the build time of the program, and the last deploy time. L-STUDIO can be configured to store an entire project archive on the device; this is shown in **Project archive**.

On models with the IEC61131 programming option in L-STUDIO, the data exchange of the L-STUDIO program can be disabled by disabling the I/O driver. As a result the program is not able to receive or send update from/to the appropriate data points. Hence, for debugging purpose, the data point values can be manipulated regardless of the data set from the L-STUDIO program.

The option **Enforce cyclic output updates** makes sure that the output data points will contain the calculated logic value after each cycle. For more information refer to the Chapter L-STUDIO of the L-INX/L-GATE User Manual.

3.6.2 L-LOGICAD Configuration

On the **L-LOGICAD** configuration page under the **Programming** menu the user can download an L-LOGICAD program as well as controlling the behavior of the I/O driver, see Figure 100. After downloading the L-LOGICAD program the PLC kernel is restarted with the new program. After it has been restarted check the PLC LED for a successfully started program.

Important! ***Downloading a new L-LOGICAD program may result in the need for a new data point configuration. Hence, take care about the requirements of the downloaded program and in case of a different set of IEC61131 variables use the L-INX Configurator to adapt the data point configuration. The I/O check feature disables the I/O driver if missing data points are detected.***

The data exchange of the L-LOGICAD program can be disabled by disabling the I/O driver. As a result the L-LOGICAD program is not able to receive or send update from/to the appropriate data points. Hence, for debugging purpose, the data point values can be manipulated regardless of the data set from the L-LOGICAD program. The I/O check feature disables the I/O driver after a reboot, if any variables with missing data points are detected. Deselect the I/O check to disable this feature. Variables, which could not be loaded are listed at the bottom of the page. The information about the running program is also displayed. The L-LOGICAD program can be removed from the device by clicking the button **Remove**. The device needs to reboot after this action.

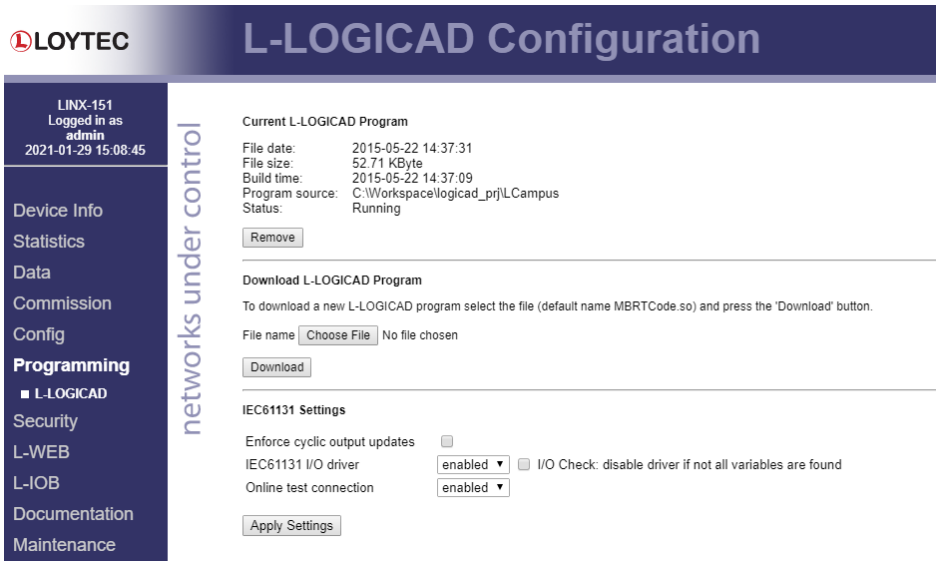


Figure 100: L-LOGICAD Configuration Page.

The option **Enforce cyclic output updates** makes sure that the output data points will contain the calculated logic value after each cycle. For more information refer to the Chapter L-LOGICAD of the L-INX/L-GATE User Manual.

3.6.3 Scripting

LOYTEC device models that support script modules have this configuration page. Under the **Programming** menu, the **Scripting** page displays the status of running scripts and the installed script resource modules as shown in Figure 101. The **Stop** and **Start** buttons allow stopping and starting the scripting engine. The check-box **Respawn scripts when exited** causes script modules that stopped because of an uncaught exception to be respawned. This is the default setting. The log window at the bottom contains the console output of the running script (printed by console.log). It can be downloaded and is a useful tool when developing a script to output status information.

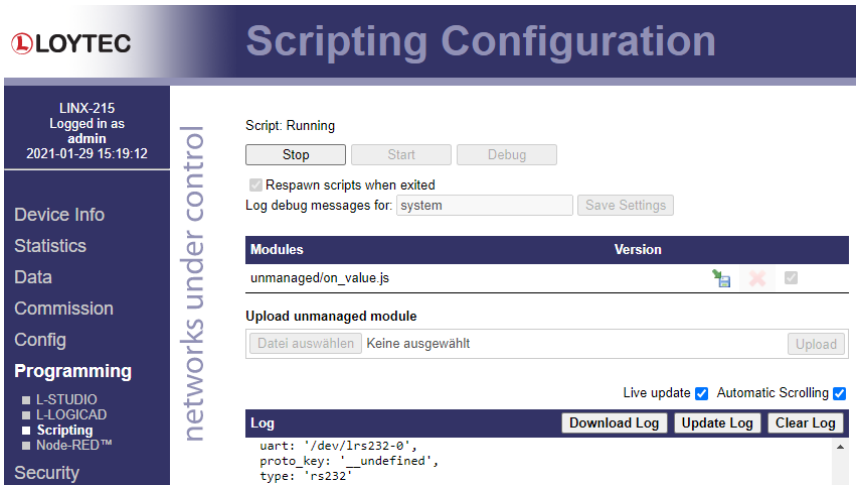


Figure 101: Scripting Web interface.

In order to debug a script, first stop the running scripts. Enter a debug message filter in the **Log debug messages** field and activate by clicking on **Save Settings** or leave it empty to disable any debug messages. Then click the **Debug** button. The script is then launched in inspect mode and an inspection URL is displayed as shown in Figure 102. Copy this URL and paste it into Google Chrome. The Devtools page of Chrome will connect to the device and launch the JavaScript debugger.

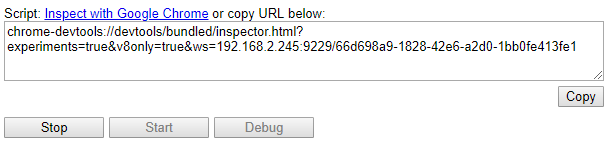


Figure 102: Inspect URL for script debugging

When debugging it is useful to turn auto-respawn of scripts off. In this case the root cause of an uncaught exception is easier to find. It may also be useful to disable execution of certain script resources. For doing so, stop the scripts, then deselect the checkboxes for those scripts to be disabled. For a more detailed discussion on developing of and debugging techniques for scripts please read the Chapter Script Engine in the LINX Configurator User Manual [1].

3.6.4 Node-RED™ Editor

LOYTEC devices that support the scripting feature now also natively integrate the Node-RED™ run-time. Under the **Programming** menu the Web interface provides a configuration menu to open the Node-RED™ editor UI. As a default, the run-time is not executing and needs to be enabled. Click the **Enable** button to start the run-time. Once

enabled, the run-time automatically starts the configured flows every time the device is powered up. The run-time can be disabled by clicking the **Disable** button. The log output can be shown by clicking on the **Show Log** button. Select the **Safe Mode** checkbox in order to disable flows that are not stable and cause frequent restarts. An example is shown in Figure 103.

The editor UI can also be opened in a stand-alone Web browser page under the '/nodered' device URL. In this case log in as user 'admin' using the admin password.

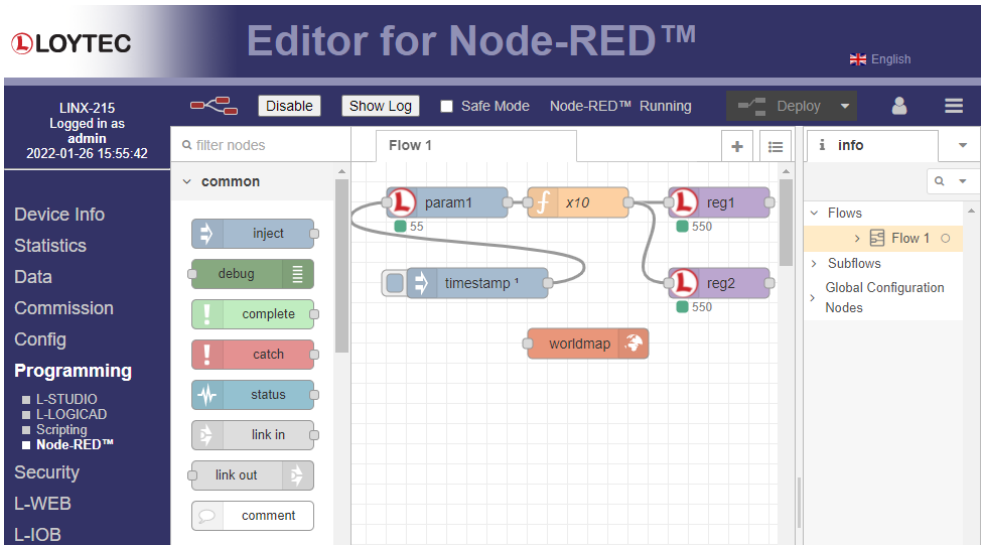


Figure 103: Node-RED™ editor UI on the device.

Flows can access data points on the device using the pre-installed 'readDP' and 'writeDP' palette items. To configure those select the data point **Server** that possesses the data points and defines a data point base path. Choose 'localhost' to refer to the root folder of device itself. Additional data point servers may be defined pointing to another device's IP address or by defining a different data point base path. These definitions are shared among all readDP/writeDP nodes.

Then enter a **Data Point Path** which is added to the server's base path, resulting in the displayed **Full Path**. The example in Figure 104 defines a readDP node that maps to the 'param1' user register of the local device. Select the **CoV** option to get automatic updates in the readDP node. Otherwise, the read action must be triggered on the node's input connector.

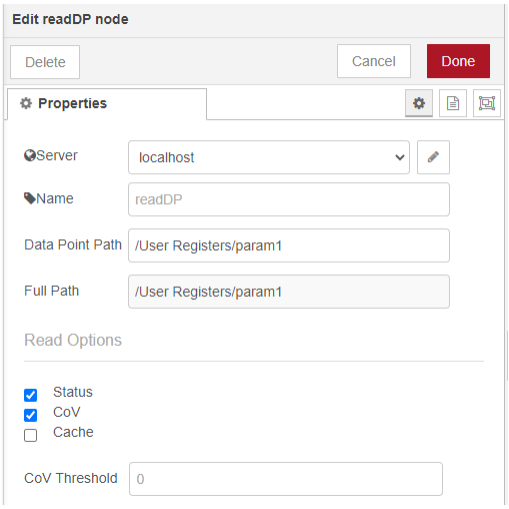


Figure 104: Example configuration of a readDP node.

If the data server shall be another LOYTEC device, click on the edit button next to the **Server** dropdown in order to add a new server configuration (see Figure 105). Enter a **Name** for the new server and a **Host** IP address. If the default operator user needs modification, edit user and password. It is also possible to search online for LOYTEC devices on the local network. Click the **Search** button under **Device Discovery**. All discovered devices are added to the dropdown list. Choose the desired device and the IP is copied to the **Host** field. Then click **Add** to add the new data server and use it in the readDP node.

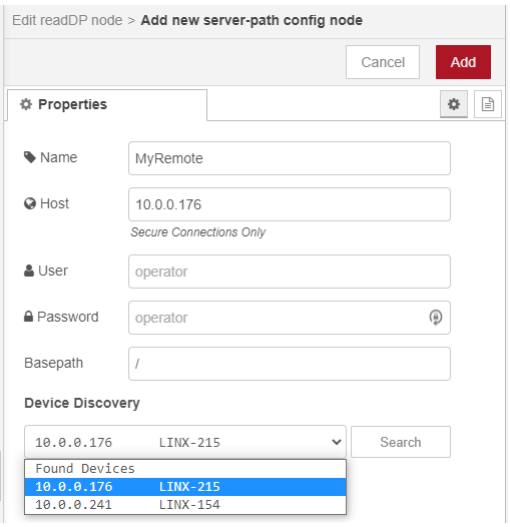


Figure 105: Use a remote device as the data server.

A similar configuration applies to the writeDP node. For additional information refer to the node's help text. A simple configuration that implements a data point connection in the flow editor is shown in Figure 93. Any update from 'param1' is multiplied by 10 and written to the user registers 'reg1' and 'reg2'. To trigger an update when starting up, use an inject node and connect it to the dpRead's input and edit the inject node's properties by setting **Inject once**.

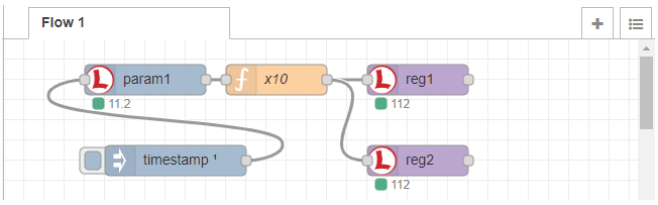


Figure 106: Example Node-RED™ data point flow.

Custom palette items can also be installed, like the 'worldmap'. These are installed onto the device and can be used in flows. Nodes that implement their own Web service can be accessed behind the '/nodered' URL, e.g. '/nodered/worldmap'.

All configured flows, installed palette items and log output are written to the device backup. The backup can then restore the full flow functionality.

3.7 Security

3.7.1 Change Passwords

The admin and operator passwords have been configured when contacting the device for the first time. Passwords for locally created users have been set when creating the user. To

change the password of the logged-in user, click on **Passwords** in the **Security** menu, which opens the password configuration page as shown in Figure 107.

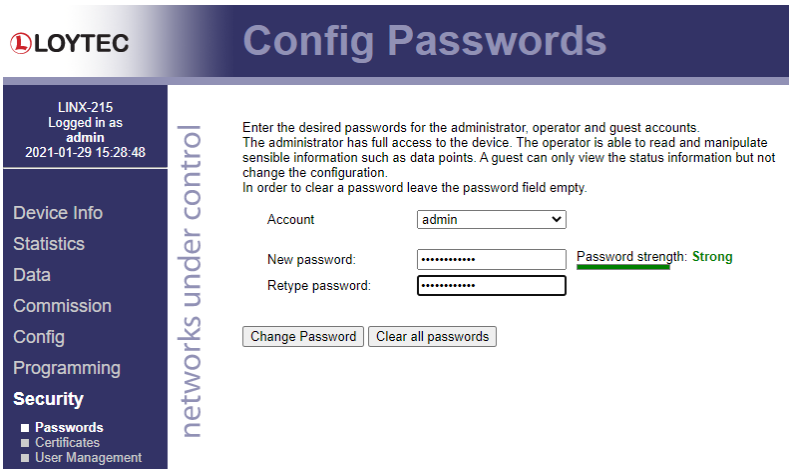


Figure 107: Password Configuration Screen.

If logged in as the 'admin' user, it is allowed to change also 'operator' and 'guest' passwords. To change the admin password, select the **admin** account in the drop-down box. Enter the new password. The password strength indicator will inform you about the security quality of your password. If the password is left empty, password protection is turned off and everyone can access the device without entering a password. Click on **Change password** to activate the change.

If logged in as 'admin', click **Clear all passwords** to clear all administrative passwords on the device. After clearing the passwords, new admin and operator passwords have to be set before proceeding on the Web UI. Passwords of locally created users are not cleared.

3.7.2 Certificate Management

Some device models provide the secure HTTPS and OPC UA in addition to HTTP and OPC XML-DA. It allows for encrypted and authenticated communication.

The HTTPS server settings can be configured in the Ethernet Port Configuration page. It is possible to enable or disable the HTTPS server and to change the TCP port of the HTTPS server. The default HTTPS server port is 443. These settings will be active after rebooting.

When connecting with a web browser to the LOYTEC device you will be warned that the server uses a self-signed certificate. You need to accept the certificate in order to continue. In some browsers this is also called "adding an exception".

Note that in default configuration, communication is encrypted, but not safely authenticated, as the default certificate is self-signed and uses a default common name "loytec.local". If you operate in a safe environment and your client accepts this, no further action has to be taken.

Some OPC UA clients, however, will not validate the LOYTEC server with the default certificate. In this case the common name of the self-signed certificate needs to excplicitly state the IP address or host name used for the client connection.

To create such a personalized self-signed certificate for the LOYTEC device:

1. Go to the **Certificates** configuration page and select the **Create Certificate** tab. The radio button **Self-Signed** is selected and all necessary data is pre-filled as shown in Figure 108. Note, that **Common Name** contains the IP address over which the device has been contacted. Check **EC Key** if the certificate shall use EC instead of RSA.

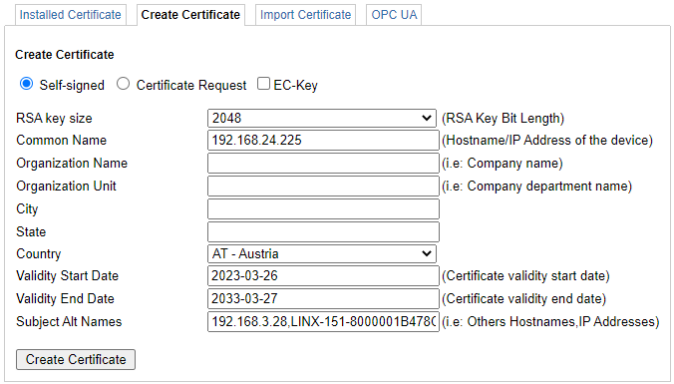


Figure 108: Create a personalized self-signed certificate

2. Optionally modify any of the fields to your choice and then click **Create Certificate**. Certificate creation may take up to a few minutes. When finished, the new self-signed certificate is shown (see Figure 109 below). Reboot the device to activate the change.

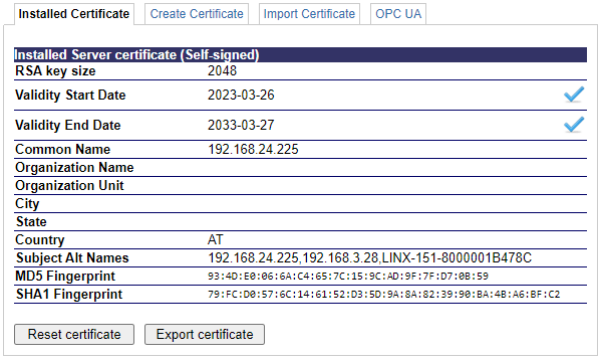


Figure 109: New created self-signed certificate

To widen acceptance of the LOYTEC server in a hostile environment (e.g. when using over the Internet), consider installing a server certificate signed by a certification authority to prevent man-in-the-middle attacks. HTTPS and OPC UA servers use X.509 certificates to authenticate themselves to clients. In order to establish communication, the client has to trust the server certificate. There are two options to accept a server certificate:

- The user manually accepts the certificate.
- The server certificate is provided by a public certification authority (CA).

LOYTEC devices are configured with a self-signed certificate, but custom server certificates can be imported in the configuration page. Please follow these steps to install a custom certificate signed by a CA.

1. Go to the **Certificates** configuration page and select the **Create Certificate** tab. Choose the radio button **CA Request** as shown in Figure 110. In **Common Name** provide a valid DNS host name (e.g., linx-g01.acme.com) or the IP address for the device. SSL certificates use host names. Enter organization name, organization unit, city, and state. Check **EC Key** if the certificate shall use EC instead of RSA. Then choose the country and click **Create Certificate Request**.

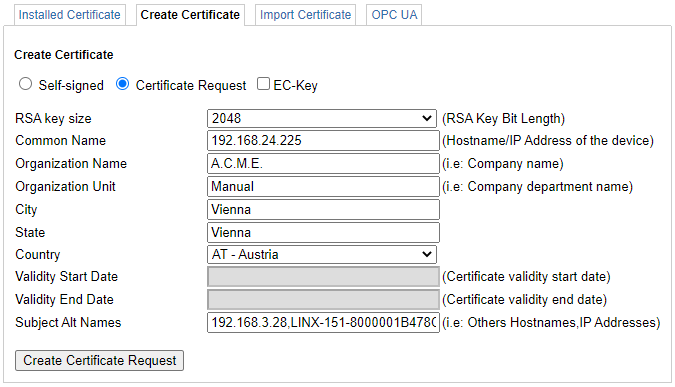


Figure 110: Create a CA certificate request.

2. Copy the X.509 certificate request from the Web page as shown in Figure 111 and follow up with the instructions provided by the certification authority.

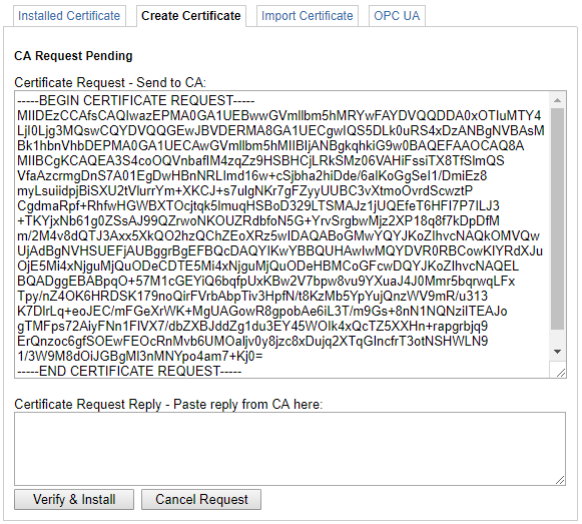


Figure 111: Copy and paste for the X.509 certificate request.

3. Order the certificate. The LOYTEC device requires the certificate to be encoded in PEM format in order to be pasted easily.

4. After receiving the certificate, copy it to the clipboard or a text file. It should look like this:

```
-----BEGIN CERTIFICATE-----
MIICyjCCAjOgAwIQEBBQUAMH4xCzAJBgNV…
… more data follows …
-----END CERTIFICATE-----
```

5. On the tab **Create Certificate** paste the information to the **Certificate Request Reply** text area as shown in Figure 111 and click **Verify & Install**.

6. After next reboot, the server uses the imported certificate, so that the web browsers will indicate the page as trustworthy.

7. Note that certificates have a lifelime, typically 1 or 2 years. You need to repeat these steps to renew your certificates before they expire.

Optionally, a certificate can also be installed from a file. Go to the **Import Certificate** tab as shown in Figure 112 Select the certificate in the **Server certificate** field and its private key in the **Server private key** field. Both can be in PEM or DER (*.der/*.cer) format.

Important! ***You cannot install a Server certificate without its private key!***

If your certification authority uses intermediate certificates, import these **CA certificates** in the CA certificate text field (same format). Press **Save** to import and store the certificates and the server certificate private key. If you want to remove your custom certificate, click on **Reset certificate**. On the **Installed Certificate** tab.

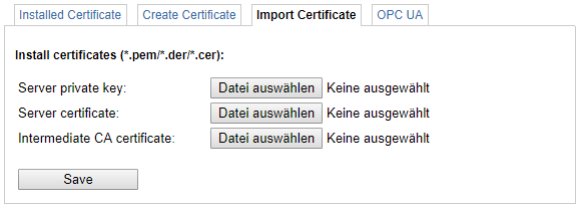


Figure 112: Install a certificate on the Web interface.

3.7.3 User Management

The device has three pre-defined user accounts: (1) **guest** allows the user to view certain information only, e.g., the device info page. By default the guest user has no password. (2) **operator** is able to read more sensible information such as calendar data. (3) **admin** has full access to the device and can make changes to its configuration. Note that the user accounts are also used to log on to the SSH, FTP and Telnet server.

It is also possible to create other users locally on the device. These users can be assigned to different roles. The ‘admin’ and ‘operator’ roles have the same administrative rigths as their pre-defined counterparts, except of creating/deleting local users. It is good practice to create separate users with the ‘admin’ role in order to keep the master administrator password a secret. Locally created users can be disabled or deleted at any time, therefore removing the administrative rights for any of them when needed.

Note: *User names must only contain lower-case letters, digits, underscore and dashes. The first character must be a lower-case letter. The length is limited to 32 characters. The number of locally created users is limited to 80.*

The ‘lweb’ role can be assigned to users that are solely meant to login over the LWEB-802/803 clients and operate within the L-WEB visualization project. These users have no other administrative rigths on the device.

To manage local users go to the **User Management** page of the **Security** menu. This page displays the list of local users (see Figure 113). Managing local users is only allowed when logged in using the ‘admin’ user account.

Click on **Add User** to add a new user and edit the username, password and role from the drop-down box. Then click the save icon. To edit the password or role of a local user, click the respective edit icon, update the content and click on the save icon.

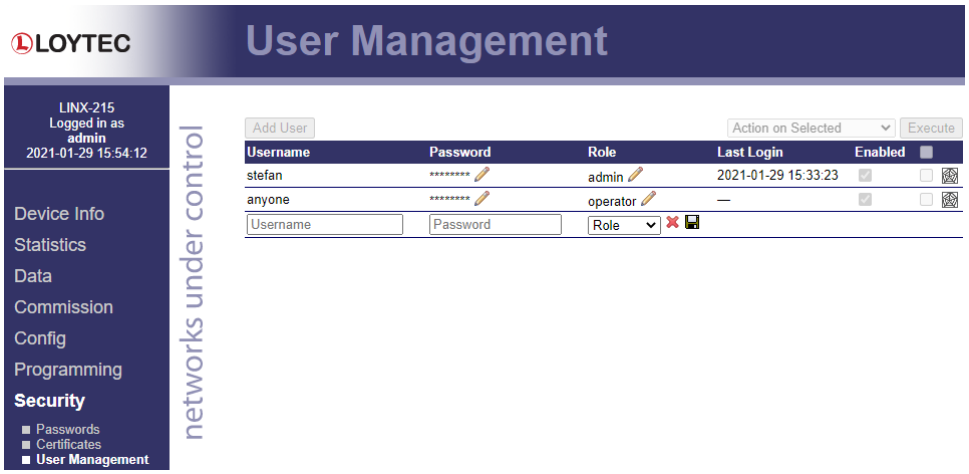


Figure 113: User management page.

Other actions on local users include enable, disable, and delete. Select the checkbox on the right-hand side for one or more users and choose an action from the **Action on selected** drop-down. Then click on **Execute**. Disabled users cannot log in anymore but their credentials remain on the device and can be enabled again.

Users with the 'lweb' role can access L-WEB projects only. The access can be further narrowed down by clicking the L-WEB icon. In the pop-up window (shown in Figure 114) choose those L-WEB projects, for which the user shall have access to and click **Save**. Other projects will not be accessible by this user.

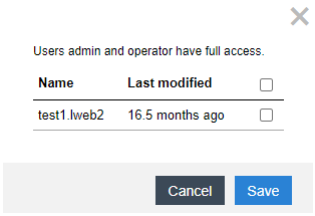


Figure 114: Assign selected projects to lweb users.

3.8 L-WEB

3.8.1 Installation

This configuration page provides a download link to the L-WEB application installer and a listing of L-WEB projects available on the device (see Figure 115). Clicking on **Install** will download the installer for LWEB-803 and start the installation process. Clicking on the Web icon will open the LWEB-802 project in a Web browser. This option is only available, if the L-WEB project has been stored as an lweb2 file. Please refer to the LINX Configurator User Manuel [1] for more information on working with the L-WEB visualization.

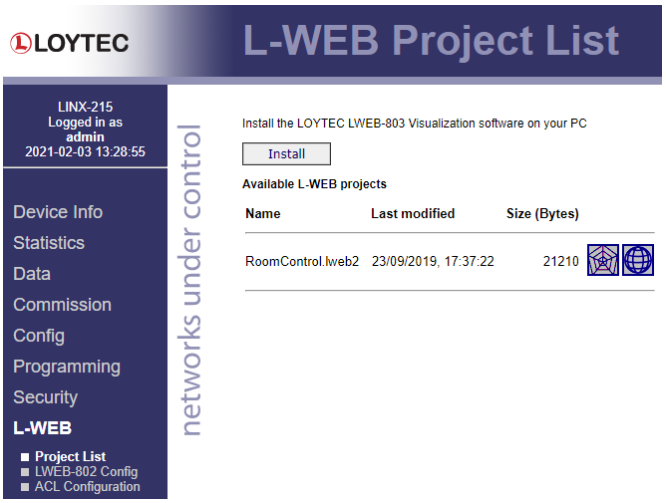


Figure 115: L-WEB Page.

3.8.2 LWEB-802 Config

To operate an LWEB-802 project in a Web browser, the LWEB-802 application must be loaded from a server URL that hosts it. The LWEB-802 configuration page allows specifying the URL used for LWEB-802 projects hosted on the device. The default setting is the LOYTEC Web site, which hosts the official LWEB-802 application release.

For installations that don't have Internet access or that require a special version of the LWEB-802 application for testing, the application can also be hosted on the Web server of the device. The following options can be configured:

- **LOYTEC Website**: This is the default setting. The URL points to the official LWEB-802 application released on the LOYTEC Web site.
- **Pre-installed on device**: With this setting, a pre-installed local version of the LWEB-802 application is used directly from the device.
- **Pre-installed & auto-update**: With this setting, the pre-installed version is used as well. However, this version will be updated automatically as soon as a newer LWEB-802 version is available on the LOYTEC website. An update check can also be triggered by clicking on the update icon .
- **User-installed on device**: Choose this setting to store a user-supplied version of the LWEB-802 application on the device.
- **Custom URL**: Choose this setting, if the LWEB-802 application has been loaded onto a Web server other than this device. Enter the appropriate URL.

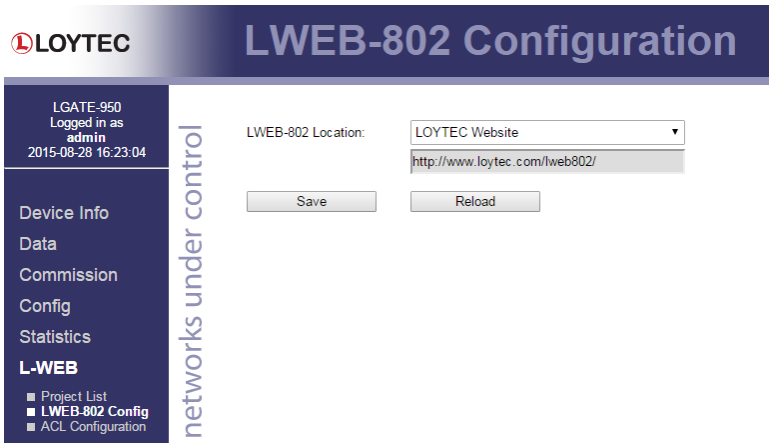


Figure 116: LWEB-802 Configuration Page.

3.8.3 Access Control List

The device provides a security feature to restrict access to the OPC XML-DA server from the Internet. This feature is based on an access control list (ACL). An example of the ACL configuration is shown in Figure 117.



Figure 117: OPC XML-DA Server Access Control List (ACL).

The user can add and delete entries to the ACL. Each entry contains a source specification, which consists of an IP address and an IP mask, and an action (allow or deny). For specifying single hosts use the IP address and the mask '255.255.255.255'. For an address range specify an appropriate mask. For example use '10.0.0.0' and the mask '255.255.255.0' to specify all hosts with IP addresses '10.0.0.xxx'. To specify all IP addresses use '0.0.0.0' and the mask '0.0.0.0'.

The ACL is evaluated from specific host entries down to wider ranges. When adding new entries the ACL is automatically sorted, having the most precise definition at the top and the most general one at the bottom. The default behavior is to allow packets from all IP addresses. This is also the default entry in the ACL.

The example shown in Figure 117 specifies the following behavior:

1. Allow requests from the device 192.168.1.64

2. Otherwise allow requests from devices in the network 10.0.0.xxx

3. Otherwise deny requests from all (other) IP addresses. Note, that a "deny" overrules an "allow".

3.9 L-IOB Host and Local I/Os

A L-INX, L-ROC, LIOB-48x/58x, LIOB-AIR can act as a L-IOB Host for a LIOB-45x/55x device, providing a Web interface to configure, operate, and test the connected L-IOB device. It also provides statistics information about the connected L-IOB device. All L-IOB I/O controllers, LIOB-AIRx, and LROC-40x are additionally equipped with local I/Os, which are also covered by this section.

3.9.1 LIOB-IP Bus

To be able to connect a LIOB-45x/55x device over the LIOB-IP bus, the firmware version of the LOYTEC device must be 4.8 or higher. After a firmware upgrade, the LIOB-IP support must be enabled in the Web-UI (menu “L-IOB / Upgrade”). The LIOB-IP bus will then be enabled by default, as shown in Figure 118. It is possible to disable the LIOB-IP bus entirely by un-checking the **LIOB-IP** checkbox. The corresponding UDP/TCP ports 16028 and 16029 will then not be open anymore. Observe that the LIOB-IP bus only acts as a virtual medium, connecting the LIOB-45x/55x device over Ethernet/IP. The rest of the configuration must be done as described in Section 3.9.2.

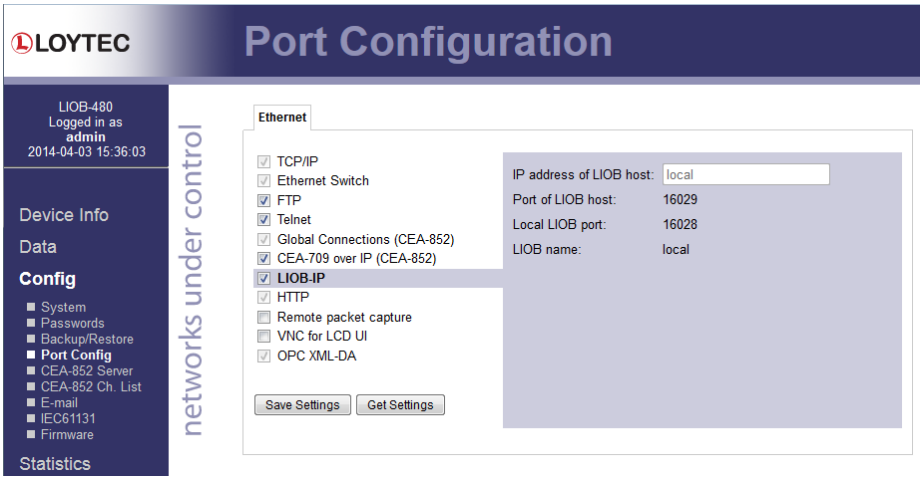


Figure 118: LIOB-IP Bus

3.9.2 L-IOB Installation Page

The **L-IOB Installation** page for the LIOB-Connect bus is shown in Figure 119. The **L-IOB Installation** page for the LIOB-FT or LIOB-IP bus is shown in Figure 120. It works similar to the Installation page of the LIOB-Connect bus with a few differences.

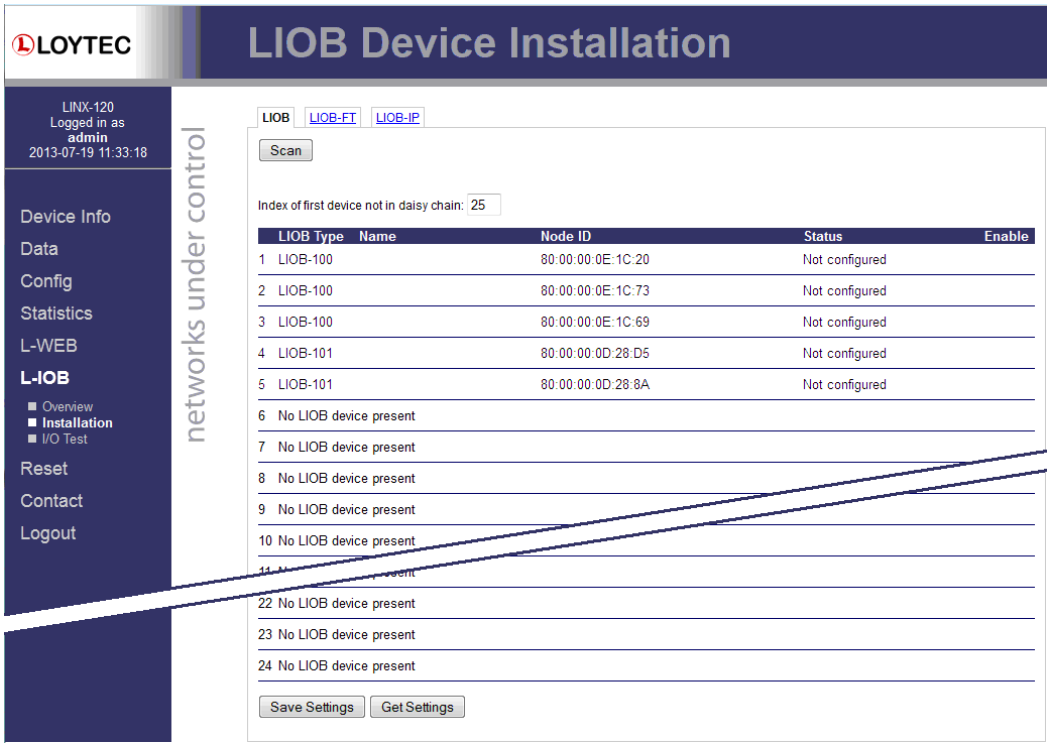


Figure 119: LIOB-Connect Device Installation and Scan.



Figure 120: LIOB-IP Device Installation and Scan

Since the LIOB-FT/IP bus does not have a mechanism to automatically enumerate connected L-IOB devices, the user must determine the order manually. This is done either by setting the Station IDs in the LCD UI of the L-IOB devices or by entering the Node IDs of the connected L-IOBs as shown in Figure 120 and clicking **Save Settings**. By clicking **Scan**, the order as currently configured in the L-IOB devices will be detected and displayed. The Node IDs can also be setup by clicking **Get Node ID** and then pressing the status button of the corresponding L-IOB device. Whenever changes have been made in the Web UI, in the end the **Save Settings** button must be clicked to configure the connected L-IOB devices accordingly.

3.9.3 L-IOB Scan and Configuration Run

Even without any configuration, the L-IOB bus can be scanned to check which L-IOB devices are connected to the L-IOB host. This can be done by clicking **Scan**. During the scan process, the status of the connected L-IOB devices is shown in the web page. At the end, the page should e.g. look like Figure 119. In this case, 3 LIOB-100 devices and two LIOB-101 devices have been found. For all shown L-IOB devices, the **Name** is blank and the **Status** is "**Not configured**" since the L-IOB host does not have a configuration downloaded yet.

If a configuration is downloaded to the L-IOB host using the Configurator software, a configuration run is started automatically and, if the configuration matches the physically attached L-IOB devices, all L-IOB devices should go online. The configuration run can also be started manually at any time by clicking **Save Settings**. This is required e.g. when a L-IOB device is replaced without power-cycling the L-IOB host. Figure 121 shows the L-IOB installation page after clicking **Save Settings**.



Figure 121: L-IOB Configuration Run

The L-IOB Installation page will also show configuration errors. In Figure 122 e.g. the last L-IOB device could not be detected.



Figure 122: Missing L-IOB Device

This could be caused by a communication problem or by a physically missing L-IOB device. In case it is OK that this device is missing, it must be disabled in the Web UI by un-checking the corresponding **Enable** checkbox and clicking **Save Settings** again, see Figure 123.



Figure 123: Disabled L-IOB Device

3.9.4 L-IOB Device Information and Statistics

By clicking on one of the L-IOB device links in the **Name** column of the L-IOB Installation page, the L-IOB device information and statistics page can be shown for that device, see Figure 124. Using the buttons **Reboot device** and **Reset to factory defaults**, the L-IOB device can be rebooted or reset to factory defaults.

The **Device information** part shows device specific configuration properties and some live values of the device (CPU load, System temperature & voltage). The system log of the L-IOB device can be displayed by clicking on **system log**.

The **L-IOB communication statistics** part shows statistics information of the communication bus. These values are mainly used for support and debugging.

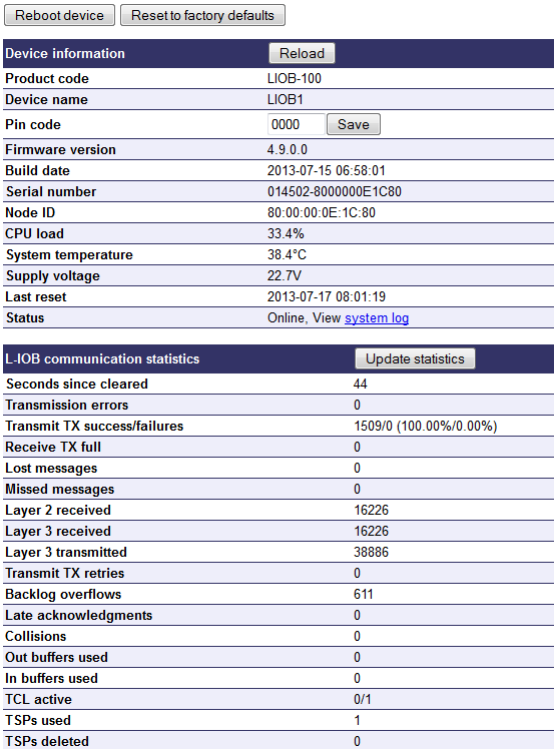


Figure 124: L-IOB Device Information and Statistics

Observe that if the L-IOB device is unconfigured (not part of the L-IOB host configuration), the L-IOB communication statistics table as well as some information in the Device information table cannot be displayed.

3.9.5 L-IOB Overview Page

The **L-IOB Overview** page provides a quick overview of all L-IOB devices and their I/Os. This page is available for the local I/Os as well as the connected LIOB-45x/55x device. Figure 125 shows the Overview page for the local I/Os. With **Reset All Count Values**, the counter inputs as well as the run hours and energy count values of all outputs can be reset.

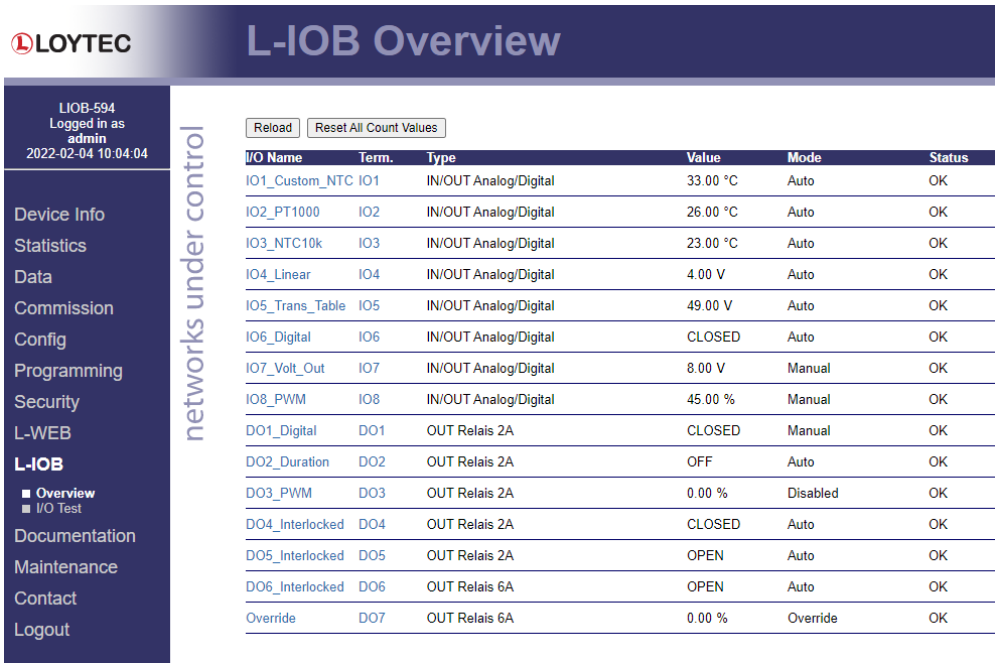


Figure 125: L-IOB Overview

The live value and a few properties are shown for each I/O of the L-IOB device. The operating mode of each I/O can be changed in the **Mode** column. The **Value** column always shows the corresponding effective value (e.g. the override value in override mode). In case of manual operating mode, the manual value is displayed and can be changed in the **Value** column.

By clicking on the link in the **I/O Name** column, a detailed view of each I/O can be invoked, see Figure 127. Please refer to the LINX Configurator User Manual [1] for a detailed description of all I/O properties. After changing configuration properties, the user must click **Save Settings** to activate the new configuration in the L-IOB device.

While a device has not yet been configured, all relay outputs (DO) will be set into "Unconfigured" mode where manual control of the relays is not possible, see Figure 126. As soon as the device is configured, the relay outputs can be used normally.

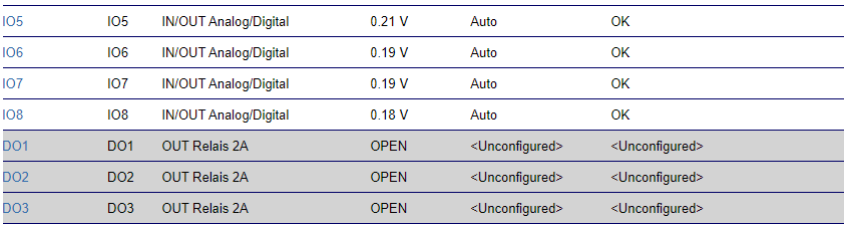


Figure 126: Unconfigured Mode

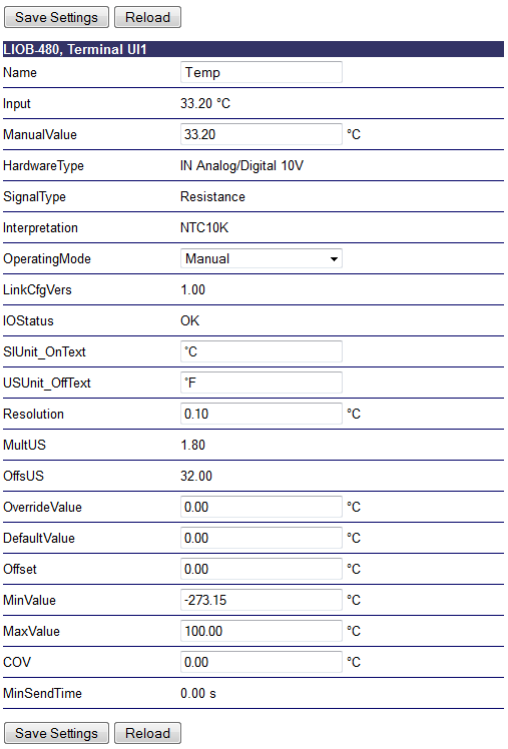


Figure 127: L-IOB I/O Details

3.9.6 L-IOB I/O Test Page

The **L-IOB I/O Test** page provides the possibility of documenting tests of the connected actuators and sensors. This page is available for the local I/Os as well as connected L-IOB I/O modules. Figure 128 shows the L-IOB I/O test page of the local I/Os.

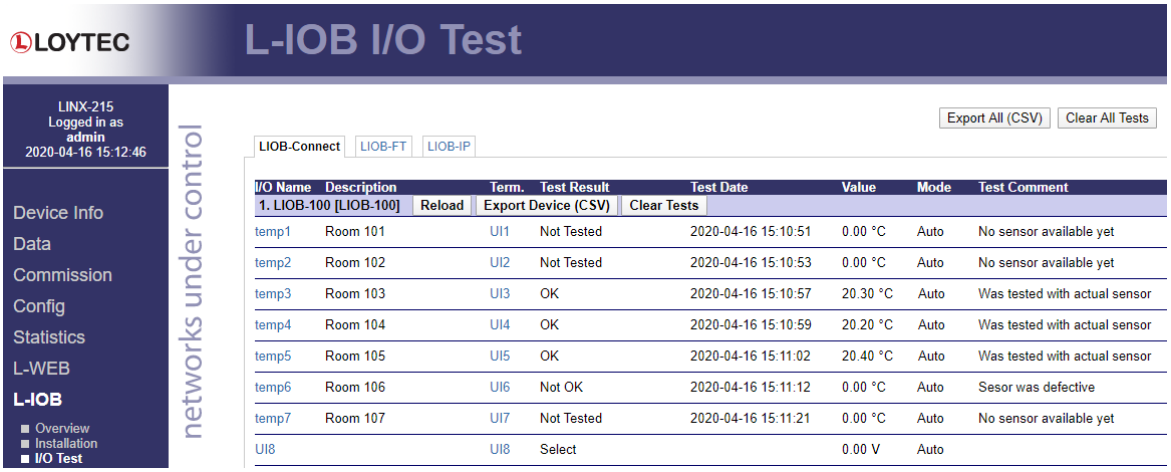


Figure 128: L-IOB I/O Test

For each I/O, the **Name**, **Description** and **Terminal** is shown for identification. Then a **Test Result** (Not Tested, OK, NOT OK) can be chosen. The **Test Date** will then be set automatically but can be manually changed afterwards. An additional **Test Comment** can be entered. This data will be stored persistently in the device until it is explicitly cleared or the type of the connected L-IOB device changes because of a new host configuration. To explicitly clear the test information, the buttons **Clear Tests** or **Clear All Tests** are used. The test information can also be exported to a CSV file by using **Export Device (CSV)** or **Export All (CSV)**.

3.10 Documentation

The documentation page allows to access documentation related to the device. See Section 3.11.3 on how to configure documentation links and upload documentation files accessible via this page.

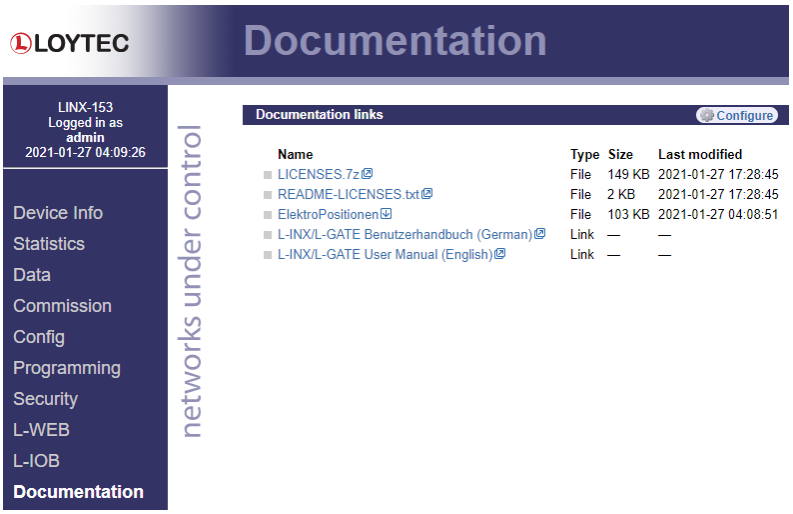


Figure 129: Documentation Page.

Note: *The Documentation page and all files available on it are accessible for all users (incl. Guest).*

3.11 Maintenance

3.11.1 Backup and Restore

A configuration backup of the device can be downloaded via the Web interface. Press the backup link as shown in Figure 130 to start the download. The device assembles a single file including all required files. A file requestor dialog allows specifying the location where the backup file shall be stored.

Some contents of the backup archive can be controlled by the option check boxes. By default users, passwords and IP settings are included. Trend log data can be added by setting the check box. When clearing the check box from passwords or IP settings, the respective items are excluded from the backup archive.

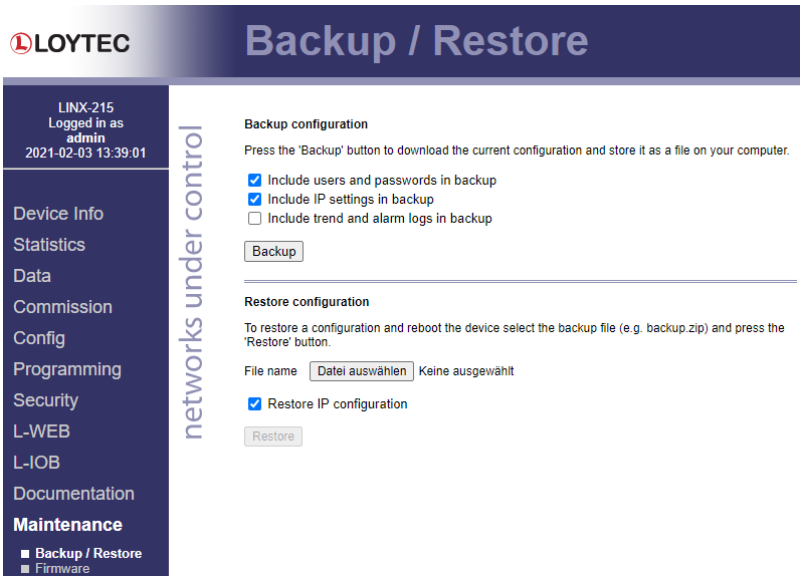


Figure 130: Backup/Restore page.

To restore the device settings, simply select a previously generated backup file in the **Restore Configuration** section of the page by clicking the button next to the **Filename** field. Then press the **Restore** button. By leaving the restore check boxes unset, the respective information is excluded from restore operation.

The backed up configuration data consists of:

- IP settings, if this option is enabled,
- Users and passwords, if this option is enabled,
- Device settings (time zone, e-mail config, etc.),
- Data point configuration and persistent values,
- Historical values in trend logs and alarm logs, if this option is enabled,
- CEA-709 binding information,
- BACnet server objects and client mappings,
- L-IOB configuration and parameters,
- AST settings,
- L-WEB configuration and custom Web pages,
- IEC61131 logic program and retain variables,
- Uploaded documentation and documentation links.

3.11.2 Firmware

The firmware page allows upgrading the device's firmware over the Web interface. It offers two options:

- **Web Update**: With Web update the device searches for the latest available firmware on the LOYTEC server. Click on the refresh symbol, if no latest version is displayed. Please note, that the device must have a DNS server configured to find the LOYTEC server. Click on the **Install** button to upgrade your device.

- **Local file**: Update the device from a local disk file. For doing so, choose a .dl file on you hard drive and then click on the **Start Update** button.



Figure 131: Firmware upgrade over the Web interface.

In both cases a device backup will be created and stored in the local download folder of the Web browser before the firmware upgrade starts. If no backup shall be created, deselect the checkbox **Automatically download a backup**.

3.11.3 Documentation

The **Documentation** page in the **Maintenance** menu allows uploading documentation files or configuring links to external documentation (e.g. Wiring plans, etc.). The documentation configured on this page is accessible via the **Documentation** menu (see Section 3.10).

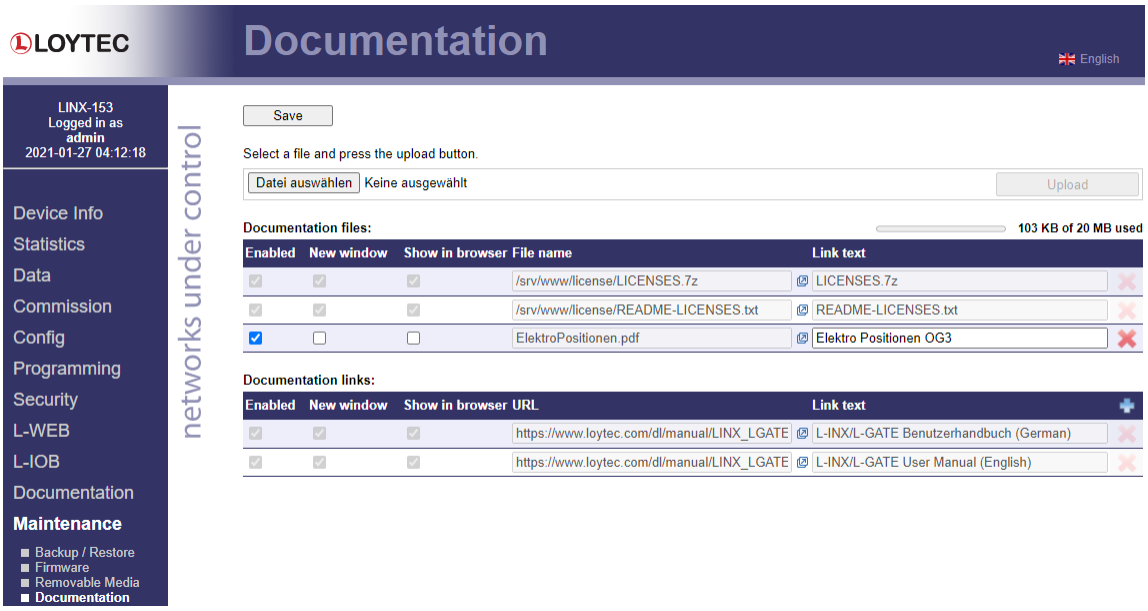


Figure 132: Upload and configure documentation.

To upload a documentation file click on the **Choose File** button. This opens a file dialog. Chose the file to upload. Click on the **Upload** button to start the upload of the selected file. After the upload is completed the file appears in the **Documentation files** section. Enter a link text used to display the uploaded file on the **Documentation** page.

To add a documentation link, click on the symbol in the header row of the **Documentation links** section. Enter the URL and the text used to display the link on the **Documentation** page.

Links and files can be set active and inactive on the **Documentation** page by checking the **Enabled** check box. Inactive entries are not displayed on the **Documentation** page. The check box **New window** determines if the link or file is opened in a new browser tab. If **Show in browser** is checked the browser will try to render the file in the browser, otherwise it will try to download the file. To remove a link or file click on the symbol on the right side of the row. To commit your changes click on the **Save** button.

3.11.4 Rebooting and Clearing Project Data

The menu item Maintenance allows the following essential operations to reboot the device or clear data:

- Rebooting the device from a remote location. Use **Cold Reboot** to reboot the device like after a power loss, while the regular **Reboot Device** is faster and restarts the application only.

- C**lear** removes the entire project configuration from the device. This clears all configuration and settings data, except those settings made under the Config, Security, and Documentation menus. It leaves the IP settings intact.

3.11.5 Safe Reboot

Whenever a setting has been changed that affects connectivity to the device's Web interface (e.g. IP address) the next reboot is executed as a safe reboot. This is indicated as shown in Figure 133.



Figure 133: Safe reboot notice.

When resetting into safe reboot mode, the user needs to log in within the next 5 minutes after the reboot. A list of possible new IP addresses to this device is displayed to help navigating to the device. If no login is detected (e.g., because the new IP setting breaks connectivity) the device will revert to the last working settings.

Sometimes, a safe reboot is not possible. For example, when re-configuring a device to use a different static IP in another network. In this case, check the box **Skip safe reboot this time** and the device performs a regular reboot.

3.12 Contact, Logout

The **Contact** item provides contact information and a link to the latest user manual and the latest firmware version. The **Logout** item closes the current session.

4 The CEA-709 Router

LOYTEC devices, which are equipped with a standard CEA-709 router (i.e., an embedded L-IP), connect the FT port and the CEA-852 port. Depending on the use case, the CEA-709 router supports different operating modes how packets are routed between the CEA-709 side and the IP-852 side. LOYTEC devices with the router option also contain a configuration server (CS) to manage members on an IP-852 channel.

4.1 CEA-709 Router

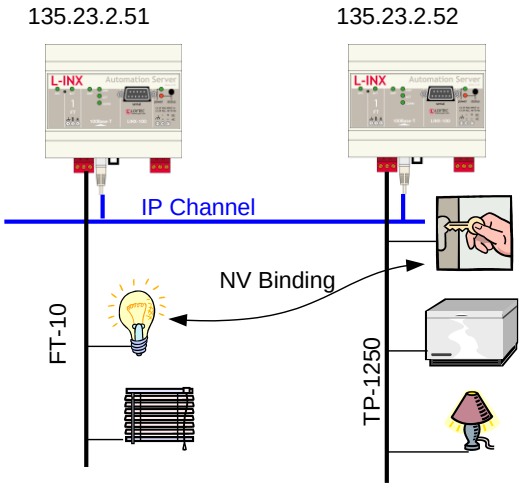


Figure 134: The L-INX supports different methods to route packets between the CEA-709 and IP-852 channel.

Depending on the CEA-709 router configuration (see Section 3.5.14) the CEA-709 router supports 4 different methods to route packets between the CEA-709 and the IP-852 channel. Those operating modes are listed below and described in more detail in the subsequent sections.

- Configured Router: The device acts like a standard CEA-709 configured router (*i*.LON 1000/600 alike)
- Smart Switch: The device acts as a self-learning plug&play router (“smart switch mode”)
- Store-and-Forward Repeater: To freeze a learned configuration and operate the switch based on the existing forwarding tables, disable group learning and Subnet/Node learning.
- Smart switch with no broadcast flooding: Set Subnet/Node Learning to “subnet”. In this mode the router learns the network topology but doesn’t flood subnet broadcasts.

4.1.1 Configured Router Mode

In this operating mode, the router acts like a standard configured router, which can be configured with standard network management tools like LonMaker or NL-220. This operating mode is compatible with the *i*.LON 1000 and the *i*.LON 600.

This operating mode uses the "channel routing" routing strategy on the IP channel. In this mode the device is fully compatible with *i*.LON 1000/600 devices. This operating mode should also be used in networks with more than 10 IP devices on one IP channel and heavy network traffic on the IP channel (more than 500 packets/s) since channel routing sends the IP packet only to the IP-852 device(s) that connect to the CEA-709 node(s) addressed in this IP packet and not to all IP-852 devices on the IP channel. This is the standard operating mode.

4.1.2 Smart Switch Mode

The router can be configured to act as a learning switch in a CEA-709 network. This operating mode is called smart switch mode. In this operating mode, the router decides if the message has to be forwarded or not, based on the destination address of a message. Thus, it isolates local network traffic (e.g., in case of heavily loaded networks).

Important:	***This operating mode doesn't support network loops!***

Important:	***Whenever a network is reconfigured, it is recommended to clear the forwarding tables in the device by pressing the status button for at least 20 seconds.***

The router supports learning of up to 4 Domains.

Note:	*All messages, which are received on an unknown domain, are forwarded to all ports!*

The subnet/node learning algorithm supports segmentation of the network traffic on a subnet/node basis. Thus, the user does NOT need to take care of any subnets spanning multiple physical channels. Even when a node is moved from one channel to another, the router keeps track and modifies its forwarding tables accordingly.

Note:	*All messages with a destination subnet/node address not yet learned are forwarded!*

The router supports group learning. Groups can span multiple router ports.

Note:	*Group learning only works for messages using acknowledged or request/response service.*

Note:	*All messages with a destination group address not yet learned are forwarded!*

The router has no learning strategy for broadcast addresses. As a result, all subnet or domain wide broadcasts are always forwarded. If subnet wide broadcasts shall not be forwarded, please use the smart switch operating mode without subnet broadcast forwarding (see Section 4.1.4).

The router has no learning strategy for unique node ID addresses. Node ID addressed messages are always forwarded.

This operating mode uses the "channel routing" strategy on the IP channel to distribute IP packets. It uses flooding to send all packets on the IP channel to all IP devices on this IP channel. The advantage of this operating mode is that it is fully plug&play and no router configuration is required. The disadvantage is that this operating mode doesn't scale very well with larger networks. We do not recommend this operating mode for IP channels with more than 10 IP-852 devices and packet rates of more than 500 packets/s. Please use the configured router mode from Section 4.1.1 for larger IP channel configurations.

Further, it is recommended to configure a multi-cast group for routers in the smart switch mode to reduce the traffic burden and improve scalability. Refer to Section 4.5 on how to configure the device to use multi-cast.

4.1.3 Store-and-Forward Repeater

The router can be configured to operate in a repeater mode, where all messages are forwarded regardless of the address format.

This operating mode uses the "channel routing" strategy on the IP channel to distribute IP packets. It uses flooding to send all packets on the IP channel to all IP devices on this IP channel. The advantage of this operating mode is that it is fully plug&play and no router configuration is required. The disadvantage is that this operating mode doesn't scale very well with larger networks. We do not recommend this operating mode for IP channels with more than 10 router devices and packet rates of more than 500 packets/s.

Further, it is recommended to configure a multi-cast group for routers in repeater mode to reduce the traffic burden and improve scalability. Refer to Section 4.5 on how to configure the device to use multi-cast.

4.1.4 Smart Switch Mode with No Subnet Broadcast Flooding

This operating mode is the same as the smart switch mode from Section 4.1.2 with the only difference that subnet wide broadcasts are not flooded in this mode. This operating mode can be used in large network installations where the network management tool uses group overloading to replace group addresses with subnet wide broadcasts. In this operating mode, the network installer must ensure that one subnet address may only exist behind one and no more than one network port. This condition is met if nodes are installed using an LNS based tool, on different channels that are separated with a router shape.

This operating mode uses the "channel routing" strategy on the IP channel to distribute IP packets. It uses flooding to send all packets on the IP channel to all IP devices on this IP channel. The advantage of this operating mode is that it is fully plug&play and no router configuration is required. The disadvantage is that this operating mode doesn't scale very well with larger networks. We do not recommend this operating mode for IP channels with more than 10 devices and packet rates of more than 500 packets/s.

Further, it is recommended to configure a multi-cast group for the router in the smart switch mode to reduce the traffic burden and improve scalability. Refer to Section 4.5 on how to configure the device to use multi-cast.

4.2 CEA-852 Device of the Router

Every L-INX acts as a device on the IP channel. It either needs to contact a configuration server or a configuration server needs to contact the device in order to set up the proper routing tables. Before a device can become a member of the IP-852 channel it needs to have proper IP settings (see Section 3.5.3):

- IP address/netmask/gateway (either via DHCP or manual entry), see Section 3.5.3
- Auto-NAT or manual NAT address if used behind a firewall/NAT router, see Section 3.5.12
- MD5 secret if authentication is required, see Section 3.5.12

Please consult Sections 3.5.3 and 3.5.12 on how to setup a CEA-852 device.

The CEA-852 device can be used together with the PC-based *i*.LON Configuration Server utility or with any LOYTEC configuration server. If multiple CEA-852 devices behind one NAT router are added, the Auto-NAT setting in the CEA-852 devices is recommended to be

used with the L-INX configuration server or an L-IP configuration server. Please refer to the following sections on how to setup the device and the configuration server.

If the "Auto member" feature is enabled in the configuration server, the CEA-852 device can add itself to the IP-852 channel without explicitly adding the device at the configuration server. Note, that enabling auto member is a potential security hole since any device can add itself to the IP-852 channel.

4.3 Configuration Server for Managing the IP-852 Channel

4.3.1 Overview

Every logical IP-852 channel requires one configuration server that manages all CEA-852 devices (LINX-121, L-IP, LOYTEC NIC852, *i*.LON 1000, *i*.LON 600, LonMaker, etc.) on this channel. A simple example is shown in Figure 135. A configuration server keeps a list of all devices on a logical IP-852 channel and distributes the routing information between those devices. If a device wants to join an IP-852 channel, it needs to register itself at the configuration server. Traditionally, a dedicated Windows PC is used to act as the configuration server. The L-INX contains an embedded configuration server and can therefore replace the PC.

The configuration server can be enabled in the CEA-852 server configuration menu in Section 3.5.15. This configuration server can manage one IP-852 channel and up to 256 devices on this IP-852 channel. In order to setup the configuration server, one must specify the following parameters:

- IP address/netmask/gateway (either via DHCP or manual entry), see Section 3.5.3
- NAT address if used behind a firewall/NAT router, see Section 3.5.12
- MD5 secret if authentication is required, see Section 3.5.12
- Enable the configuration server, see Section 3.5.15 (server LED lights up green)
- A list of IP-852 channel members, see Section 3.5.16.

Note:	*If the L-INX is also used as a configuration server it needs a fixed IP address.*

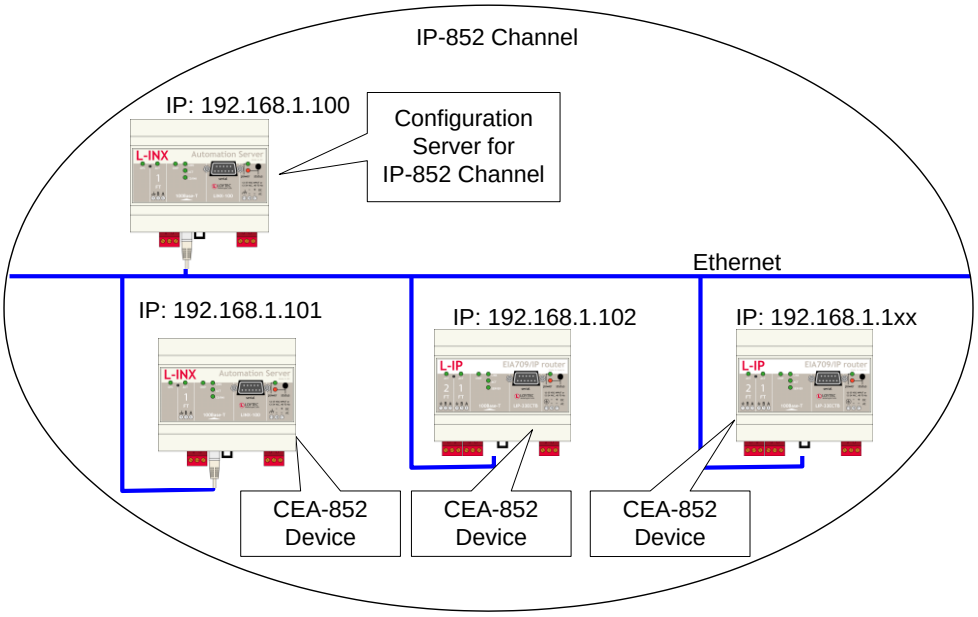


Figure 135: The configuration server manages the devices on an IP-852 channel.

4.3.2 Configuration Server Contacts IP-852 Device

In this scenario, the IP-852 device needs the following parameters set in order for the configuration server to contact the device. The remaining parameters are retrieved from the configuration server.

- IP address/netmask/gateway (either via DHCP or manual entry), see Section 3.5.3
- Auto-NAT or manual NAT address if used behind a firewall/NAT router, see Section 3.5.12
- MD5 secret if authentication is required, see Section 3.5.12

If multiple CEA-852 devices behind one NAT router are added, the Auto-NAT setting in the L-INX is recommended to be used with the L-INX configuration server.

4.3.3 IP-852 Device Contacts Configuration Server

In this scenario, the IP-852 device needs the following parameters set in order to contact the configuration server. The remaining parameters are retrieved from the configuration server.

- IP address/netmask/gateway (either via DHCP or manual entry), see Section 3.5.3
- Auto-NAT or manual NAT address if used behind a firewall/NAT router, see Section 3.5.12
- MD5 secret if authentication is required, see Section 3.5.12
- Configuration server IP address and port number, see Section 3.5.12

If the “Auto member” feature is enabled in the configuration server, the CEA-852 device can add itself to the IP-852 channel without explicitly adding the device at the configuration server. Note, that enabling auto member is a potential security hole since any device can add itself to the IP-852 channel.

4.3.4 Using the Built-In Configuration Server

For security purposes, the configuration server contacts each CEA-852 device on the IP-852 channel. Therefore, one must enter a list of all channel members in the CEA-852

Configuration Server menu (see Section 3.5.16). This ensures that no unwanted device can join the IP-852 channel.

Note that also *i*.LON 1000/600, VNI and LOYTEC NIC852 based network nodes (e.g., LonMaker or NL-220 applications) can join the IP-852 channel managed by the configuration server. Note that the built-in configuration server should be used if LOYTEC CEA-852 devices are communicating across firewalls/NAT routers.

For adding multiple devices behind a NAT router, the configuration server supports the extended NAT mode (see Section 4.4.2). The configuration server automatically switches the channel mode to extended NAT if needed. Note that the *i*.LON 600 must be configured with the *i*.LON CS to extended NAT mode before adding the *i*.LON 600 to the configuration server, because the *i*.LON 600 does not switch to that mode automatically.

4.4 Firewall and NAT Router Configuration

The CEA-709 router can be used behind a firewall and/or NAT (Network Address Translation) router as shown in Figure 136. Note, that in general, only one CEA-852 device can be used behind the NAT router. This mode of operation is referred to as “Standard” channel mode. It is fully compliant with CEA-852.

LOYTEC’s newer devices such as the L-IP and the L-INX family support more than one CEA-852 channel member behind a NAT router. This mode of operation is referred to as “Extended NAT” channel mode. This mode introduces extensions to the standard mode which need to be supported by all members. Other devices supporting the extended NAT mode are the *i*.LON 600. See Section 4.3.4 on compatibility with the *i*.LON 600.

4.4.1 Automatic NAT Configuration

In order to use the L-INX behind a firewall, the public NAT address and the local IP address must be set in the IP configuration menu (see Section 3.5.3). By default, the NAT address is determined automatically when adding the L-INX to the channel in the configuration server. Alternatively, the NAT address can be configured manually. Furthermore, the NAT router must be configured to forward ports 1628 and 1629 for UDP and TCP packets to the private IP address of the L-INX (192.168.1.100 in Figure 136). In summary we can say, the following parameters must be set in order to operate a L-INX behind a NAT router.

- Specify the IP address (private IP address: 192.168.1.100),
- Specify the gateway address (e.g., 192.168.1.1),
- Specify the NAT address (public IP address: 135.23.2.1) or use automatic NAT router discovery,
- Enable port forwarding for ports 1628 and 1629 in the NAT router for TCP and UDP,
- Enable the SNTP port 123 in the firewall if SNTP is used.

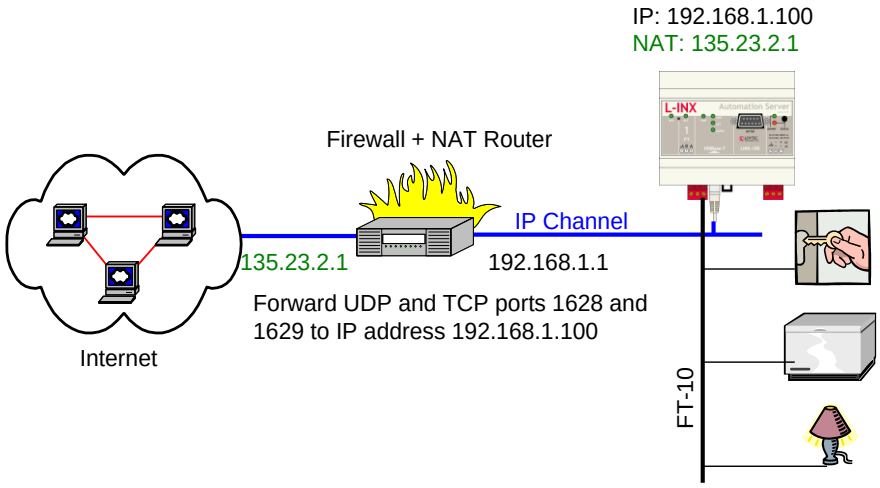


Figure 136: Operating a L-INX behind a NAT router and firewall.

Note that a L-INX must be used as configuration server when the device is installed behind a firewall or NAT router. The L-INX with the configuration server can also be located behind a firewall.

4.4.2 Multiple IP-852 Devices behind a NAT: Extended NAT Mode

When using more than one IP-852 device behind a single NAT router, the recommended method in the L-INX configuration server is to use the extended NAT mode. This mode requires that all devices support this feature. Currently these are L-INX with CEA-709 router, L-IP 3.0, *i*.LON 600, the NIC852 PC software and other CEA-852 capable devices from LOYTEC. If there are other devices in the channel, this method does not work. Incompatible devices are disabled from the channel in this case. Please refer to the classic method in Section 4.4.3 to setup this network.

When using multiple devices behind a NAT router, each device needs a separate port-forwarding rule in the NAT router. This implies that each device must use a unique client port (e.g., 1628, 1630, 1631, etc). The port-forwarding rules must be setup so that each port points to one of the IP-852 devices. In the L-INX, change the client port in the CEA-852 device configuration menu. Figure 137 shows an example configuration for three L-INX devices behind the NAT router 135.23.2.1.

It is recommended that both ports 1628 and 1629 are forwarded to the same private address. It is then also possible to turn on the configuration server behind a NAT router. In this case, activate the CS on the L-INX which has port-forwarding to 1628 and 1629. In the example in Figure 137, the L-INX with private address 192.168.1.100 also acts as a configuration server.

If the CS is activated on a L-INX behind a NAT router, the NAT router must have a fixed public IP address. The L-INX with the CS also cannot use automatic NAT discovery. In this case, enter the NAT address of the NAT router manually in the IP configuration menu (Auto-NAT can no longer be enabled on a L-INX with a CS). To diagnose possible problems in the NAT configuration with port forwarding, use the enhanced communications test (see Section 3.2.5).

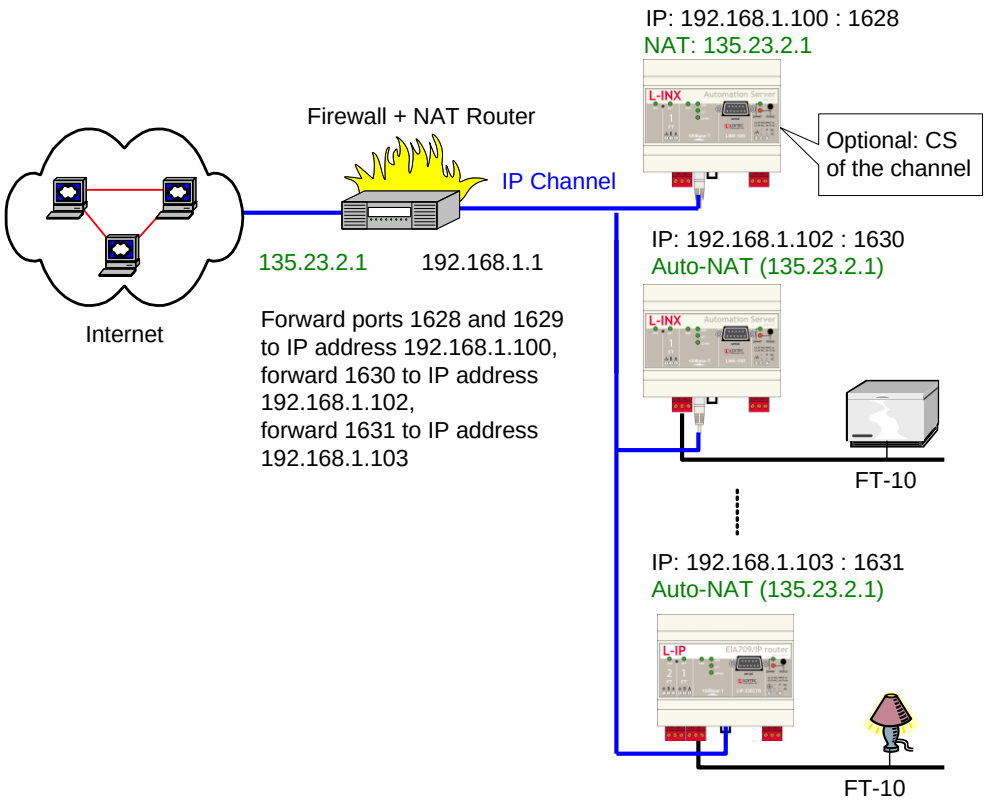


Figure 137: Multiple L-INX devices behind a NAT: Extended NAT Mode.

After the NAT router has been configured with the port-forwarding settings and the CS has been turned on, the channel members can be added. This can be done either through the Web interface of the CS.

In the Web UI, add the members with their private IP addresses and the client ports as defined by the port-forwarding. Then select the added member by checking the check box and select the action **Assign to NAT**. Enter the public NAT address of the NAT router. An example to add the two IP-852 devices in Figure 137 through the Web UI is depicted in Figure 138. To remove a device from a NAT router but not delete it, select it and choose **Remove from NAT** as the action.

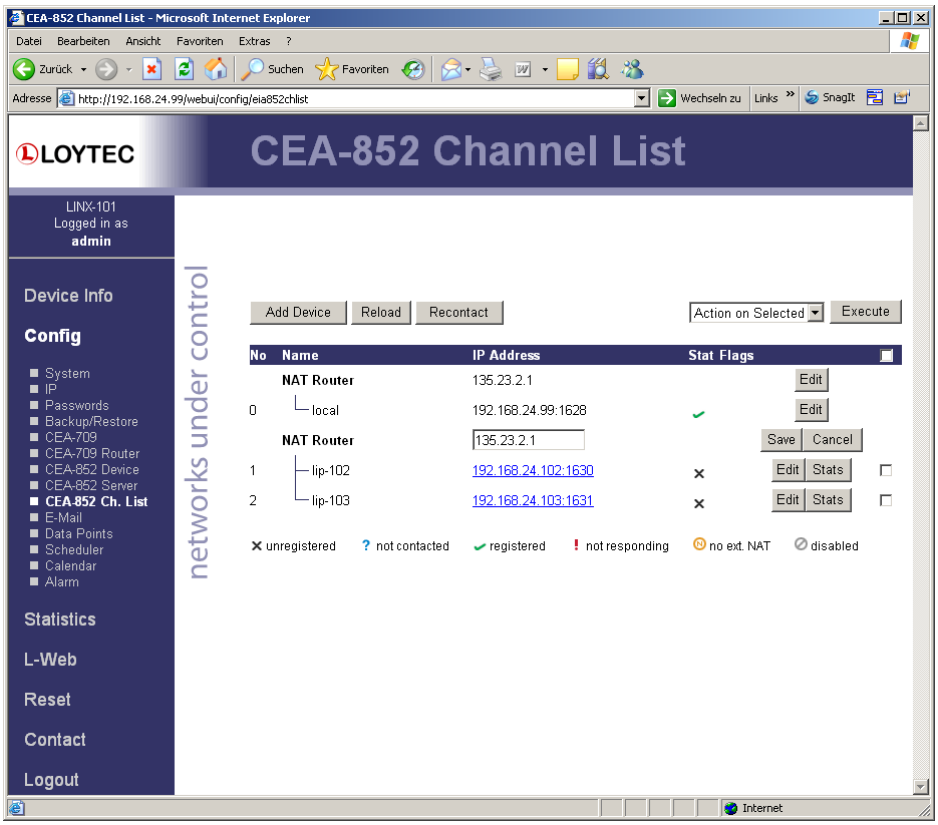


Figure 138: Adding a member with extended NAT Mode on the Web UI.

4.4.3 Multiple IP-852 devices behind a NAT: Classic Method

If more than one CEA-852 device must be used behind the NAT router and there are devices which do not support the extended NAT mode, we propose the setup from Figure 139.

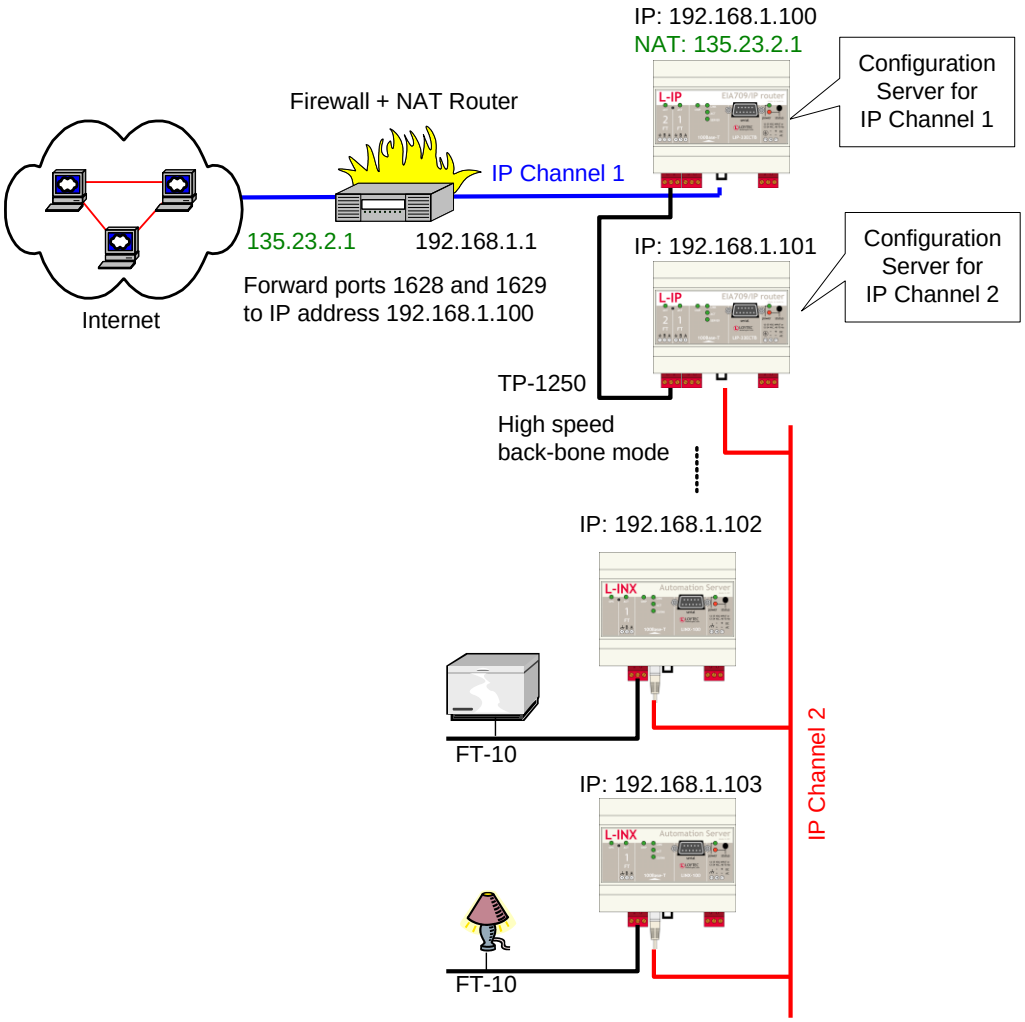


Figure 139: Application that uses multiple L-INX devices behind a NAT router firewall.

The L-INX with IP address 192.168.1.100 is member of IP Channel 1 and can be accessed through the Internet. The L-INX devices with IP addresses 192.168.101 to 192.168.1.110 form another logical IP Channel 2 that communicates with the devices on the IP Channel 1 over the TP-1250 channel, which is used in high-speed backbone mode for optimum networking performance. Note that devices on both IP Channels 1 and 2 can of course connect to the same physical network wiring. Furthermore, both IP Channels 1 and 2 must have a separate configuration server that manages the L-INX devices on the different channels. In the example in Figure 139, the L-INX with address 192.168.1.100 acts as the configuration server for IP Channel 1 and the L-INX with IP address 192.168.1.101 acts as the configuration server for IP Channel 2.

4.5 Multi-Cast Configuration

IP multi-casting is a feature of the IP protocol that allows one packet to be delivered to a group of IP hosts. To receive such multi-cast packets, each IP host must be member of a multi-cast group. This group is identified by a multi-cast address (e.g., 225.0.0.37) and a UDP port number.

The L-INX supports both unicast and multi-cast delivery of CEA-852 data packets. Using multi-cast is recommended when using the router in the Smart Switch Mode. For those devices, configure a multi-cast address in the IP configuration menu. Please contact your system administrator to obtain a valid multi-cast address for your network. Note, that all channel members must be configured with the same multi-cast address and use the same

client port (1628 is recommended). Also note, that multi-cast addresses cannot be routed on the Internet. They can only be used in a LAN or VPN environment.

If you configure multi-cast, there may be some devices, which do not support this feature. In this case, the device uses a hybrid scheme and sends unicast to those devices, which are not configured for multi-cast. Note, that the device determines automatically, when to switch to the multi-cast mode depending on what types of devices are in the channel and on the traffic burden for those devices. As a rule of thumb, multi-cast is used when there are only switches/repeaters in the channel and it is not used when there are only configured routers.

To detect if the device utilizes the multi-cast feature, contact the Extended CEA-852 device statistics in the statistics menu (Section 3.2.4). The entry “Channel Routing Mode” reads SL (send list) if packets are routed to the multi-cast group. It reads CR (channel routing) if the normal unicast method is employed. Also the entry “Multi-cast packets sent” in the CEA-852 device statistics menu (Section 3.2.4) counts the number of multicast packets transmitted to the group. If this item remains zero, no multi-cast is used by the device.

4.6 Remote LPA Operation

The L-INX supports remote LPA access. This means that a CEA-709 protocol analyzer connected to the Ethernet network can connect to the L-INX and record all packets on the CEA-709 channel (FT-10). Our LPA-IP supports this sophisticated feature. The functionality is shown in Figure 140.

The LPA-IP runs on a Windows PC that is connected to the Ethernet network. In a device selection window, one can e.g. select the L-INX with IP address 192.168.1.210 and display all packets on the FT-10 channel connected to the L-INX with IP address 192.168.1.210. For this operation, the LPA-IP does not need to be a member of the IP-852 channel. Note that this functionality is only available with LOYTEC CEA-852 devices.

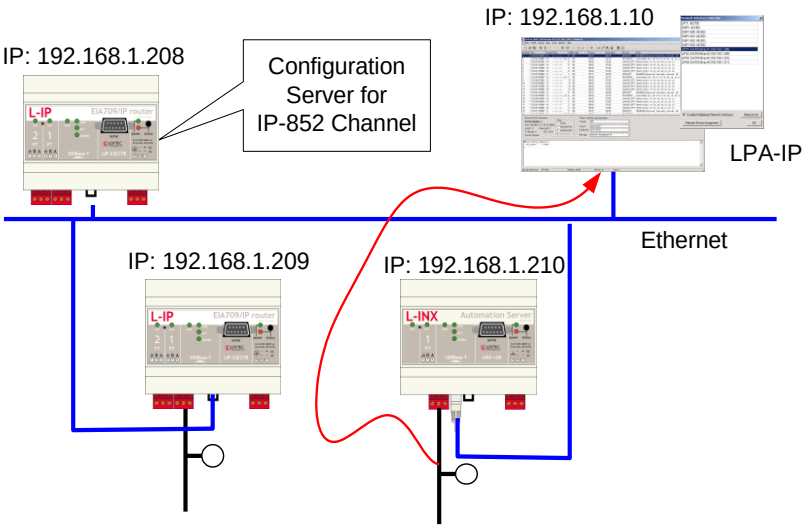


Figure 140: Remote LPA principle.

4.7 Internet Timing Aspects

If the CEA-709 router is used over the Internet or in a large Intranet with unpredictable network delays, the user should become familiar with the following advanced timing aspects. Channel Timeout is set in the configuration server whereas escrowing and aggregation are

set in the CEA-852 client device. The Channel Delay is a channel property of LNS and can be set in NL220, LonMaker or other network management tools.

Table 4 summarizes the timing values that must be set when operating the device under WAN conditions.

Timing Parameter	Value
Channel Timeout	Average ping delay + Aggregation Timeout
Escrowing (Packet Reorder Timer)	The smaller value of: 0.25*Channel Timeout or 64ms
Aggregation Timeout (Packet Bunching)	Typically 16 ms
Channel Delay in LonMaker	Average ping delay +10% + 2* Aggregation Timeout

Table 4: Advanced IP-852 timing parameters.

Please use a PC to determine the average ping delay between the different CEA-852 devices in the network. If multiple devices are communicating with each other always use the largest measured average ping delay for the input value for the calculations in Table 4.

Escrowing should be disabled in a LAN (0 ms). The Channel Delay in LonMaker should be set to 2*Aggregation Timeout in a LAN if MD5 is disabled.

In LANs, Channel Timeout is only required if MD5 authentication is enabled. Set Channel Timeout to 200 ms and Channel Delay to 20 ms.

4.7.1 Channel Timeout

The Channel Timeout is a property of the IP-852 channel. If a packet travels across this IP-852 channel for longer than what is specified in Channel Timeout in ms, the packet is discarded. The device always needs to synchronize with an SNTP timeserver when a Channel Timeout is set other than 0 ms.

Channel Timeout is highly recommended if MD5 authentication is enabled in order to prevent replay attacks. Set Channel Timeout to 200 ms and Channel Delay to 20 ms in a LAN environment. Please refer to Section 3.5.15 on how to enable or disable the Channel Timeout.

If an LNS based network management tool like LonMaker or NL220 is used on a network that has channel timeout enabled, please install an NTP client program (e.g., achron4.exe) on this PC that synchronizes the PC clock to the NTP time. Otherwise the PC clock and the clock inside the CEA-852 device will drift apart and communication between the PC and the device will terminate.

4.7.2 Channel Delay

Channel Delay is an LNS channel property that specifies the expected round-trip time of a message and its response. This value is used by LNS to adjust the protocol timers in the CEA-709 nodes. Please consult the documentation for your network management tool about the Channel Delay details.

4.7.3 Escrowing Timer (Packet Reorder Timer)

The Escrowing Timer or Packet Reorder Timer is an IP-852 channel property that specifies the amount of time the device will wait for an out-of-sequence IP packet to arrive. This parameter is important in WANs like the Internet, where packets pass many routers that can change the order in which packets arrive at the destination node. The default value is 64 ms.

Do not use the Escrowing Timer in LANs since the packet order is always guaranteed in a LAN. This will add unnecessary delays, which negatively impacts the performance of your CEA-852 devices if a packet is lost or destroyed.

Whether enabled or disabled, out-of-sequence packets are never sent to the CEA-709 channel. Please refer to Section 3.5.12 on how to enable or disable escrowing.

4.7.4 SNTP Time Server

Small IP networks like LANs have a small propagation delay for packets traveling in these networks. In this case it is not necessary to specify an SNTP server.

In larger IP-852 networks like the Internet with possibly long packet delays, one must specify an SNTP server to synchronize the local clocks of the CEA-852 devices. The local clocks must be synchronized to a common notion of time in order to make CEA-852 protocol features like Escrowing and Channel Timeout work properly.

The SNTP timeserver can be specified on the IP-852 channel level in the configuration server, which distributes the timeserver address to all CEA-852 devices on the IP-852 channel. A primary and a secondary SNTP server can be defined please refer to Section 3.5.12 and Section 3.5.15 on how to enable the SNTP server.

4.8 Advanced Topics

4.8.1 Aggregation

Aggregation (or packet bunching) is a technique that collects multiple CEA-709 packets into a single larger IP packet. Aggregation improves overall system performance since one IP-852 packets, now carries multiple CEA-709 packets und with the same number of IP-852 transactions, more CEA-709 packets can be exchanged between CEA-852 devices thus reducing protocol overhead. The Aggregation Timeout defines the time period in ms in which the transmitting device collects the CEA-709 packets before it transmits the CEA-852 packet over the IP-852 channel. Please refer to Section 3.5.12 on how to enable aggregation. Note, that aggregation adds a delay to the transactions but dramatically improves the throughput of your IP-852 channel. Use aggregation if you have a high channel load but can tolerate some additional propagation delay given by the aggregation time value.

4.8.2 MD5 Authentication

MD5 authentication is a method of verifying the authenticity of the sending device. Only devices that have MD5 enabled and use the same MD5 secret can share information with each other. If the configuration server has MD5 enabled, only devices that have MD5 enabled and use the same MD5 secret as the configuration server can join the logical IP-852 channel. Please refer to Section 3.5.12 and 3.5.15 for details.

4.8.3 Dynamic NAT Addresses

A common practice for Internet providers is to assign addresses on a per-session basis to a client. Each time a connection is established (e.g., an ADSL link is set up), the Internet provider may choose an IP address from a pool. Since this address will be the public address of a NAT router, the NAT address configured in the device would need to be updated. The Auto-NAT feature in the device permanently monitors the current NAT address. When the device detects a change in the NAT address it re-registers with the configuration server using this new address. This feature requires a LOYTEC configuration server (e.g., L-INX, L-IP) and “Roaming Members” enabled on that CS.

A consequence of this monitoring process is that the device contacts the CS every 45 seconds to probe for the NAT address. This causes a small amount of additional traffic on the Internet link. The Auto-NAT feature also causes any shut-down connection to be re-established. The NAT monitoring functions as a keep-alive for the connection. If neither the additional traffic

nor the automatic initiation of a new connection is tolerable, the Auto-NAT feature must be disabled and the NAT address configured manually. In this case, the Internet service provider needs to assign a fixed public IP address to the NAT router.

5 Remote Network Interface

5.1 RNI Function

Devices without the router provide a remote network interface (RNI) function, if the device is configured to use the FT interface (FT mode). In this mode the device provides a remote network interface, which appears like a LOYTEC NIC-IP it is intended to be used together with the LOYTEC NIC software. The RNI can be utilized for remote access and configuration as well as trouble-shooting with the remote LPA.

In particular, the RNI appears as a regular LOYTEC network interface on the PC. The LOYTEC NIC software needs to be installed to utilize this interface also in LNS-based applications such as NL220 or LonMaker. Using this software, the L-INX can act as a direct interface to its local FT channel to be managed by LNS or similar tools. For more information on how to configure the LOYTEC NIC software on the PC, please refer to the LOYTEC NIC User Manual [4].

5.2 Remote LPA Operation

The LGATE-950 and the L-INX supports remote LPA access through its RNI. This means that a CEA-709 protocol analyzer connected to the Ethernet network can connect to the L-INX and record all packets on the CEA-709 channel (FT-10). The LOYTEC LPA-IP supports this advanced feature. The functionality is shown in Figure 141.

The LPA-IP runs on a Windows PC that is connected to the Ethernet network. In the NIC-IP/RNI device selection window, one can for example select the device with IP address 192.168.1.210 and display all packets on the FT-10 channel connected to the device with IP address 192.168.1.210. Please consult our product literature for the LPA-IP to learn more about this IP-based CEA-709 protocol analyzer.

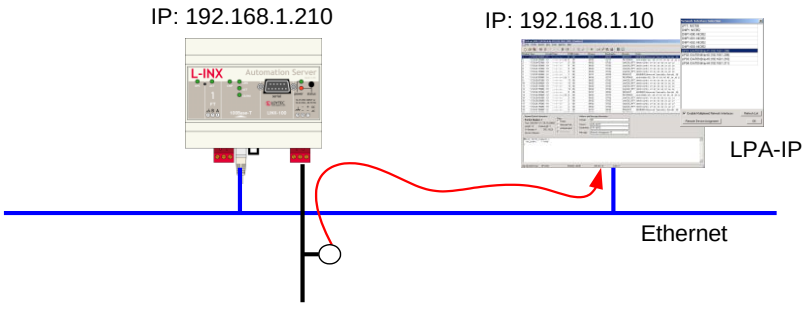


Figure 141: Remote LPA on the L-INX.

6 OPC Server

6.1 XML-DA OPC Server

6.1.1 Access Methods

LOYTEC devices with the built-in OPC server can expose data points over a Web service. The OPC tag namespace is built from the data point hierarchy, which has been configured by the Configurator software. The OPC server on the device implements the data access standard via the Web service interface XML-DA. The OPC XML-DA Web service is accessible via the URI

http://192.168.24.100/DA

where the IP address has to be replaced with the actual IP address of the device. The Web service is accessible over the same TCP port as the Web server. The default TCP port is 80. The Web server port can only be changed via the device configuration tab in the Configurator or in the L-Config tool (see NIC User Manual [4]).

Since the Web service is easily routable on the Internet, the embedded OPC server implements the basic authentication method to protect the system from unauthorized access. The basic authentication involves the operator user and the password configured for this user. On how to configure the operator's password, please refer to Section 3.1.

To disable the basic authentication, clear the operator's password. On the LINX-12x, 15x, 22x models, the anonymous OPC access must be enabled. For doing so, change to the port configuration on the Web UI, select the OPC protocol on the Ethernet tab and check the anonymous OPC box.

Note: *It is highly recommended to use basic authentication when exposing crucial data points over the Web service.*

To use the exposed OPC data points, there exist several possibilities:

- Use LOYTEC's L-WEB visualization tool that comes free with the device,
- use LOYTEC's L-VIS device as OPC XML/DA client, or
- use a standard OPC client or SCADA package, or
- create your own Web service client with custom Web Pages.

The easiest way to visualize the network's data points over a Web-based interface using the device is the L-WEB software. This software is fully integrated into the Configurator and allows designing graphical page content. The tool is intuitive to use like the L-VIS graphical page designer. The resulting L-WEB application is stored on the device and can be directly accessed in your Web browser or other Internet appliances, such as tablets or smart phones..

Standard OPC clients and SCADA packages, which shall visualize the device's data points, must conform to the OPC XML-DA standard. This means they must support the OPC Web

service and not only the COM/DCOM protocol. If your SCADA package does not support OPC XML-DA, a PC-based bridge from XML-DA to the COM-based protocol can be used. The bridge software is running on a PC and translates from COM/DCOM requests into XML-DA Web service requests. The system is depicted in Figure 142.

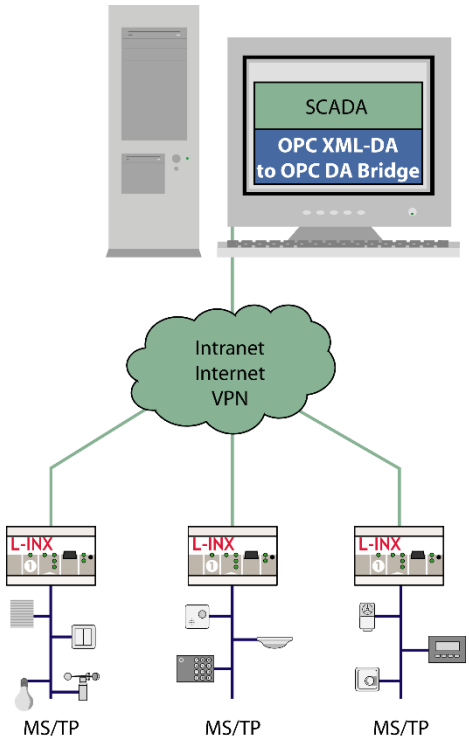


Figure 142: Using a XML-DA/DCOM bridge.

With the bridge is configured to access a number of OPC devices, the COM-based SCADA application can access a COM-based OPC server for each of those devices. The bridge software needs to be purchased from an OPC bridge software vendor.

If L-WEB is not used, customers can create their own XML-DA clients based on the WSDL for OPC XML-DA. Refer to Section 6.3 for more information.

6.1.2 Data Points

The data point hierarchy as configured by the Configurator software is exposed to the OPC tag namespace by the device. This is done internally for all data points, which are marked for OPC exposure (i.e., have the OPC check-mark set).

Folders are translated into OPC nodes. Any of the data point classes, analog, binary, multi-state, string, and user, are exposed as OPC tags. Each OPC tag contains the value of the data point and some of its meta-data. An example of browsing the OPC tags on the device is shown in Figure 143.

The OPC quality property of a given OPC tag is coupled to the data point status. If a data point is offline or unreliable, the OPC quality property changes to *uncertain*.

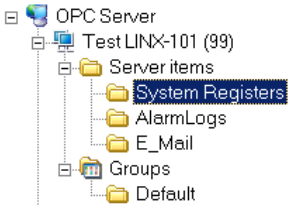


Figure 143: Client browsing the OPC tag namespace on a L-INX.

6.1.2.1 Analog

Analog data points are exposed as a one-to-one mapping to OPC tags. For each analog data point, an OPC tag is created. The OPC tag contains a number of OPC properties, which are derived from the data point's properties:

- Item Canonical Data Type (SmallInt): This property indicates the data type '5' (Double).
- Item Value (Double): The present data point value.
- Item Quality (SmallInt): The value quality. It is "good" if the data point is in normal state, or "uncertain" if the data point has an off-normal state, e.g., offline or unreliable.
- Item Timestamp (Date): This property contains the timestamp of the last value update.
- Item Access Rights (Integer): This property defines whether the tag is read-only or read/write.
- Item Description (String): This is the description of the data point.
- Item EU Type (Integer): This property is '1'.
- High EU (Double): This is the analog maximum value of the data point.
- Low EU (Double): This is the analog minimum value of the data point.
- EU Units (String): This is the human-readable engineering units text of the data point.

6.1.2.2 Binary

Binary data points are exposed as a one-to-one mapping to OPC tags. For each binary data point, an OPC tag is created. The OPC tag contains a number of OPC properties, which are derived from the data point's properties:

- Item Canonical Data Type (SmallInt): This property indicates the data type '11' (Boolean).
- Item Value (Boolean): The present data point value.
- Item Quality (SmallInt): The value quality. It is "good" if the data point is in normal state, or "uncertain" if the data point has an off-normal state, e.g., offline or unreliable.
- Item Timestamp (Date): This property contains the timestamp of the last value update.
- Item Access Rights (Integer): This property defines whether the tag is read-only or read/write.
- Item Description (String): This is the description of the data point.

- Contact Close Label (String): This property contains the active text of the binary data point.
- Contact Open Label (String): This property contains the inactive text of the binary data point.

6.1.2.3 Multi-state

Multi-state data points are exposed as a one-to-one mapping to OPC tags. For each multi-state data point an OPC tag is created. The OPC tag contains a number of OPC properties, which are derived from the data point's properties:

- Item Canonical Data Type (SmallInt): This property indicates the data type '3' (Integer).
- Item Value (Integer): The present data point value.
- Item Quality (SmallInt): The value quality. It is "good" if the data point is in normal state, or "uncertain" if the data point has an off-normal state, e.g., offline or unreliable.
- Item Timestamp (Date): This property contains the timestamp of the last value update.
- Item Access Rights (Integer): This property defines whether the tag is read-only or read/write.
- Item Description (String): This is the description of the data point.
- Item EU Type (Integer): This property is '2' for multi-state.
- Enumerated EU (Array of String): This property contains the state texts of the data point.

6.1.2.4 User Type

User-type data points contain a byte array of user-defined data. Data points of user-type are also exposed as a one-to-one mapping to OPC tags. For each such data point, an OPC tag is created. The item value of the user-defined data is a hex string without whitespace representing the byte array, e.g., "B034". The OPC tag contains a number of OPC properties, which are derived from the data point's properties:

- Item Canonical Data Type (SmallInt): This property indicates the data type '8' (String).
- Item Value (String): A hex string without whitespace representing the byte array.
- Item Quality (SmallInt): The value quality. It is "good" if the data point is in normal state, or "uncertain" if the data point has an off-normal state, e.g., offline or unreliable.
- Item Timestamp (Date): This property contains the timestamp of the last value update.
- Item Access Rights (Integer): This property defines whether the tag is read-only or read/write.
- Item Description (String): This is the description of the data point.

6.1.2.5 String

String data points contain a string of text characters. Data points of string type are also exposed as a one-to-one mapping to OPC tags. For each such data point, an OPC tag is created. The item value of the tag is the string data, e.g., "Room4". The OPC tag contains a number of OPC properties, which are derived from the data point's properties:

- Item Canonical Data Type (SmallInt): This property indicates the data type '8' (String).

- Item Value (String): The string value.
- Item Quality (SmallInt): The value quality. It is “good” if the data point is in normal state, or “uncertain” if the data point has an off-normal state, e.g., offline or unreliable.
- Item Timestamp (Date): This property contains the timestamp of the last value update.
- Item Access Rights (Integer): This property defines whether the tag is read-only or read/write.
- Item Description (String): This is the description of the data point.

6.1.2.6 Structured Data Points

Structured data points are modeled as one user-type data point, which contains the entire structure value as a byte array. The respective structure fields are created as sub-data points of appropriate class. For example, a SNVT_switch in CEA-709 would be modeled as one user-type data point of 2 bytes length, and two sub-data points, one an analog (value member) and one a multi-state (state member).

The relation between user-type data point and sub-data points is also exposed to OPC. In this case, an OPC node is created for the user-type data point. In that node, the sub-data points are exposed as OPC tags. The entire structure is also exposed as a user-type OPC tag under the same OPC node.

Important!	***Deselect any un-used structure members from OPC exposure to reduce the number of total OPC tags.***

It is important to note, that when using structured data points the top-level and all its structure members are exposed as OPC tags by default. Using many structured data points may lead to exceeding the OPC tag limit. Please observe this limit in the Configurator’s statistics tab and deselect the **OPC Tag** check box for unwanted structure members. This helps to keep your configuration lean and improves the performance of the OPC server when browsing and subscribing.

6.1.3 AST Objects

The alarming, scheduling, and trending (AST) objects are more complex than regular data points. The OPC XML-DA standard does not have appropriate tags for those objects. Therefore, the device exposes AST objects as a set of OPC tags describing the object. All tags for one AST object are collected under an OPC node representing the AST object.

6.1.3.1 Scheduler Object

The device exposes the scheduler objects to OPC XML-DA tags. Each scheduler object is represented by a node in the OPC name space. The content of the schedule XML document referred to in this section must be compliant to the scheduleCfg schema. This schema can be found at the LOYTEC Web site. The XML documents can refer to the target namespace ‘http://www.loytec.com/xsd/scheduleCfg/1.0/’.

In that node, the following OPC tags are available:

- ServiceType (string, Read-only, const): This is a constant tag of type string, which contains “schedule”. It identifies this folder as a schedule folder. This can be used as an additional identification to the vendor-specific property of the folder tag.
- Schedule (string, read/write): This tag configures the schedule. The data type is string and the format is in XML. The XML document contains the *scheduleCfg* element as the root element.

- Caps (string, read-only): This tag contains the schedule capabilities. The data type is string and the format is in XML. The XML document contains the *scheduleCapabilities* element as the root element.

- CalItemPath (string, Read-only, const): This is an optional tag. If present, it contains the item path to the calendar object, that the schedule references. To read the calendar referenced by the schedule, use this item path and the "Calendar" item name to read the calendar XML document.

- EmbeddedCal (node): This is an optional OPC node. If present, it contains the OPC tags for the embedded calendar. The embedded calendar structure is as defined for calendar objects in Section 6.1.3.2.

6.1.3.2 Calendar Object

The device exposes the calendar objects to OPC XML-DA tags. Each calendar object is represented by a folder in the OPC name space. In that folder, the following OPC tags shall be available:

- ServiceType (string, Read-only, const): This is a constant tag of type string, which contains "calendar". It identifies this folder as a calendar folder. This can be used as an additional identification to the vendor-specific property of the folder tag.

- Calendar (string, read/write): This tag configures the calendar. The data type is string and the format is in XML. This document contains the *calendarCfg* element as the root element.

- Caps (string, read-only): This tag contains the calendar capabilities. The data type is string and the format is in XML. The XML document contains the *calendarCapabilities* element as the root element.

6.1.3.3 Alarm Objects

The alarm objects on the device provide the *alarm summary* and can be used to acknowledge alarms. The alarm objects are exposed to XML-DA tags. Each alarm is uniquely identified by an XML alarm ID (XAID). The XAID must identify the alarm object and the alarm ID in that object. The XAID is used in the acknowledge service to identify the alarm. The XAID can also be transmitted in e-mail notifications.

Each alarm object is represented by a folder in the OPC name space. In that folder, the following OPC tags shall be available:

- ServiceType (string, Read-only, const): This is a constant tag of type string, which contains "alarm". It identifies this folder as an alarm folder. This can be used as an additional identification to the vendor-specific property of the folder tag.

- Summary (string, Read-only): Reading from this tag, the current alarm summary can be obtained. The data type is string and the tag contains an XML document. This tag should not be subscribed to as it contains a large document. Subscribe to NotifyNewCnt instead, to get notified about new alarms. The root element of the XML document is the *alarmSummary* element.

- NotifyCnt (unsigned, Read-only): This tag is updated with an incremented notify count for each alarm update notification. This is the case for new or cleared alarm conditions, and for acknowledged alarms. Clients can subscribe to this tag in order to be notified about changes in the alarm summary. The client has then to read the complete alarm summary when notifications occur.

- NotifyNewCnt (unsigned, Read-only): This tag is updated with an incremented notify count each time a new alarm appears. This tag does not update when alarms are acknowledged or go inactive.

- Ack (string, Write): Writing to this tag acknowledges an alarm. The data type is string. The written data is an XML document, which contains the *alarmAck* element. The write must specify the XAID.

6.1.3.4 Trend Log Objects

Each trend log object on the device is represented by a folder in the OPC name space. This folder contains a number of tags describing and controlling the trend log. To retrieve log records, however, the XML-DA tag interface cannot be used. There are two options: retrieve the complete log as a CSV file, or use the LOYTEC proprietary Data Log Web service (XML-DL). That Web service uses the logHandle provided by a tag. The CSV file location can be obtained from a tag also.

- ServiceType (string, Read-only, const): This is a constant tag of type string, which contains “trendLog”, or “alarmLog”. It identifies this folder as a trend log, data log or alarm log folder. This can be used as an additional identification to the vendor-specific property of the node tag.

- Purge (Boolean, read/write): When writing TRUE to this tag, the log is purged.

- TotalCnt (unsignedInt, read-only): This tag contains the total number of logged records. This number can be larger than the BufferSize.

- BufferSize (unsignedInt, read/write): The size in records of the log buffer. Writing to this tag can resize the log buffer, if it is disabled.

- LogHandle (string, read-only, const): This handle specifies the data log. The logHandle must be used with the proprietary Data Log Web service.

- CsvFile (string, read-only, const): This tag specifies the file path and file name of the CSV data log file.

- CentralDL0, CentralDL1 (string, read/write): These tags are obsolete and kept for backward compatibility.

6.1.3.5 E-mail Templates

E-mail templates can be configured in the Configurator software. When an e-mail template is triggered, the corresponding e-mail is transmitted. The e-mail template can also be triggered over the OPC interface. Therefore, a node is added to the OPC name space for each e-mail template under the “E_Mail” node.

Each e-mail node is named after the e-mail template and contains the following OPC tags:

- ServiceType (string, Read-only, const): This is a constant tag of type string, which contains “email”. It identifies this folder as an e-mail template folder.

- Send (Boolean, read/write): When writing TRUE to this tag, the e-mail transmission is triggered.

6.1.4 OPC Groups

OPC groups are used to subscribe to data coming from OPC tags. The group specifies the subscribed tags and a server refresh rate, which the OPC server can interpret, how often it shall refresh data of the underlying data points.

In network technologies that are event-based, this refresh rate has no further impact, as the data is as fresh as possible. In technologies, that rely on polling, the OPC server activates dynamic poll-groups for the subscribed OPC tags. The data server of the device can then employ dynamic polling, if the technology supports it (see Chapter "Concepts" of the LINX Configurator User Manual).

6.2 OPC UA Server

6.2.1 Introduction

OPC UA (Unified Architecture) is a new International standard (IEC 62541) designed for communication between information systems. It has been specified by the OPC Foundation which also released the "classical" OPC: DA, HDA, A&E and XML-DA. OPC UA has been conceived to be the successor of those old specifications in order to overtake some drawbacks they imply. LOYTEC device models with enhanced security features have a built-in OPC UA server (see also the respective product manual).

OPC UA innovates with some new features such as: Security based on certificates exchange, heartbeat for connections in both directions and acknowledgements of transmitted data. LOYTEC devices with a built-in OPC UA server use the binary protocol over TCP/IP giving you the best performance and least overhead while taking minimum resources.

The OPC UA server is accessible via two URIs:

opc.tcp://192.168.24.100:4840

https://192.168.24.100/UA

where the IP address has to be replaced with the actual IP address of the device. The default TCP port is 4840. It can be changed on the OPC UA configuration page of the Web interface. The OPC UA Server is also accessible via secure Web Services with HTTPS.

One of the most interesting features of OPC UA is built-in security. Therefore, the LOYTEC OPC UA server comes with default parameters only allowing secure connections. It is required to setup the OPC UA Server before establishing a connection with any OPC UA client. The Web interface Ethernet port configuration has OPC UA protocol settings and the Web interface **Certificates** page has a dedicated OPC UA tab.

6.2.2 OPC UA and Security

The LOYTEC OPC UA server can be enabled on the **Ethernet** tab of the **Port Config** page. To enable OPC UA select the OPC UA protocol as shown in Figure 144. The OPC UA protocol settings box allows you to configure different options for the OPC UA server: its transport protocols, its port number, the security policies and the user authentication modes available to OPC UA clients. Changing one of them requires rebooting the device.

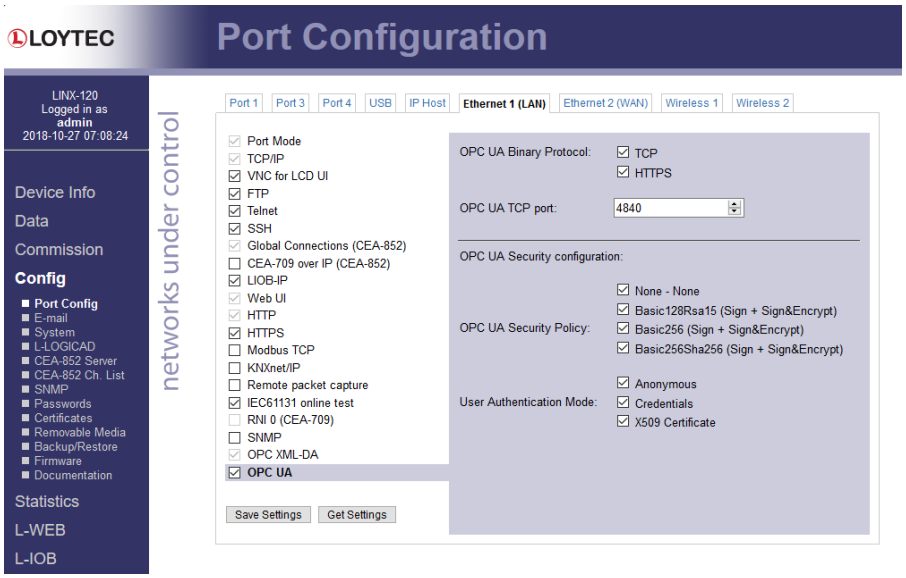


Figure 144: OPC UA server configuration

The OPC UA Server is accessible via two transport protocols: TCP or HTTPS. Both are using binary-encoded data. OPC UA over HTTPS requires activation of the HTTPS service on the device.

The default port number of the OPC UA server is 4840. This is the official registered port at the IANA (Internet Assigned Numbers Authority) for OPC UA TCP protocol for OPC Unified Architecture from OPC Foundation. It is also possible to change it to any other available port number. However, some OPC UA services (Find Servers and GetEndpoints) used to discover OPC UA server endpoints may be only available through the default port number 4840 depending of the client used.

Using the non-default port number might also require to establish a direct connection from your OPC UA client by giving the willing Security Policy and Authentication Mode without having the possibility to know and choose them with FindServers and GetEndpoints OPC UA services. Thus a warning message will appear when changing the port number to the non-default port number value.

By default the LOYTEC OPC UA server is configured to accept secure connections only, requiring certificate exchange. An unsecure mode, however, not requiring certificate exchange can be enabled if so required. The **OPC UA Security Policy** defines the level of security that will be applied to the OPC UA connection:

- **None – None**: Deactivated by default, this is the only security policy not requiring certificate exchange. This connection security policy shall be avoid as much as possible since security is a requirement for any OPC UA Clients, they must have the possibility to establish secure connections and to manage certificates exchange.

- **Basic128Rsa15 (Sign + Sign&Encrypt)**: Security Policy group for both Basic128Rsa15Sign and Basic128Rsa15Sign&Encrypt. The first levels of security for an OPC UA connection. Those security policies use RSA15 as Key-Wrap-algorithm. Messages between Client and Server will be signed by both Client and Server certificates. If

    - **Sign**: Messages will not be encrypted and remain readable with a Network Analyzer such as Wireshark.

    - **Sign&Encrypt**: A 128-Bits key length will be used as encryption algorithm. This Security policy uses encryption implying that messages will not be readable from Network Analyzer.

- **Basic256 (Sign + Sign&Encrypt)**: Security Policy group for both Basic256Sign and Basic256Sign&Encrypt. The second level of security for an OPC UA connection. Those security policies use RSASHA1 as Key-Wrap-algorithm. Messages between Client and Server will be signed by both Client and Server certificates.

    - **Sign**: Messages will not be encrypted and remain readable by a Network Analyzer.

    - **Sign&Encrypt**: A 256Bits key length will be used as encryption algorithm. This Security policy uses encryption implying that messages will not be readable from Network Analyzer.

- **Basic256Sha256 (Sign + Sign&Encrypt):** Security Policy group for both Basic256Sha256Sign and Basic256Sha256Sign&Encrypt. The third level of security for an OPC UA connection. Those security policies use RSASHA256 as Key-Wrap-algorithm. Messages between Client and Server will be signed by both Client and Server certificates.

    - **Sign:** Messages will not be encrypted and remain readable by a Network Analyzer.

    - **Sign&Encrypt:** A 256Bits key length will be used as encryption algorithm. This Security policy uses encryption implying that messages will not be readable from Network Analyzer. When available on the OPC UA Client, this must be the preferred connection.

The **User Authentication Mode** on the LOYTEC OPC UA Server includes three possible ways for OPC UA clients to authenticate. Each authentication mode could work independently of the Security Policies enabled. By default only the **Credentials** authentication mode is activated. The following authentication modes can be activated:

- **Anonymous**: Not activated by default. This authentication mode does not require actions from users. As security is one major aspect of OPC UA, it should not be used unless for testing.

- **Credentials**: This authentication mode requires a user account with a password to establish an OPC UA connection. Accounts must be managed through the Web interface Account Management. OPC UA does not require any special accounts.

- **X.509 Certificate:** By default this option is not activated. This authentication mode uses X.509v3 certificates to assure identity of OPC UA clients. The certificate used with that authentication mode need also be added to the Trusted Clients List before establishing a connection.

6.2.3 OPC UA Trusted Clients

OPC UA security is based on X.509 certificates exchange. By default a LOYTEC OPC UA server comes with a pre-installed self-signed certificate that will have to be trusted by your OPC UA client. The OPC UA server also requires trusting OPC UA clients before establishing a connection. It is possible to upload a new self-signed or signed-by-CA certificate through the WebUI.

The **Certificates** page on the Web interface has a dedicated **OPC UA** tab allowing you to manage X.509 certificates by getting the OPC UA server certificate from the device, trusting a new OPC UA client, rejecting a trusted OPC UA client or deleting a trusted/rejected OPC UA client certificate.

The OPC UA specification requires that each managed certificate must be compliant with the X.509v3 certificate standard. The LOYTEC OPC UA server also requires that every OPC UA client certificate must be encoded into the binary .DER format.

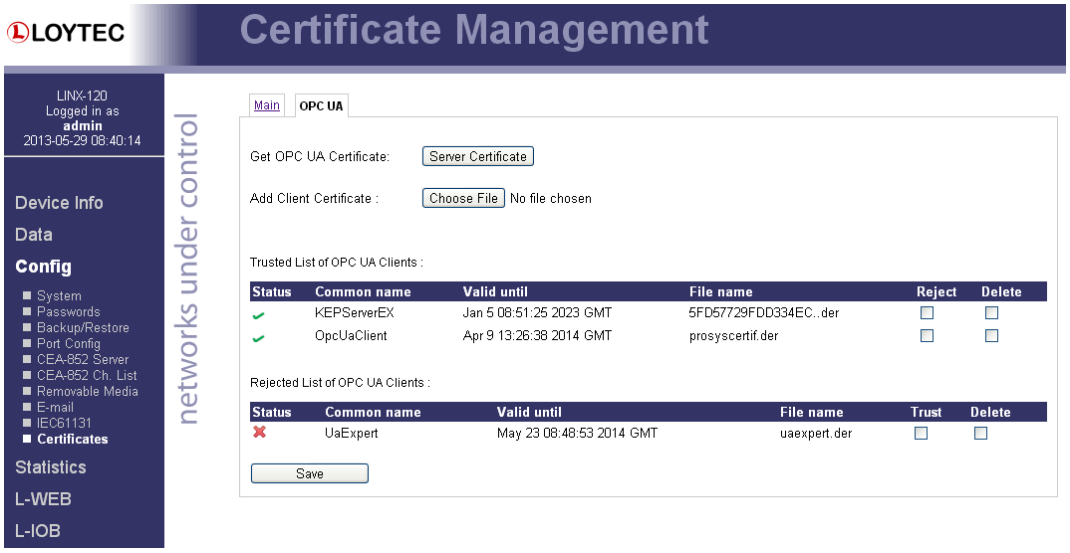


Figure 145: OPC UA client certificate management.

To allow a secure connection initiated by an OPC UA client, the OPC UA server needs to find the client's X.509 certificate in its **Trusted List of OPC UA Clients**. To trust a new OPC UA client, add a new client certificate by clicking on the **Choose File** button. A popup window will be opened asking you to provide a valid X.509v3 Certificate. Once a correct OPC UA client certificate has been added to the trusted list of OPC UA clients, a client will be granted access to the OPC UA server. The Web interface displays some internal certificate information such as the common name or the time limit of validity. No reboot is necessary after adding a trusted client certificate.

The list of trusted OPC UA clients can be edited. The following actions are available:

- **Reject a trusted OPC UA Client**: Check the reject checkbox of one or more certificates in the trusted list and click **Save**. The certificates are now be considered as rejected and a secure connection with the selected clients will not be possible until they are added back to the trusted list. They appear in the rejected list.

- **Trust a rejected OPC UA Client:** Check the trust checkbox of one or more certificates in the rejected list and click **Save**. The selected certificates will be moved to the trusted list again and a secure connection with the selected clients can be established again.

- **Delete a trusted/rejected OPC UA Client:** Check the delete checkbox of one or more certificates in either the trusted or rejected list and click **Save**. The selected certificates will be entirely removed from the LOYTEC device.

6.2.4 OPC UA Client Setup

The last step before establishing a secure connection is on the OPC UA clients side. The OPC UA client also requires trusting a LOYTEC OPC UA server before connecting to it. This is usually done by adding the LOYTEC device's certificate to the trusted server list of the OPC UA client. The LOYTEC OPC UA server X.509v3 Certificate is downloadable by clicking on the **Server Certificate** button. Then add it to the trusted list of OPC UA server of your client.

Some OPC UA clients may not require to be configured with a trusted server certificate and will ask you, if you want to trust it when connecting. It may also warn that the pre-installed LOYTEC OPC UA server certificate is a self-signed certificate. However, installing the LOYTEC server certificate in your client list of trusted OPC UA servers is the safest approach since it reliably prevents man-in-the-middle attacks.

Note : *Installing a new Server certificate in the WebUI with a key size > 4096 bits might lead to connection problems with some OPC UA Clients !*

6.2.5 Connect with an OPC UA Client

In order to connect a Third party OPC UA Client to your LOYTEC device OPC UA Server with secure communication, please follow the specified steps:

- Activate the OPC UA Server (deactivated by default) and the wanted Security Policies / User Authentication mode on the Web interface Port Config page.
- Create or Import a new Certificate (self-signed or signed by CA) on your LOYTEC device (see Section 3.7.2 Certificate Management)
- Import the OPC UA Client certificate in the Trusted List of OPC UA Clients on your LOYTEC device (see Section 6.2.3)
- Optional: Import the LOYTEC's device OPC UA Server certificate in the trusted list of OPC UA Servers of your third party OPC UA Client (see Section 6.2.4).
- Connect and Trust your device OPC UA Server certificate, if presented.

6.2.6 OPC UA Address Space

The data point hierarchy as configured by the Configurator software is exposed to the OPC UA address space by the device. This is done internally for all data points, which are marked for OPC exposure (i.e., have the OPC check-mark set). That hierarchy is accessible under the folder Loytec ROOT.

Folders are translated into OPC UA folder object. Any of the data points classes, analog, binary, multi-state, are exposed as OPC UA variables with OPC UA properties. Any of the data point classes string and user are exposed as OPC UA variables. An example of browsing the OPC UA address space on the device is shown in Figure 146.

All OPC UA variables also possess a Node ID by which they can be identified by an OPC UA client alternatively to the full browse path. The node ID remains constant between device restarts and is derived from the data point ID:

UA Node ID = (Data Point ID * 16) + 20000.

The OPC UA specification requires some special nodes, which are not part of the data point hierarchy. They can be found under the folder 'Types' and under the OPC UA object server.

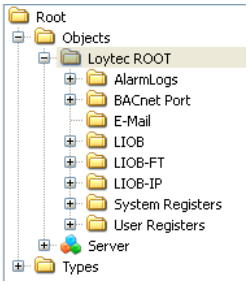


Figure 146: Client browsing the OPC UA address space on a LOYTEC device.

6.2.6.1 OPC UA Data Types

OPC UA specification defines some special data types used as internal structures by OPC UA node instances.

- **NodeId**: A structure containing a unique identifier in an OPC UA server used to address the node by OPC UA services. The LOYTEC OPC UA server only uses numeric NodeIds.
- **QualifiedName**: The structure used when browsing the OPC UA server. It also contains a unique identifier used for multiple address spaces. In the LOYTEC OPC UA server, this identifier is '0'.
- **LocalizedText**: A structure composed of two strings. The LOYTEC OPC UA server always contains 'en' as the **Locale** and the data point's value as **Value**. For example, an attribute using this data type is the optional description of a data point.
- **DataValue**: The structure used to expose the value. It contains the variant value, a status (Integer) and two timestamps, one for the OPC UA server read time, the other one for the last data point update.

6.2.6.2 Common Attributes

Scalar data points exposed to OPC UA contain the following list of attributes common to analog, binary, multi-state data points:

- **NodeId** (NodeId): The unique numeric identifier of a data point in the OPC UA server.
- **NodeClass** (Integer): This attribute indicates that the OPC UA node is a variable and is equal to '2'.
- **BrowseName** (QualifiedName): The name of the data point used by the browse service.
- **DisplayName** (LocalizedText): The name of the data point used by the read service.
- **Description** (LocalizedText): The optional attribute containing the description of the data point.
- **WriteMask/UserWriteMask** (Byte): Optional attribute defining which attributes of the OPC UA variable are writable. In the LOYTEC OPC UA server, only the value is writeable so WriteMask and UserWriteMask contain '0'.
- **Value** (DataValue): The actual variant value of the data point, the data point's times tamp of the last update, the OPC UA server time stamp of the last update and the actual OPC UA status code of the data point.
- **DataType** (NodeId): The actual data type of the OPC UA variable.
- **ValueRank** (Integer): This attribute classifies the value as a scalar or an array.
- **ArrayDimensions** (Integer): If the value is an array, this attribute specifies the size of that array.
- **AccessLevel/UserAccessLevel** (Byte): Contains information whether the OPC UA node is readable and/or writable.
- **MinimumSamplingInterval** (Double): Optional attribute providing a sample interval used for subscriptions. This is set to '0' (default) in each OPC UA variable.

- **Historizing** (Boolean): Indicates whether the server is currently using that OPC UA variable as an historical data point.

6.2.6.3 Analog

Analog data points are exposed as one OPC UA variable with three Properties to OPC UA nodes. The OPC UA variable holds the data point's name. The properties are: EU Range, EU Type and EU Units, where EU stands for engineering units.

The EU Range property contains an Array value of Double with the analog maximal value and analog minimal value of the data point. The EU Type contains a scalar value '1' for analog data points and the EU Units property holds a string value for the human-readable engineering unit text of the data point.

6.2.6.4 Binary

Binary data points are exposed as one OPC UA variable with two Properties to OPC UA nodes. The OPC UA variable holds the data point's name. The properties are: EU Info, EU Type.

The EU Info property contains an array value of strings with active and inactive text of the data point. The EU Type contains a scalar value '2' for binary data points.

6.2.6.5 Multi-state

Multi-state data points are exposed as one OPC UA variable with two Properties to OPC UA nodes. The OPC UA variable holds the data point's name. The properties are: EU Info, EU Type.

The EU Info property contains an array value of strings with the different state texts of the data point. The EU Type contains a scalar value '2' for a multi-state data point.

6.2.6.6 User Type

Data points of class user are exposed as a one-to-one mapping to OPC UA nodes. The OPC UA node value is a hexadecimal string without whitespace representing the byte array, e.g., 'B034'.

6.2.6.7 String

String data points are exposed as a one-to-one mapping to OPC UA nodes. The OPC UA value of a string OPC UA variable contains the string data, e.g., 'Room4'.

6.2.6.8 Structured Data Points

In OPC UA, structured data points are represented as in OPC XML-DA: one user-type data point containing the entire structure value as a byte array. The respective structure fields are created as sub-data point of the appropriate class. For detailed information on how structure sub-data points are mapped to OPC variables please refer to Section 6.1.2.6.

6.2.7 AST Objects

The alarming, scheduling, and trending (AST) objects are more complex than regular data points. Therefore, the device exposes AST objects as a set of OPC UA nodes describing the object as in the OPC XML-DA Server. All tags for one AST object are collected under an OPC UA node representing the AST object. For a detailed description of the involved OPC variables please refer to Section 6.1.3.

6.2.8 Subscriptions and Monitored Items

The LOYTEC OPC UA server allows users to create and manage subscriptions and monitored items. Subscriptions enable monitoring a group of monitored items. The total

number of subscriptions that may be active at a time on a LOYTEC device is 64. The user can setup the following parameters for its favorite OPC UA client:

- **PublishingInterval**: The interval in ms between each publish response. The minimum publish interval value is 1second and the maximum is 86,400,000ms (1 day).

- **LifetimeCount**: The number of times the publish interval can expire without the server sending data updates or keep-alive messages. It must be at least 3 times the MaxKeepAliveCount. The valid range is 3 to 4,294,967,295 (MaxUInt32).

- **MaxKeepAliveCount**: This number specifies the number of publish intervals that must expire before a keep-alive message is sent. The valid range is 1 to 1,431,655,765 (MaxUInt32/3).

- **Priority:** This byte number indicates the relative priority of one subscription. Subscription notifications are sent regarding subscription priorities when there is more than one subscription active on the OPC UA Server. This parameter can not be managed by all OPC UA Clients.

A monitored item is created for each OPC UA node requested to be monitored. When data points associated with OPC UA nodes, which are linked to the created monitored items, are updated, a new publish response is sent containing the updated value.

AST object data points cannot be monitored excepted CentralDL0, CentralDL1, TotalCnt of Trend Log Objects and NotifyCnt, NotifyNewCnt of Alarm Objects.

Parameters for monitored items on LOYTEC device are:

- **SampleInterval**: The rate, at which the monitored items are sampled. It is always the interval of the subscription's publishing interval.

- **QueueSize**: The OPC UA Server supports queue size <= 2 as required by the Embedded OPC UA Server Profile.When QueueSize =2 and a monitored Items changes more than 1 time between a timelapse < PublishInterval, 2 values will be sent to Client.

- **DiscardOldest**: This parameter only matters if QueueSize > 1. If true, the oldest value gets deleted from the subscription DataNotification queue, if False the last value added to the subscription DataNotification queue gets replaced with the new value.

- **DataChangeFilter**: The OPC UA Server only supports DataChangeTrigger: Status/Value and Status/Value/Timestamps will only send a DataNotification when value has been updated! The default value is Status/Value. Deadband is only supported by datapoints with Numeric values.

6.2.9 OPC UA Statistics

For analyzing problems with OPC UA communication the device offers statistics information. The Web interface displays that information on the **OPC UA Server** page of the **Statistics** menu. Figure 147 shows a typical output of such statistics information.

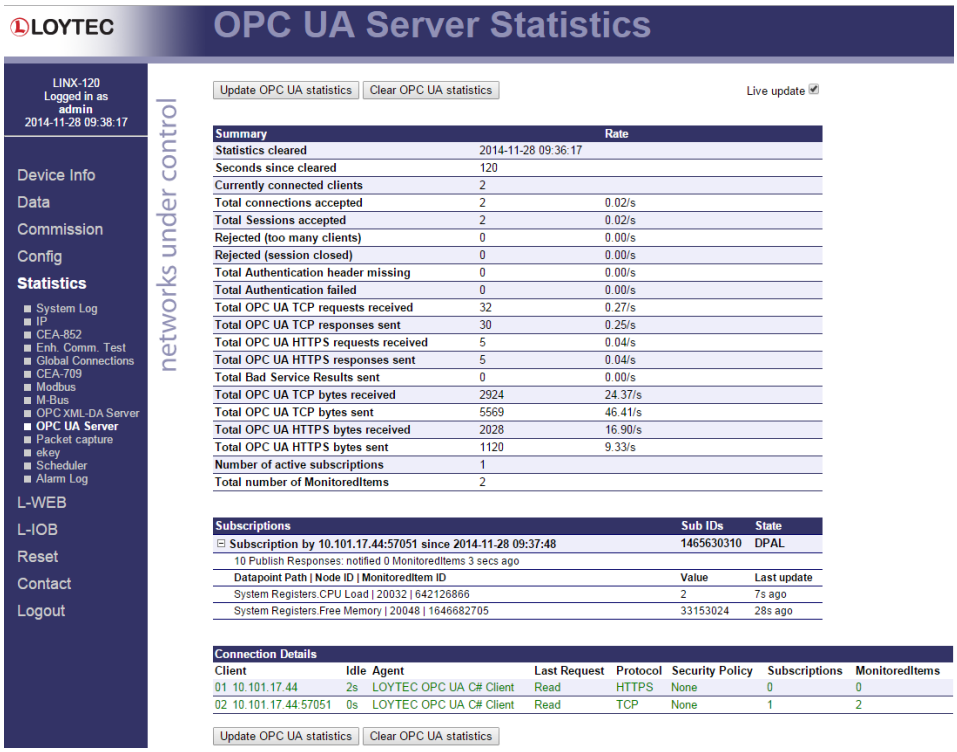


Figure 147: OPC UA Server Statistics.

The following information is available:

- Currently connected Clients: Number of OPC UA clients currently connected to the OPC UA server.
- Total connections accepted: Number of connection accepted since last cleared.
- Total Session accepted: Number of sessions accepted since last cleared.
- Rejected (too many clients): Number of sessions rejected due to too many clients already connected since last cleared.
- Rejected (Session closed): Number of sessions rejected due to the fact that the session has been closed by the server or the client.
- Total Authentication header missing: Number of sessions opened without a matching authentication mode in the server.
- Total Authentication failed: Number of sessions opened without valid authentication.
- Total OPC UA TCP requests received: Number of OPC UA TCP requests received since the last statistic reset.
- Total OPC UA TCP responses sent: Number of OPC UA TCP responses sent since the last statistic reset.
- Total OPC UA HTTPS requests received: Number of OPC UA HTTPS requests received since the last statistic reset
- Total OPC UA HTTPS responses sent: Number of OPC UA HTTPS responses sent since the last statistic reset.

- Total Bad Service Results sent: Number of Bad Response sent in OPC UA TCP Responses.
- Total OPC UA TCP bytes received: Number of TCP bytes received by the OPC UA server.
- Total OPC UA TCP bytes sent: Number of TCP bytes sent by the OPC UA server.
- Total OPC UA HTTPS bytes received: Number of HTTPS bytes received by the OPC UA server.
- Total OPC UA HTTPS bytes sent: Number of HTTPS bytes sent by the OPC UA server.
- Number of active subscriptions: Total number of subscriptions for all the currently connected clients.
- Total number of monitored items: Total number of monitored items for all the currently connected clients.

6.2.10 Error Codes and Solutions

The OPC UA specification defines numerous status codes. Table 5 lists some of them which may occur and provides possible solutions to resolve those problems.

OPC UA Error Code	Meaning	Solutions
BadNotReadable	OPC UA client read a non-readable node.	Set the data point to readable in the Configurator Software.
BadNotWritable	OPC UA client tried to write to a non-writeable node.	Set the data point to writeable in the Configurator Software.
BadNodeIdInvalid	This node does not support the requested operation	Trying to add non-data point to subscription lead to that error codes.
BadIdentityTokenInvalid	OPC UA client tried to connect with a non-valid authentication mode	Change the authentication mode of the client or activate the desired authentication mode on the server.
BadServiceUnsupported	OPC UA client tried to use a currently unsupported service.	The OPC UA server does not implement all available OPC UA services. Operations like adding a node to the address space or using a method are currently not supported.
BadUserAccessDenied	OPC UA client did not send the right credentials.	Connect with one of the account credentials available on the device.
BadTooManyMonitoredItems	OPC UA server cannot create any more monitored items for that subscription.	Create a new subscription and add the monitored items wanted. The maximum number of monitored items per subscription is 5000.
BadTooManySubscriptions	OPC UA server can not create more subscriptions.	Delete one active subscription to create a new one. The maximum number of subscriptions is 64.
BadTooManySessions	OPC UA server cannot create more Sessions.	Disconnect one active session to create a new one. The maximum number of active sessions is 32.
UncertainInitialValue	OPC UA server does not know the status of the data point	Configure a default value for this data point in the Configurator software.
BadCertificateTimeInvalid	OPC UA Client certificate time entry is not valid.	Verify that your certificate time (notBefore and notAfter fields) is matching with the LINX Local Date.
BadCertificateRevoked	OPC UA Client certificate is revoked.	Verify that the client certificate is not in the LINX Rejected List.
BadCertificateUntrusted	OPC UA Client certificate is not trusted.	Verify that the client certificate is in the LINX Trusted List.
BadCertificateHostNameInvalid	OPC UA Client certificate host name is not valid.	Verify that the certificate HostName is valid.
BadCertificateInvalid	Client certificate is not valid.	The OPC UA Client certificate sent is not valid. Verify that information and keys are correct.
BadSecurityChecksFailed	OPC UA Client certificate is not valid.	OPC UA does not allow sending internal certificate error code to Client. Log into the WebUI and check the System Log to know the right Error Code.

Table 5: OPC UA Error Codes and Solutions

6.3 Using Custom Web Pages

Custom Web pages can also be developed for the L-INX. For doing so, the applications engineer must implement an OPC XML-DA Web service client, which adheres to the WSDL interface. This can be done in C++ or script languages such as Perl. The WSDL must be

obtained from the OPC Foundation's Web site following the OPC XML-DA namespace http://opcfoundation.org/webservices/xmlda/1.0/.

Any Web content, including scripts, applications or static Web pages can be stored directly on the L-INX's file system. Use the admin account to upload the content via FTP into the directory

```
/var/www
```

For example, a page named 'my_page.html' put directly into '/var/www' can be accessed via 'http://192.168.24.100/my_page.html', given that the IP address is correct.

7 M-Bus

7.1 Introduction

The M-Bus (Meter-Bus) is a European standard (EN 13757-2, EN 13757-3) designed for remote reading of meters. With its standardization as a galvanic interface for remote readout of heat, water, and energy meters, this bus has become an important interface for automatic meter reading applications with different vendor's meters on the same cable.

The M-Bus is a serial bus, which is controlled by a single bus master. This master can request data from several slave devices connected to the network. The data transmission from master to slave is done by a modulation of the output voltage (36 V means a logical '1', 24 V means logical '0'). During data transmission from slave to master the current is modulated (1.5 mA represent the logical '1', 11-20 mA represent a logical '0'). M-bus devices can be powered over the bus. The number of devices which can be powered depends on the M-Bus transceiver used.

7.2 Hardware Installation

For using the M-Bus with the device an external M-bus interface with an RS-232 connector is required. The external interface must be connected to the LOYTEC device either via the serial connector or the extension port EXT. The M-Bus functionality must be enabled on the device itself.

7.2.1 Console Connector

When using the serial console connector, the M-Bus interface is enabled on the device by setting DIP-switch 7 to ON. This disables the console of the device and activates M-Bus over the console connector. After the device is rebooted, the M-Bus is active on the device. When rebooting the device with M-Bus activated and the console connected, a couple of boot messages are displayed in the console, before the console is turned off.

If the console is needed again, set the DIP switch 7 to OFF and reboot the device. This is required, if the firmware shall be updated over the serial port using the LSU tool.

When using the L-MBUS coupler, connect the L-MBUS to the device's console connector via a null-modem cable (female to female sub-D connector) as shown in Figure 148. On the L-MBUS remove the jumper as indicated on the front label The null-modem cable must be an 8-wire, single shielded, type AWG28 with the pin assignment according to Table 6.

Terminal 1	Terminal 2
1	4
2	3
3	2
4	1
5	5
7	8
8	7
9	9
S	S

Table 6: Pin assignment for the L-MBUS null-modem cable

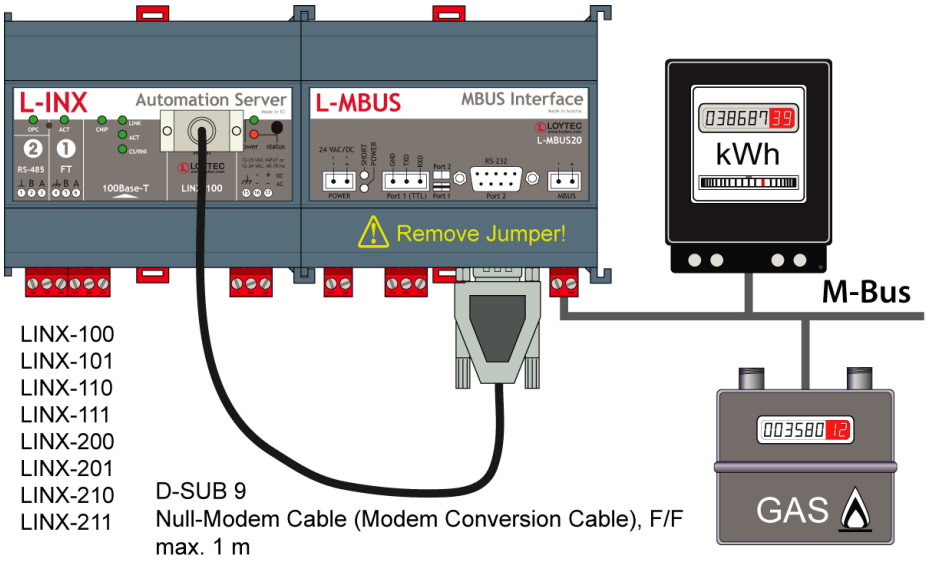


Figure 148: Connecting L-MBUS over console connector.

7.2.2 Extension Port

Devices that do not have a serial console connector provide an extension port marked **EXT** on the device as shown in Figure 149. Those devices need to use the L-MBUS converter. On the L-MBUS set the jumper as indicated on the front label. Follow the cabling instructions of Figure 149 between the **EXT** port of the L-INX and the **PORT1** on the L-MBUS.

Devices that have more than one **EXT** port can operate several L-MBUS converters, thus increasing the total number of M-Bus devices that can be integrated.

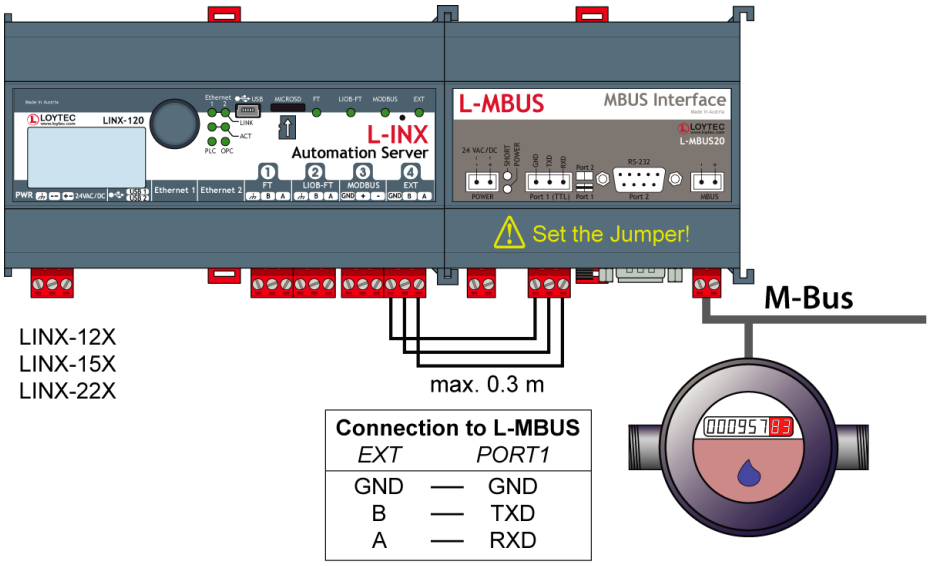


Figure 149: Connecting L-MBUS over the extension port.

7.3 M-Bus Network

The M-Bus network utilizes a two-wire connection. Several M-Bus slave devices are connected in parallel to the transmission medium. Each M-bus device has a primary address in the range from 0 to 250. This primary address must be unique for each device. Also a secondary address can be used for the slave devices. The secondary addressing mode is currently not supported by the LOYTEC device. The M-Bus network also supports two kinds of broadcast messages. A broadcast to address 255 does not force the slaves to give a response. A broadcast to address 254 forces an answer from the slave. This broadcast message is mainly used for peer-to-peer connections.

The M-Bus allows the use of devices with different Baud rates of up to 9600 Baud. M-Bus devices are not always able to fulfill the complete functional specification of the M-Bus standard. For readout two different modes are known (some slave devices implement both):

- A default read usually reads all the data of a device.
- A selective read selects the data points, which are to be read.

Some devices also support writing special data points.

Some M-Bus devices support a synchronized action. This means that when a device receives such a synchronize command, it stores specific data points for later readout. This way, specific information of even a larger number of devices can be read out in a synchronized manner.

M-Bus supports network management functions such as changing the primary address of a device, changing the Baud rate of a device, reading all data from a device as well as pinging a device. It is therefore possible to scan M-Bus devices in an M-Bus network.

M-Bus data points are specified by a DIF/DIFE and VIF/VIFE combination. The DIF/DIFE (data information field and data information field extension) specify storage number, tariff, subunit as well as the data coding (BCD, int, etc.) and the function (min, max, etc.) of the data point. The DIF/DIFE can be up to 11 bytes long (1 byte for the DIF and up to 10 extensions). The VIF/VIFE combination (value information field and value information field

extension) specifies the type of the data point (e.g. energy count value) and how it is presented (e.g., the value is given in "Wh"). Like the DIF/DIFE, the VIF/VIFE can consist of one VIF and up to 10 VIF extensions. It defines the fixed network unit of an M-Bus data point. The Configurator allows the configuration by either entering the DIF/DIFE combination or by specifying the appropriate numbers.

7.4 Web Interface

This section describes the Web interface for the M-Bus port.

7.4.1 Configuration

A configuration of the M-Bus port is not necessary, as no parameters are required for the M-Bus. On devices that have **EXT** ports, the M-Bus protocol can be enabled on any of those ports.

7.4.2 Data Points

M-Bus data points can be accessed through the Web UI as described in Section 3.3.1.

7.4.3 Commission

The commissioning Web UI allows assignment of physical devices to existing devices in the data point configuration, that have been created with the commission later option. Under the **Commission** menu choose the M-Bus technology to open the M-Bus commissioning interface.

The Web page shows a list of all **Devices in configuration**. An example is shown in Figure 150. Each line displays the device name, the primary **Address**, the communication **Port**, and the secondary address (**ID**). The **Status** column shows their current status. It can be one of the following:

- OK: The device is configured for communication.
- Offline: The device is configured for communication but appears offline.
- Uncommissioned: The device is not yet commissioned.
- Disabled: The device is disabled.

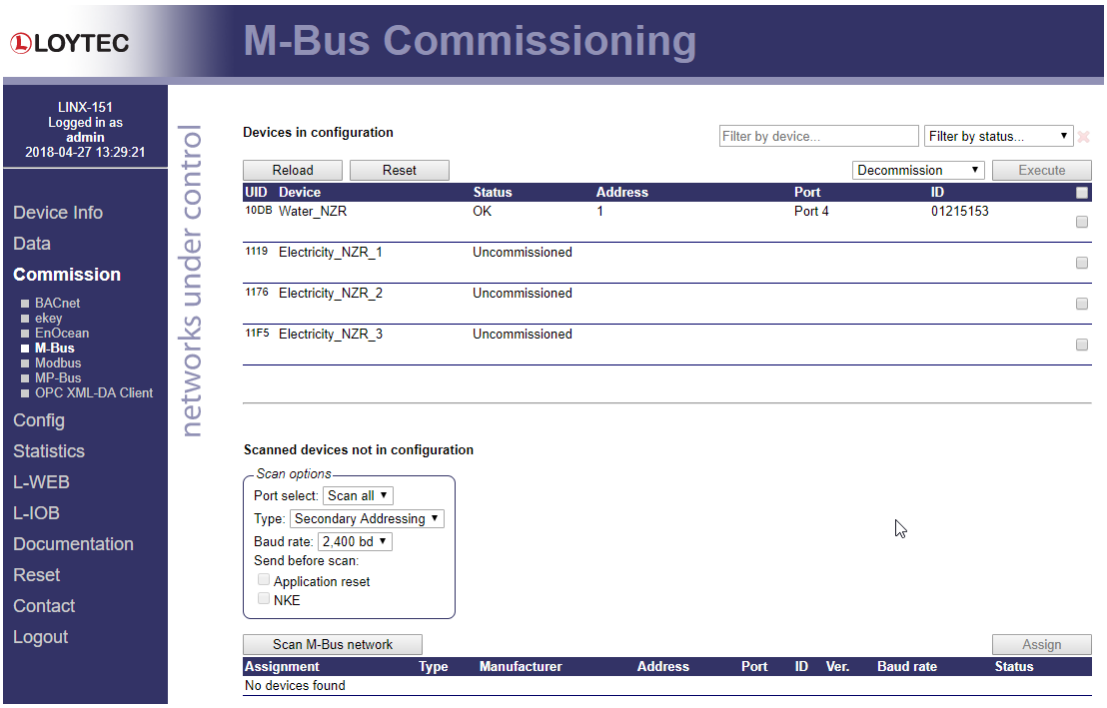


Figure 150: M-Bus commissioning Web interface.

In order to execute an action on devices, select the checkbox at the end of the line. Then choose an action in the drop-down **Action on selected** and click on the **Execute** button. Actions that can be executed on all devices are enable and disable. A disabled device will stop communication on the network until it is enabled again.

Those devices created as commission later can be assigned to physical devices on the network. The device description displayed beneath the device name can be edited, where the edit symbol appears. The assignment can be done manually by editing the fields in the **Address**, **Port**, and **ID** column or by executing a network scan. Edit the scan options as appropriate for your M-Bus network. Choose to **Scan all** available M-Bus ports or select a specific port from the drop-down list, and click on **Scan M-Bus network**. The scan progress will be displayed and fill the list for **Scanned devices not in configuration**. An example is shown in Figure 151.

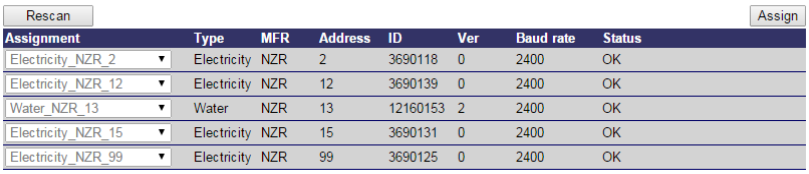
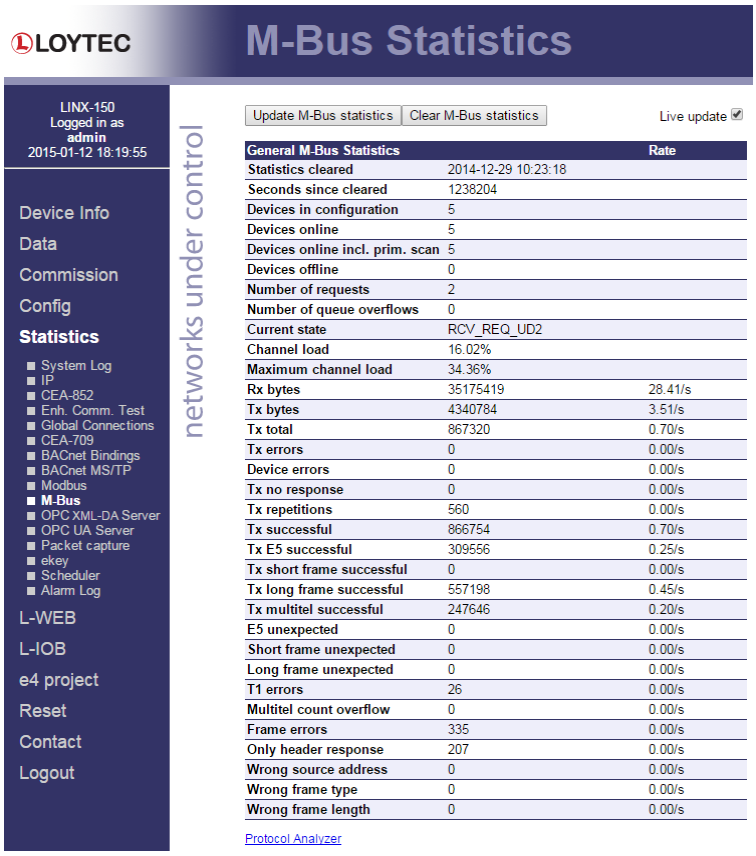


Figure 151: Result of the M-Bus scan on the Web interface

To assign a scanned device to an uncommissioned device in the configuration, select the corresponding device name from the drop-down box in the **Assignment** column. Repeat that for all other devices and then click the button **Assign**.

7.4.4 Statistics

Figure 152 shows a typical output of the statistics information which can be displayed for the M-Bus port. The statistics can be cleared for each M-Bus port separately by pressing the **Clear M-Bus statistics** button. A refresh of the statistics is done automatically. To stop automatic update, deselect the **Live update** checkbox. For manual update press **Update M-Bus statistics**.



General M-Bus Statistics		Rate
Statistics cleared	2014-12-29 10:23:18	
Seconds since cleared	1238204	
Devices in configuration	5	
Devices online	5	
Devices online incl. prim. scan	5	
Devices offline	0	
Number of requests	2	
Number of queue overflows	0	
Current state	RCV_REQ_UD2	
Channel load	16.02%	
Maximum channel load	34.36%	
Rx bytes	35175419	28.41/s
Tx bytes	4340784	3.51/s
Tx total	867320	0.70/s
Tx errors	0	0.00/s
Device errors	0	0.00/s
Tx no response	0	0.00/s
Tx repetitions	560	0.00/s
Tx successful	866754	0.70/s
Tx E5 successful	309556	0.25/s
Tx short frame successful	0	0.00/s
Tx long frame successful	557198	0.45/s
Tx multitel successful	247646	0.20/s
E5 unexpected	0	0.00/s
Short frame unexpected	0	0.00/s
Long frame unexpected	0	0.00/s
T1 errors	26	0.00/s
Multitel count overflow	0	0.00/s
Frame errors	335	0.00/s
Only header response	207	0.00/s
Wrong source address	0	0.00/s
Wrong frame type	0	0.00/s
Wrong frame length	0	0.00/s

Figure 152: Statistics of the M-Bus port.

The following information is available:

- Statistics cleared: last time of statistics reset
- Devices in configuration: number of devices in data point configuration
- Devices online: number of devices which are currently online
- Devices online incl. prim. scan: number of devices in configuration which are online
- Devices offline: number of devices which currently appear offline
- Current state: state of the M-Bus stack (IDLE, SEND_REW, SEND_NOK, SEND_E5, RCV_REQ_UD2, WAIT_DONE)
- Channel load: channel load of the M-Bus channel averaged over 5 minutes
- Maximum channel load: maximum channel load since the last statistics clear
- Rx bytes: number of bytes received
- Tx bytes: number of bytes sent
- Tx total: total number of transmissions
- Tx errors: number of errors during a transmission
- Device errors: number of timed-out transmissions
- Tx no response: number of transmissions without a response
- Tx repetitions: number repeated messages
- Tx successful: number of successful transmissions
- Tx E5 successful: number of successfully received E5 responses

- Tx short frame successful: number of successfully received short frames
- Tx long frame successful: number of successfully received long frames
- Tx multitel successful: number of successfully received multi telegram frames
- E5 unexpected: number of unexpected E5 responses (misbehaving slave)
- Short frame unexpected: number of unexpected short frame responses (misbehaving slave)
- Long frame unexpected: number of unexpected long frame responses (misbehaving slave)
- T1 errors: number of slave responses not received
- Multitel count overflow: number of messages exceeding the maximum multi telegram number
- Frame errors: number of received frames with errors
- Only header response: number of responses containing only the message header
- Wrong source address: number of responses with a wrong slave address
- Wrong frame type: number of responses with wrong frame type
- Wrong frame length: number of responses with wrong frame length

7.4.5 M-Bus Protocol Analyzer

By activating the link Protocol Analyzer (available in the M-Bus statistics tab), the protocol analyzer page is shown as displayed in Figure 153.

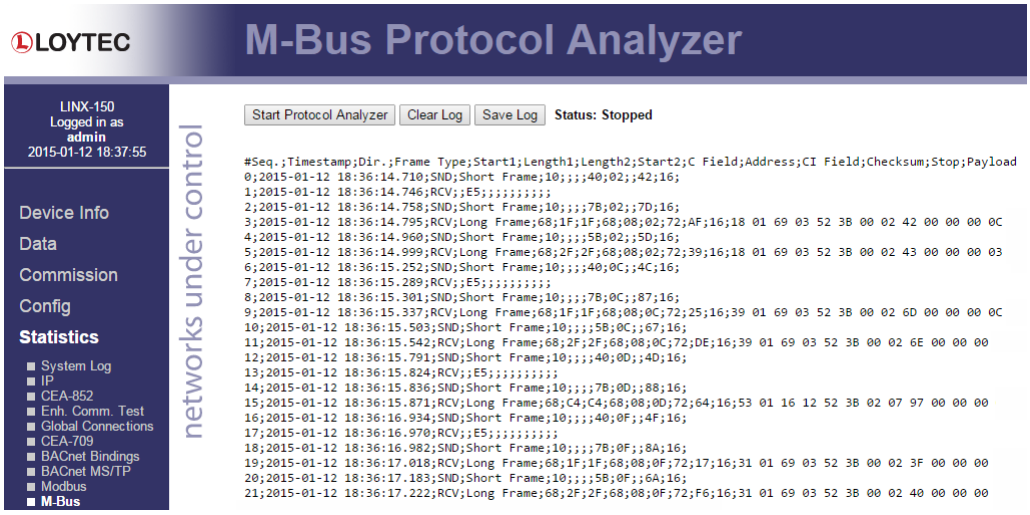


Figure 153: M-Bus protocol analyzer.

Next to the button the status of the protocol analyzer is shown. If the analyzer is started, an automatic refresh is performed every 60 seconds. By pressing the button **Start Protocol Analyzer** / **Stop Protocol Analyzer** the protocol analyzer can be started / stopped.

For every frame sent or received a line is presented using comma separated values. When stopped click on **Save Log** to store the protocol log as a CSV file. **Clear Log** clears the log data.

8 Modbus

8.1 Introduction

The Modbus is a de facto industrial standard which was initially intended for the communication between PLCs. In the meantime the Modbus has become an important interface for automatic meter reading applications and industrial applications. As the Modbus is an open protocol a large number of automation devices providing Modbus communication is available.

Two communication methods are available for Modbus. Modbus TCP utilizes Ethernet for the Modbus communication. Modbus RTU uses a RS-485 bus for Modbus data transfer. Modbus RTU uses a serial bus, which is controlled by a single master. This master can request data from several slave devices connected to the network. Modbus ASCII is also available on the RS-485 port.

8.2 Modbus Network

Modbus TCP utilizes the Ethernet for the communication. Several Modbus slave devices can be connected. In Modbus TCP a unit identifier is used instead of the slave address. Modbus slaves may have the same unit identifier. This unifier is usually used to communicate with bridges, routers and gateways. According to the Modbus specification, Modbus TCP masters should always use identifier 255 for the communication with a Modbus TCP slave.

The Modbus RTU network utilizes an RS485 connection. Several Modbus slave devices are connected in parallel to the transmission medium. Each Modbus device has a unique slave address in the range from 1 to 255. The Baud rate of the RS485 can be configured to use 1200, 2400, 4800, 9600, 19200, and 38400 Baud. The parity on the LINX-10x/11x/20x/21x models is always none and stop bits are not configurable. On the LINX-12x/15x/22x models and on the LGATE-950 parity and stop bits can be configured.

Modbus devices use function codes for the specification of the desired data. The following function codes for read/write actions are supported by the LOYTEC device:

- 02: Read discrete inputs.
- 01: Read coils.
- 05: Write coil.
- 04: Read input register
- 03: Read holding registers
- 06: Write holding registers

For optimizing the communication adjacent holding registers are usually read using a single read request. This behavior can be turned off for devices which do not support reading a random number of holding registers.

Modbus data points are specified by the function code, the address and the length. Furthermore, a data type has to be specified together with the information how the order of the bytes look like. Analog Modbus Master data points have a fixed network unit, while Modbus Slave data points adapt their representation on the network according to the selected unit system.

8.3 Web Interface

This section describes the Web interface for the Modbus port.

8.3.1 Port Configuration

The Modbus ports can be configured under the port configuration tabs of the Web UI (see Section 3.5.2). If available on a given port, the Modbus protocol can be enabled. If enabled, the Modbus communication settings on that port are displayed on the right-hand side. The RS485 port configuration tab is shown in Figure 154.

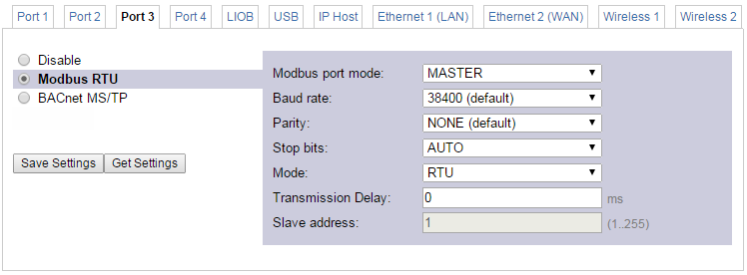


Figure 154: Modbus RS485 port configuration.

Modbus on RS-232 can be enabled on the LRS232-802 interface. This extension interface is connected to the USB port and needs to be enabled on the USB port tab as shown in Figure 156. Underneath the LRS232 selection, the two RS-232 ports can be configured. Choose **Modbus** in the drop-down box.

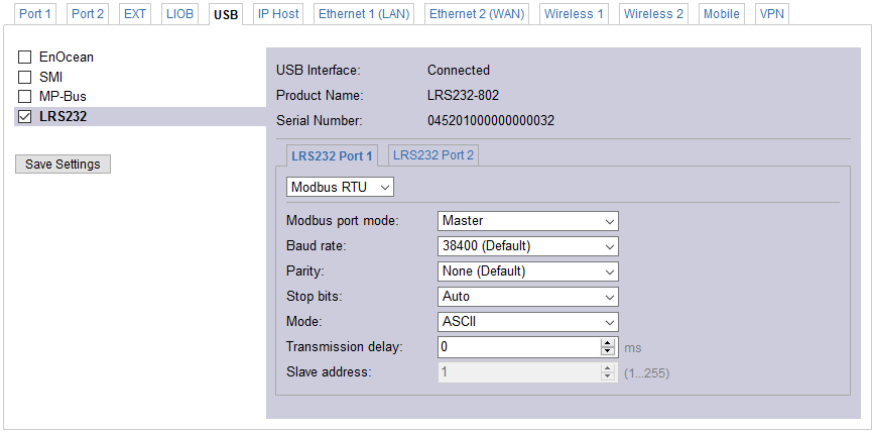


Figure 155: Configure Modbus on an LRS232-802 port.

For **Modbus port mode**, the following selections are available: **MASTER** can be selected, if the device shall operate as Modbus master. **SLAVE** can be selected, if the device shall operate as a Modbus slave on this port.

Under Baud rate the Baud rate for the Modbus communication can be configured. The available Baud rates are **1200, 2400, 4800, 9600, 19200, 38400 (default)**. The parity can be configured to **NONE**, **ODD** or **EVEN**, leading to the options 8N2, 8O1, 8E1, respectively[1]. The **Mode** specifies if the communication shall use the Modbus **RTU** mode or the Modbus **ASCII** mode.

If operated as Modbus master, an additional **Transmission delay** can be defined in milliseconds. This can improve communications on Modbus RS485 with slow devices that operate outside the timing specifications. Normally, leave this setting at '0'. If set, the transmission delay ensures that after sending a frame on the Modbus, the Modbus master holds back transmission of further frames for the specified time. As a Modbus slave, the user needs to define a unique **slave address** that this port will have on the Modbus channel.

Press the button **Save Settings** for storing the parameter configuration into the device or press **Get Settings** for overwriting the changes with the original configuration.

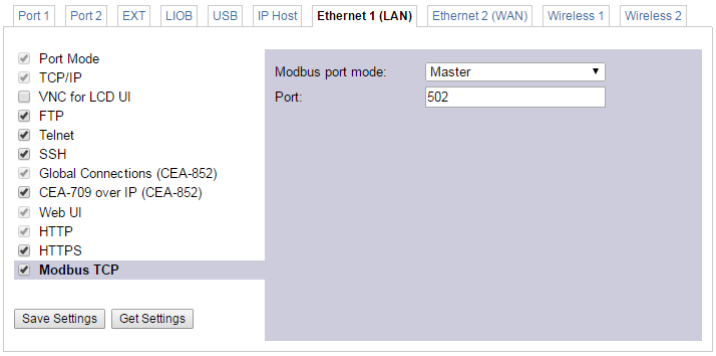


Figure 156: Modbus TCP port configuration.

On an Ethernet port, Modbus TCP can be enabled by selecting the check box. On devices with multiple IP interfaces, the Modbus TCP protocol can be activated only on one of them.

The Modbus TCP communication settings are displayed on the right-hand side as shown in Figure 156. For **Modbus port mode**, the following selections are available: **MASTER** can be selected, if the device shall operate as Modbus master. **SLAVE** can be selected, if the device shall operate as a Modbus slave on this port. Configure the desired TCP port, which is used by Modbus TCP devices on that channel. The default Modbus port number is 502.

8.3.2 Data Points

Modbus data points can be accessed through the Web UI as described in Section 3.3.1.

8.3.3 Commission

The commissioning Web UI allows assignment of physical devices to existing devices in the data point configuration, that have been created with the commission later option. Under the **Commission** menu choose the Modbus technology to open the Modbus commissioning interface. Select the appropriate Modbus interface tab.

The Web page shows a list of all **Devices in configuration**. An example is shown in Figure 157. Each line displays the device name and the Modbus device **Address** and communication **Port**. The **Status** column shows their current status. It can be one of the following:

[1] On LINX-100/101/110/111/200/201/210/211 models only **NONE** can be selected as parity, using 2 stop bits (8N2).

- OK: The device is configured for communication.
- Offline: The device is configured for communication but appears offline.
- Uncommissioned: The device is not yet commissioned.
- Disabled: The device is disabled.

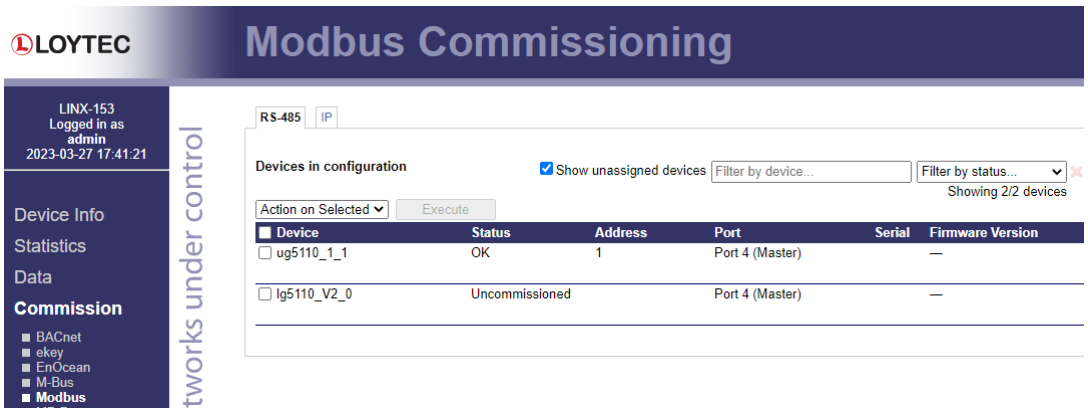


Figure 157: Modbus commissioning Web interface.

In order to execute an action on devices, select the checkbox at the beginning of the line. Then choose an action in the drop-down **Action on selected** and click on the **Execute** button. Actions that can be executed on all devices are enable and disable. A disabled device will stop communication on the network until it is enabled again.

Those devices created as commission later can be assigned to physical devices on the network. The device description displayed beneath the device name can be edited, where the edit symbol appears. The assignment can be done manually by editing the field in the **Address** and **Port** column. It is also possible to modify the Port setting (e.g. if the Modbus device has been moved to another channel).

To commission a Modbus TCP device, click on the IP tab. The list of devices includes an **IP** address column. Enter the IP address and optionally a port number, if the Modbus TCP slave device usese a non-standard port number, e.g., '192.168.24.220:1502'. You may also enter a Modbus **Address**. This is typically needed for Modbus TCP gateways.

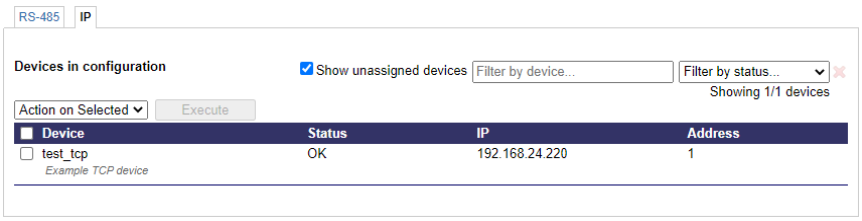
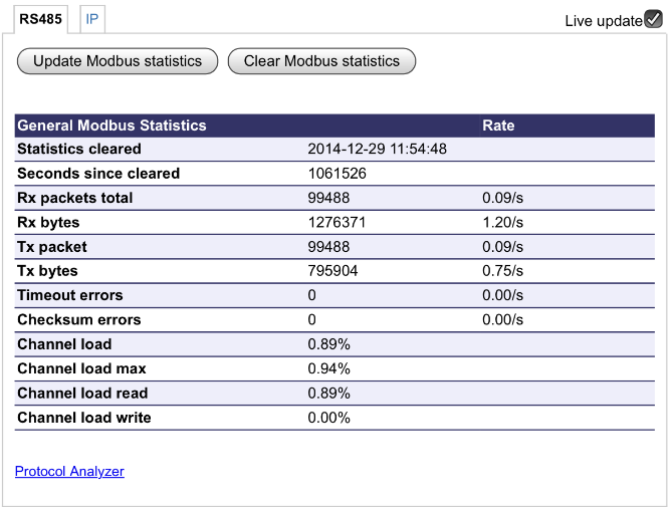


Figure 158: Modbus TCP commissioning Web interface.

8.3.4 Statistics

Figure 159 shows a typical output of the statistics information which can be displayed for the Modbus ports. For each port available one statistics tab is displayed. The statistics can be cleared for each Modbus port separately by pressing the **Clear Modbus statistics** button. A refresh of the statistics is done automatically. To stop automatic update, deselect the **Live update** checkbox. For manual update press **Update Modbus statistics**.



General Modbus Statistics		Rate
Statistics cleared	2014-12-29 11:54:48	
Seconds since cleared	1061526	
Rx packets total	99488	0.09/s
Rx bytes	1276371	1.20/s
Tx packet	99488	0.09/s
Tx bytes	795904	0.75/s
Timeout errors	0	0.00/s
Checksum errors	0	0.00/s
Channel load	0.89%	
Channel load max	0.94%	
Channel load read	0.89%	
Channel load write	0.00%	

Figure 159: Statistics of the Modbus port.

The following information is available:

- Statistics cleared: last time of statistics reset
- Rx packets: number of Modbus packets received
- Rx bytes: number of bytes received
- Tx packets: number of Modbus packets sent
- Tx bytes: number of bytes sent
- Timeout errors: number of communication errors (timeout)
- Checksum errors: number of communication errors (wrong checksum)
- Channel load: Current channel load averaged over 5 minutes.
- Channel load max: Maximum channel load since last statistics clear.
- Channel load read: Current channel load due to read requests.
- Channel load write: Current channel load due to write requests.

8.3.5 Modbus Protocol Analyzer

By activating the link Protocol Analyzer (available in all Modbus statistics tabs), the protocol analyzer page is shown as displayed in Figure 160.

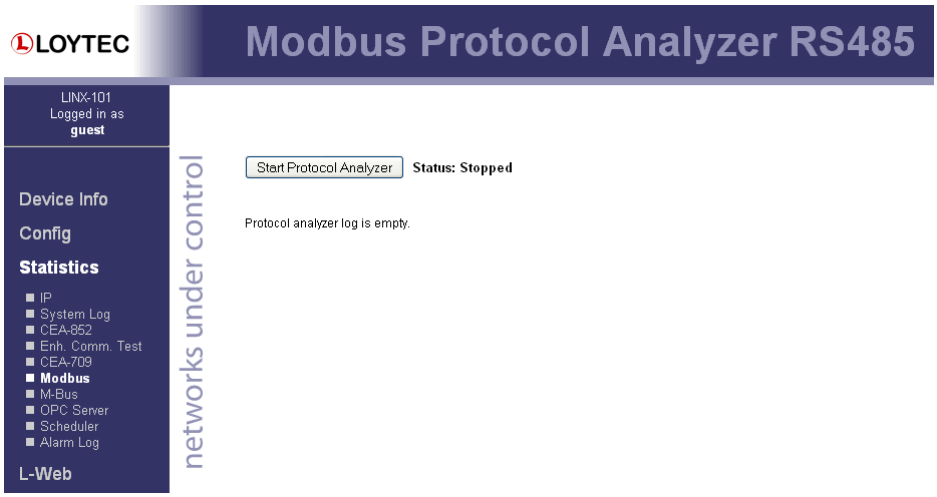


Figure 160: Modbus protocol analyzer.

Next to the button the status of the protocol analyzer is shown. If the analyzer is started, an automatic refresh is performed every 60 seconds. By pressing the button **Start Protocol Analyzer** / **Stop Protocol Analyzer** the protocol analyzer can be started / stopped.

For every frame sent or received a line is presented using comma separated values. When stopped click on **Save Log** to store the protocol log as a CSV file. **Clear Log** clears the log data.

8.3.6 L-STAT Device Management

L-STAT devices are listed on the Modbus commission Web UI along with other Modbus devices. They have, however, special management options such as firmware upgrade and configuration backup and restore. The device list shows the columns **Serial** and **Firmware Version** to display information available for L-STAT Modbus devices. An example is shown in Figure 161.

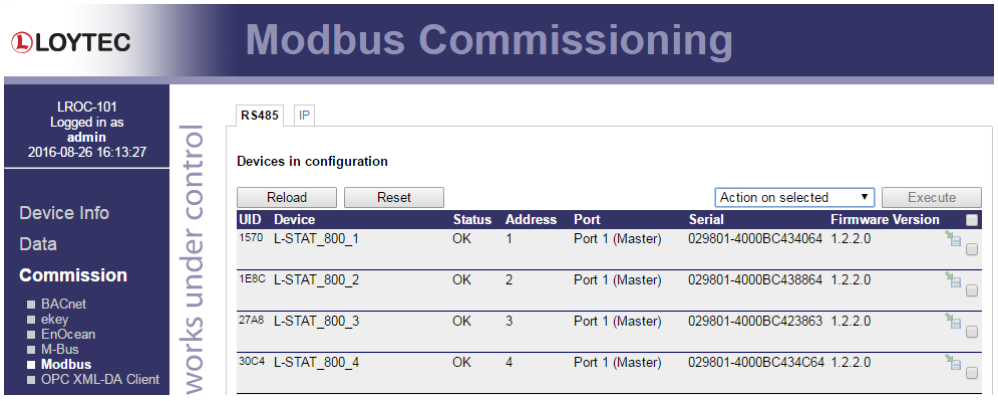


Figure 161: Modbus commission for L-STAT devices.

For L-STAT Modbus devices the following actions are available in addition to the standard Modbus device actions:

- **Update Firmware**: Select this action to upgrade all selected L-STAT devices. The **Execute** button changes to a **Select File** button. Choose an L-STAT firmware image and start the upgrade. L-STAT devices are upgraded all in parallel to utilize the available Modbus bandwidth in the best way.

- **Backup Configuration**: Execute this action in order to upload L-STAT device backups. One backup file per selected L-STAT device is stored on the local disk.

- **Restore Configuration**: Select this action to restore all selected L-STAT devices. The **Execute** button changes to a **Select File** button. Choose an L-STAT backup image and start the restore process. The selected backup image is restored to all selected L-STAT devices.

9 KNX

9.1 Introduction

KNX is a European and international standard (EN 50090, ISO/IEC 14543-3) designed for building automation. It is the successor to the European Installation Bus (EIB) and also merged Batibus and the European Home System Protocols (EHS) into one standard. KNX covers lighting, HVAC, sunblinds, A/V control, metering among many other application areas.

KNX models actuators and sensors as a set of communication objects. A communication objects represents a typed value, such as a room temperature, a switch state or an illumination level. These objects are then mapped to group addresses. Typically, a sensor emits a group message containing its present value which is received and processed by the actuators. Sensors and actuators can be parameterized to implement various switching and controlling scenarios.

KNX supports different media, among them twisted pair (TP1), powerline, RF and IP-based networks (KNXnet/IP). Each KNX node is a master and can transmit a frame at any time.

LOYTEC devices support two media types, KNX/TP1 and KNXnet/IP. KNX/TP1 is a twisted pair medium, which uses a CSMA protocol with collision avoidance at 9600 baud. Simple devices can be bus-powered while routers and gateways are typically self-powered. KNXnet/IP transmits KNX frames over a UDP multicast address and is typically used in the backbone area.

A KNX network can be structured in a loopless topology. KNX routers are called couplers and connect two network segments, which are called lines. The smallest topology contains a single line with up to 64 devices which can be extended to 256 devices. If the system exceeds this limit, up to 15 lines can be connected to an area using line couplers. Finally, up to 15 areas can be connected which allows approximately 57600 devices to be connected to a KNX network.

9.2 Hardware Installation

KNXnet/IP is supported on the built-in Ethernet interface, so no additional hardware is required for KNXnet/IP. KNXnet/IP can be enabled in the port configuration of the Ethernet interface.

For using KNX/TP1, the LKNX-300 interface has to be attached to the extension port of the LOYTEC device. This port is labeled EXT on the LINX-12x/15x/22x and LGATE-950 devices. The KNX/TP1 functionality has to be enabled in the port configuration settings for the extension port.

9.2.1 LKNX-300 Installation

The LKNX-300 needs to be attached to the extension bus of the L-INX or L-GATE. It is possible to connect the LKNX-300 before, mid of or behind L-IOB devices. In any case, you

need to connect the 3-wire **EXT** port. Follow the cabling instructions of Figure 162 between the **EXT** port of the L-INX and the **EXT** port on the LKNX-300.

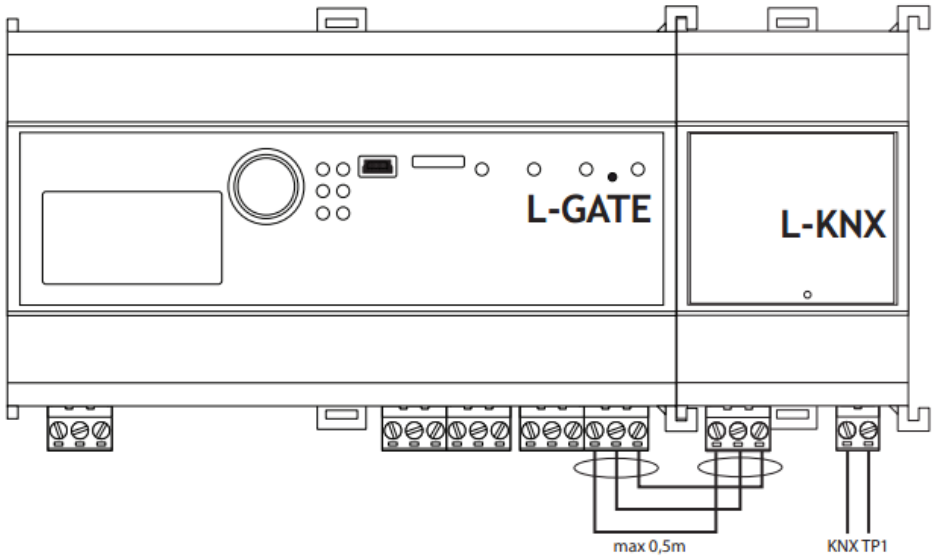


Figure 162: Connection L-KNX over the extension port.

9.3 KNX Network

KNX devices are modeled as a set of communication objects which communicate over group message to each other. Each possible communication target receives the group message and checks if there are communication objects connected to this group address. The communication objects use the standardized KNX data point types (DPTs).

The KNX interfaces can be used independently. It is possible to use a KNX TP1 and a KNXnet/IP network at the same time. The interfaces can be connected to the same or to two different KNX networks.

The LOYTEC KNX interface allows sending and receiving these messages and to connect them to data points which can be used for Alarming, Scheduling and Trending. They also can be used in connections to other technologies and as variables for math objects and IEC 61131 programs.

9.4 Web Interface

This section describes the Web interface for the KNX interfaces.

9.4.1 Configuration

To enable the KNX ports, use the port configuration web interface. The settings for enabling the KNX/TP1 interface are shown in Figure 163 and the settings for enabling the KNXnet/IP interface are shown in Figure 164. On devices with multiple IP interfaces, the KNXnet/IP protocol can be activated only on one of them.

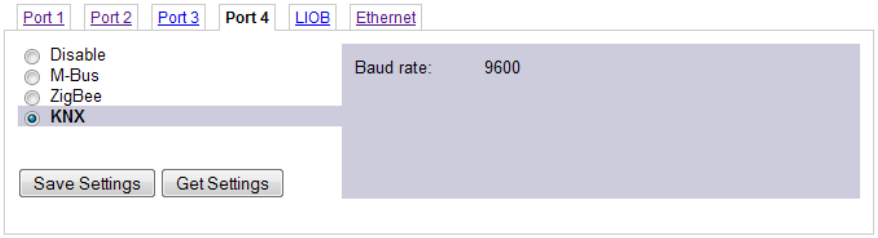


Figure 163: Enabling the KNX/TP1 interface

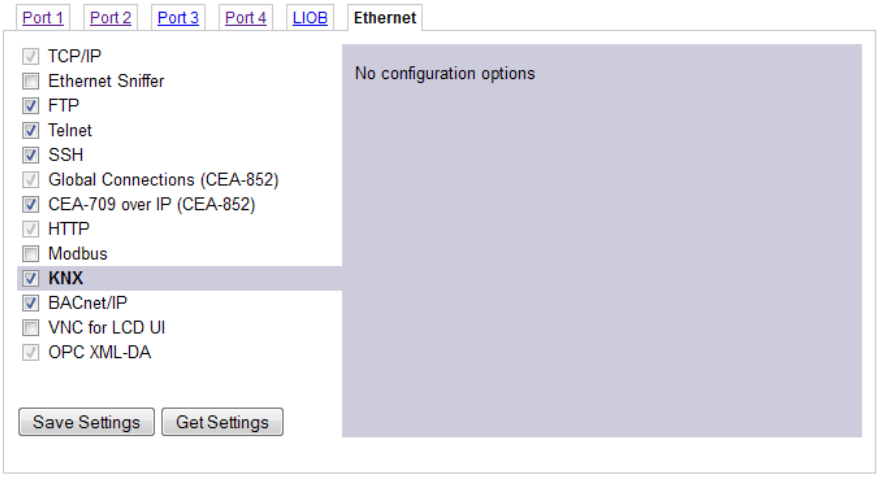


Figure 164: Enabling the KNXnet/IP interface

9.4.2 Data Points

KNX data points can be accessed through the Web UI as described in Section 3.3.1.

9.4.3 KNX Protocol Analyzer

By clicking the link **KNX PA** in the **Statistics** menu, the KNX protocol analyzer page is shown as displayed in Figure 165.

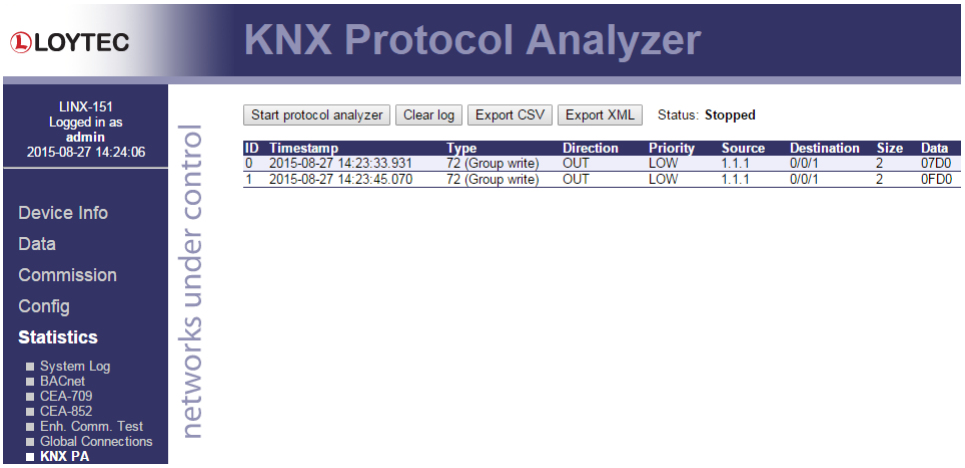


Figure 165: KNX protocol analyzer.

Next to the control buttons the status of the protocol analyzer is shown. If the analyzer is started, an automatic refresh is performed every 60 seconds. By pressing the button **Start Protocol Analyzer** / **Stop Protocol Analyzer** the protocol analyzer can be started / stopped.

For every frame sent or received a line is presented in the table. When the protocol analyzer has been stopped, click on **Export CSV** to store the protocol log as a CSV file or **Export XML** to store as an XML file. The XML file can be opened in the ETS protocol viewer. **Clear Log** clears the log data.

10 SMI

10.1 Introduction

The Standardized Motor Interface (SMI) allows controlling sunblinds over a bus-topology network. Depending on the operating voltage of the electrical motors, SMI devices come in low-voltage (LoVo) or high-voltage (HiVo) models. SMI allows for precise motor control by steps instead of position estimation by measuring motor run-time. One SMI channel can operate up to 16 sunblind motors.

All LOYTEC devices with an EXT port can be extended by the L-SMI interface and connect to an SMI bus. The LSMI-800 supports one HiVo SMI channel. The LSMI-804 supports up to 4 channels, both LoVo and HiVo. The LINX Configurator provides SMI device templates, which can be commissioned on the device Web interface. The Web interface supports manual address assignment, scanning for SMI devices and calibration.

The LOYTEC product supports the SMI standard and provides the following features:

- Support common SMI equipment to control sunblinds.
- Configurable through device templates using the Configurator software.
- Web UI for SMI device assignment and calibration.
- Easy device replacement on the Web UI.
- Connected via L-SMI to the EXT port or USB port.

10.2 Hardware Installation

It is possible to command an SMI motor in button operation mode. This is done by connecting phase L to either I+ or I– to manually drive the sunblind down (I+) or up (I–) without bus communication. When doing such a test, attach the LOYTEC SMI interface after having completed this test.

Important!	***In button operation mode (phase connected to I+ or I–) the LOYTEC SMI interface must be disconnected!***

10.2.1 LSMI-800

The LSMI-800 interface serves one SMI channel and must be attached to the EXT port of the LOYTEC device. It is possible to connect the LSMI-800 before, mid of or behind L-IOB devices. In any case, you need to connect the 3-wire **EXT** port. Follow the cabling instructions of Figure 162 between the **EXT** port of the device and the **EXT** port on the LSMI-800. The cabling should not exceed 0.5m.

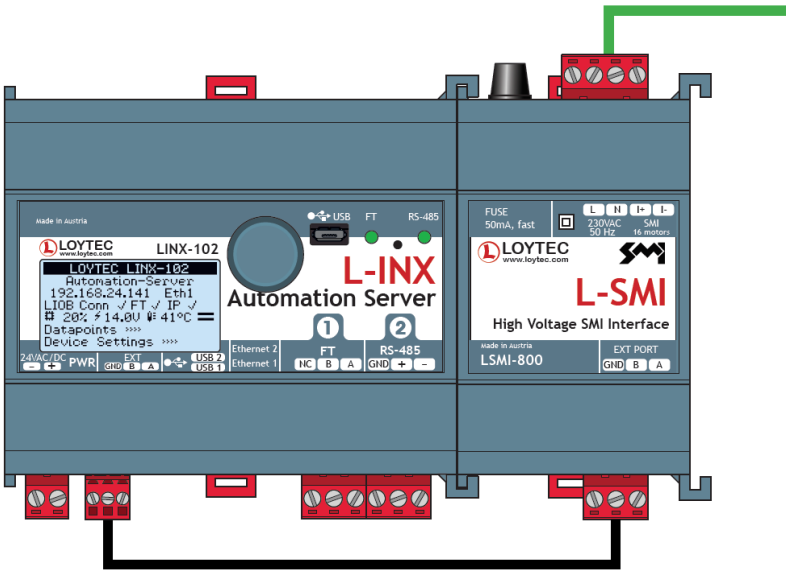


Figure 166: Connecting the LSMI-800 over the EXT port.

10.2.2 LSMI-804

The LSMI-804 interface is connected via USB to the LOYTEC device. It supports up to 4 SMI channels as well as an integrated circuit for power cut-off for each channel. For power cut-off a separate relay can turn off power to the SMI channel. The relay is available as a data point in the device configuration, which can be connected to the SMI channel's power-on data point.

The power-on data point is then able to turn on the SMI channel power before the LOYTEC device sends a command to an SMI motor device. This saves power in motor idle state.

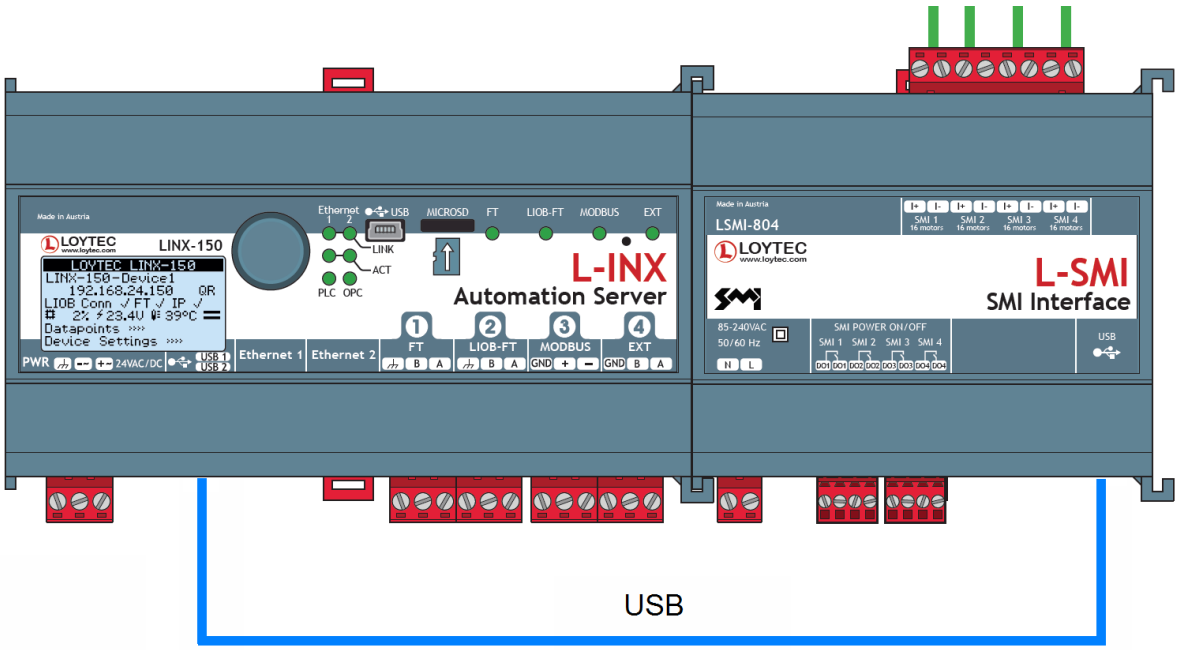


Figure 167: Connecting the LSMI-804 over the USB port.

10.3 Web Interface

10.3.1 Configuration

To enable the SMI port, use the port configuration Web interface. The settings for enabling the SMI interface are shown in Figure 168.

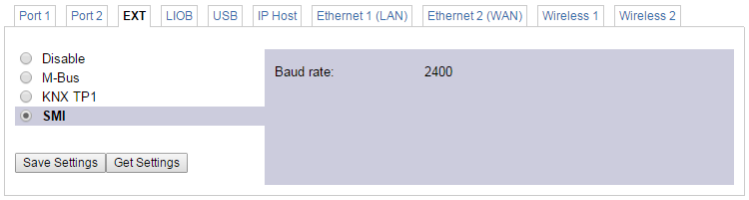


Figure 168: Enabling the SMI interface

10.3.2 Data Points

SMI data points can be accessed through the Web UI as described in Section 3.3.1.

10.3.3 Commissioning

The **Commission** Web interface provides a page for managing and commissioning SMI devices. This page lists all SMI devices, which have been created in the data point configuration as shown in Figure 169. The list shows device names as created in the configuration. The device **Status** can be one of the following:

- OK for a configured, online and working SMI device,
- Offline: The device is configured for communication but appears offline,
- Uncommissioned for an unlinked SMI device that needs assignment,
- Disabled for a temporarily disabled SMI device.

The **Manufacturer** column shows information on the SMI device manufacturer. In the **Serial** number column, the serial numbers of the SMI devices to be installed can be pre-configured. It can also be left empty, in which case the serial numbers of attached SMI devices can be scanned. **Port** and **Address** are assigned automatically once a device is online. The **Port** can be manually changed, if the device has been moved to another physical port (e.g. from internal SMI to LSMI-804).

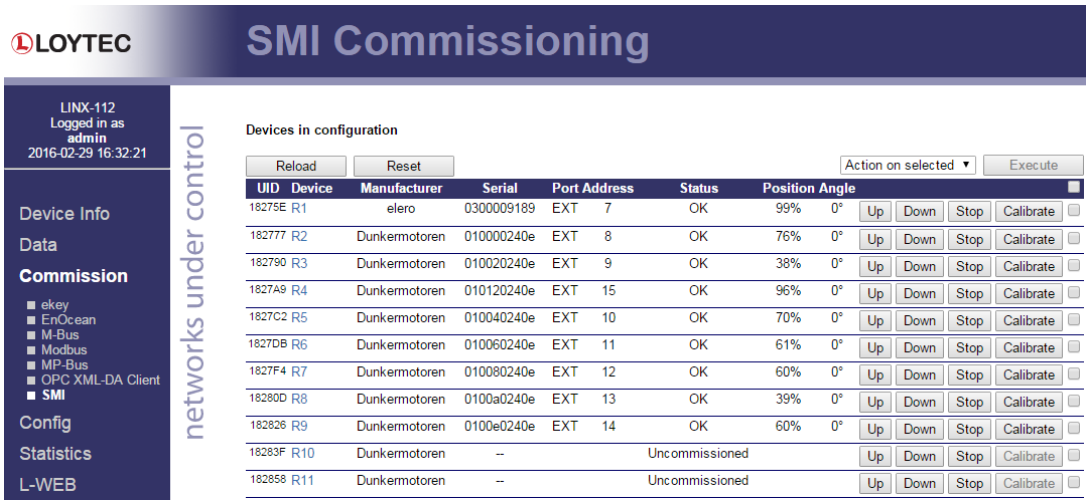


Figure 169: SMI commissioning Web interface.

For a quick online test and to identify an SMI device, the buttons **Up** and **Down** can be used to command a sunbind to the upper or lower position. The **Stop** button stops the sunblind motor.

In order to execute an action on devices, select the checkbox at the end of the line. Then choose an action in the drop-down **Action on selected** and click on the **Execute** button. Actions that can be executed on all devices are unassign, enable, disable, UP, DOWN, and STOP. A disabled device will stop communication on the network until it is enabled again.

Assignment of SMI devices can be done by scanning attached SMI devices. Select the port to be scanned in the **Scan options** drop-down list. If **Scan all** is selected, the scan will produce a list of devices attached to any of the available SMI ports. This is shown in the list **Scanned devices not in configuration** as depicted in Figure 170.



Figure 170: Result of the SMI scan on the Web interface

To assign a scanned device to an uncommissioned device in the configuration, select the corresponding device name from the drop-down box in the **Assignment** column. Use the buttons **Up**, **Down** and **Stop** to physically identify a scanned device in the list. Repeat that for all other devices and then click the button **Assign**. Those SMI devices with a pre-configured serial number will be automatically assigned. The port and address information is also automatically assigned in this step.

Note:	*When assigning an address manually, choose addresses starting from 15 downwards to 0. Assigning address 0 only works, if all other addresses have been assigned already.*

10.3.4 Calibration

Calibration of the SMI devices is also done on the commissioning Web page. In order to operate an SMI sunblind accurately using position/rotation, a number of parameter settings need to be set. This can be done manually or by following the steps of a calibration wizard.

To manually calibrate an SMI device, click on the Calibrate button for a commissioned SMI device. A dialog opens as shown in Figure 171. Calibration data usually depends on the mechanical construction of the sunblind and not only on the SMI motor.

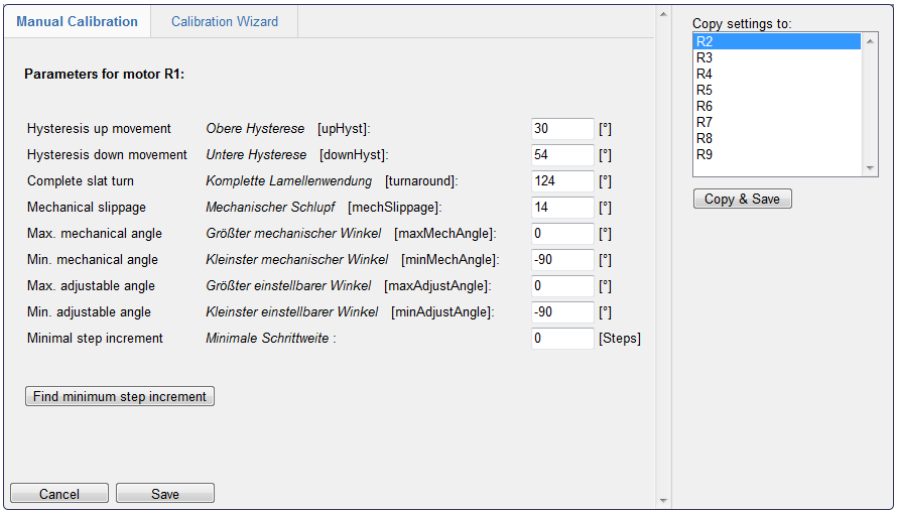


Figure 171: Manual calibration on the Web interface.

Enter the following calibration parameters:

- **Hysteresis up movement:** The upper hysteresis specifies the number of motor axis degrees needed in order to get actual angular movement when starting out of the upper angular position.
- **Hysteresis down movement:** The bottom hysteresis specifies the number of motor axis degrees needed in order to get actual angular movement when starting out of the bottom angular position.
- **Complete slat turn:** The number of required motor axis degress to reach a complete slat turn.
- **Mechanical slippage:** The mechanical slippage specifies the number of motor axis degrees needed in order to get physical rotation when reversing motion from an angular position in the opposite direction.
- **Max. mechanical angle:** The maximum angle, which is mechanically possible. This value is defined by the sunblind.
- **Min. mechanical angle:** The minimum angle, which is mechanically possible. This value is defined by the sunblind.
- **Max. adjustable angle:** Limits the maximum angle which can be set.
- **Min. adjustable angle:** Limits the smallest angle which can be set.
- **Minimal step increment:** Minimal amout of steps required to trigger a movement of the SMI motor.

Use the **Find minimum step increment** button to perform a calibration run in order to determine the minimal step increment. This is done by executing movments in downwards and upwards direction. The result is displayed next to the button and it is also automatically saved to the associated calibration paramter.

Once an SMI device has been calibrated, the motor is ready to be precisely operated via position and rotation commands. To copy calibration data on similar SMI motors, multi-select the devices in the list **Copy settings to** and click the **Copy** button.

If calibration data is not known, a calibration wizard can be used to calibrate an SMI device online. In the calibration dialog select the **Automatic Calibration** tab as shown in Figure 172.

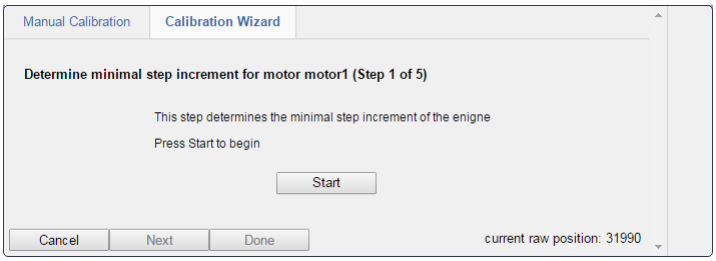
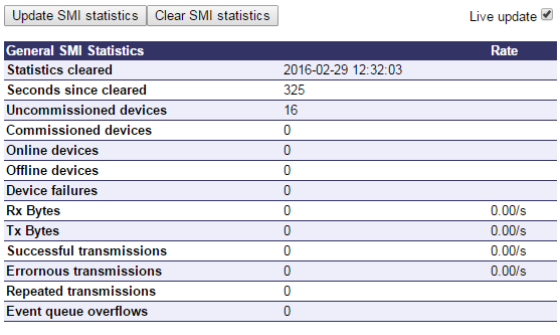


Figure 172: SMI calibration wizard on the Web interface.

Click on the **Start** button and follow the instructions of the wizard. For each calibration step follow the instructions and click the **Next** button. The calibration process can be terminated at any time by clicking **Cancel**. In the end the dialog shows a summary of the calculated calibration data for later use.

10.3.5 Statistics

Figure 173 shows a typical output of the statistics information which can be displayed for the SMI ports. The statistics can be cleared by pressing the **Clear SMI statistics** button. A refresh of the statistics is done automatically. To stop automatic update, deselect the **Live update** checkbox. For manual update press **Update SMI statistics**.



General SMI Statistics		Rate
Statistics cleared	2016-02-29 12:32:03	
Seconds since cleared	325	
Uncommissioned devices	16	
Commissioned devices	0	
Online devices	0	
Offline devices	0	
Device failures	0	
Rx Bytes	0	0.00/s
Tx Bytes	0	0.00/s
Successful transmissions	0	0.00/s
Errornous transmissions	0	0.00/s
Repeated transmissions	0	
Event queue overflows	0	

Figure 173: SMI statistics of the Web interface.

The following information is available:

- Statistics cleared: last time of statistics reset
- Seconds since cleared: number of seconds since last clear
- Uncommissioned devices: Number of devices in configuration, which have not been commissioned
- Commissioned devices: Number of commissioned devices

- Online devices: Number of devices currently online
- Offline devices: Number of commissioned devices which are not online
- Device failures: Number of devices that have the SMI error_code bit set. This error bit is set, if the SMI motor reports an error during a status query.
- Rx bytes: number of bytes received.
- Tx bytes: number of bytes sent.
- Successful transmissions: Transmitted which have been acknowledged by an SMI device (ACK, NACK, or data).
- Erroneous transmissions: Number of failed transmissions. There has been a CRC error or the device did not respond in time.
- Repeated transmissions: Number of repeats because of timeouts or erroneous responses.
- Event queue overflows: This counter increases if the queue overflows for transmit or receive messages.

10.3.6 Protocol Analyzer

By activating the link Protocol Analyzer (available in all SMI statistics tabs), the protocol analyzer page is shown as displayed in Figure 174.

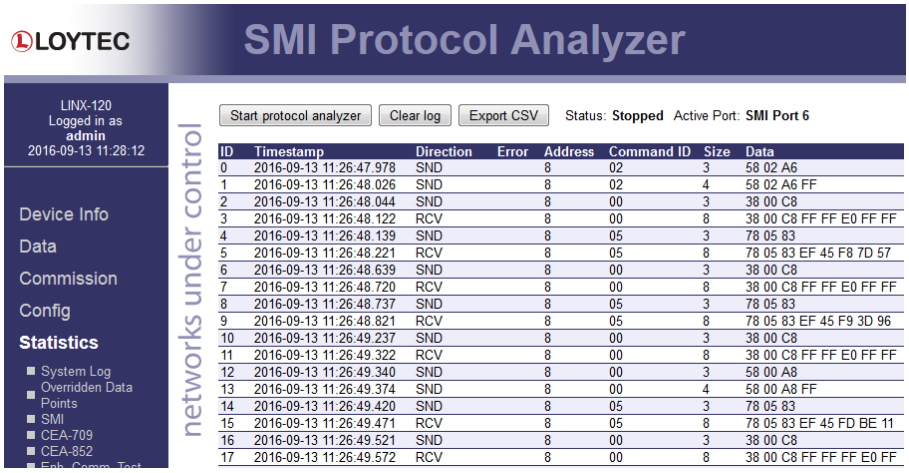


Figure 174: SMI protocol analyzer.

Next to the button the status of the protocol analyzer is shown. If the analyzer is started, an automatic refresh is performed every 60 seconds. By pressing the button **Start Protocol Analyzer** / **Stop Protocol Analyzer** the protocol analyzer can be started / stopped.

For every frame sent or received a line is presented using comma separated values. When stopped click on **Export CSV** to store the protocol log as a CSV file. **Clear Log** clears the log data.

11 EnOcean

11.1 Introduction

EnOcean is an international standard (ISO/IEC 14543-3-10) designed for wireless devices optimized for solutions with ultra-low power consumption and energy harvesting. This means EnOcean sensors can be self-powered and draw energy from a button press or a solar cell without the need for a battery. EnOcean wireless communication uses different frequency bands in Europe, U.S. and Japan.

The EnOcean Alliance standardizes so-called EnOcean equipment profiles (EEPs) to make sensors and actuators from different vendors interoperable. The EEP is an identifier which is used for interpreting a wireless datagram and extracting its contents. For secure communication EnOcean provides a security option, that device vendors may choose to implement.

The LOYTEC product supports the EnOcean standard and provides the following features:

- Support all common EnOcean equipment profiles (EEPs) for sensors and actuators.
- Configurable through device templates using the Configurator software.
- Web UI for teach-in, signal strength, and value test.
- Easy device replacement on the Web UI.
- Connected via L-ENO EnOcean interface over the USB port.
- Support of multi-channel EnOcean devices.
- Encrypted wireless connection for EnOcean devices that support it.
- Supports Mailbox function for sleepy actuators (e.g., battery-powered radiator valve).

11.2 Hardware Installation

For using EnOcean, the LENO-80x EnOcean interface has to be attached to the USB port of the LOYTEC device. This port is labeled USB1 or USB2 on the LINX-12x/15x/22x and LGATE-950 devices. The EnOcean functionality has to be enabled in the port configuration settings for the USB port.

The L-ENO EnOcean interfaces are available in three different versions for worldwide use:

- LENO-800: Europe 868 MHz band
- LENO-801: USA/Canada 902 MHz band

- LENO-802: Japan 928 MHz band

11.3 Web Interface

11.3.1 Configuration

To enable the EnOcean protocol on the USB port, use the port configuration Web interface. The settings for enabling the EnOcean protocol are shown in Figure 175. The protocol information area shows whether a LENO-80x EnOcean interface has been connected and provides some details on that interface such as EnOcean ID and serial number.

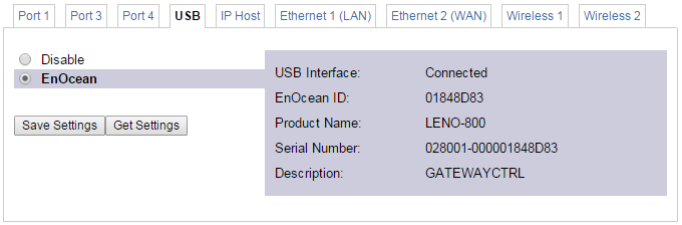


Figure 175: Enabling the EnOcean protocol

11.3.2 Data Points

EnOcean data points can be accessed through the Web UI as described in Section 3.3.1.

11.3.3 Commissioning

The **Commission** Web interface provides a page for managing and commissioning EnOcean devices. This page lists all EnOcean devices, which have been created in the data point configuration as shown in Figure 176. The list shows device names as created in the configuration. The device **Status** can be one of the following:

- OK for a working EnOcean device,
- Uncommissioned for an unlinked EnOcean device that needs teach-in,
- Old Data if no new data has been received within a reasonable timeframe (one day),
- Waiting for Device ID if a teach-in is in progress.

The **Profile** column shows information on the profile ID and received data when expanding it. The **RSSI** column shows the signal strength and intermediate hops this device is reached over.

To teach-in an uncommissioned device, click the **Teach-In** button. The Web interface then waits for a teach-in message sent by an EnOcean device with matching profile ID. Press the button on the EnOcean device and the corresponding EnOcean device ID is associated with the device. A manual assignment can be done by editing the device ID of the respective device.

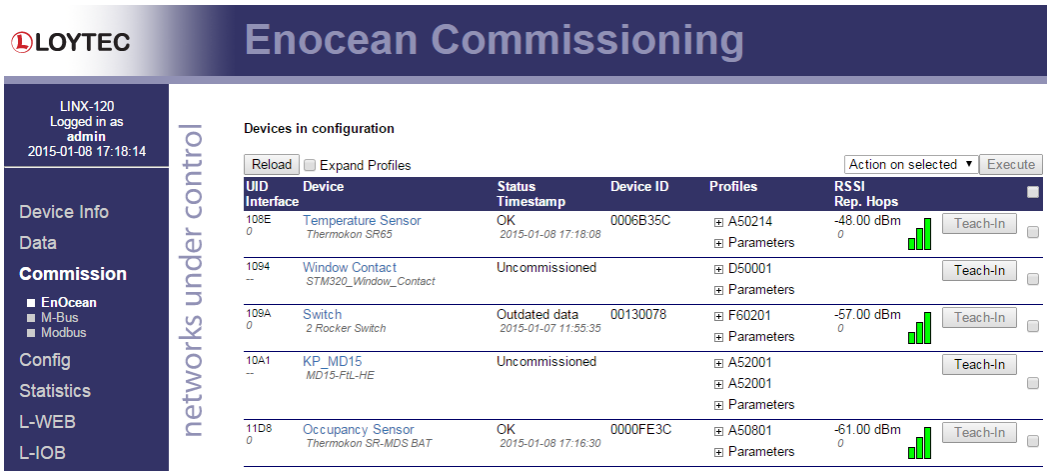


Figure 176: Commission EnOcean devices

Expand the **Parameters** item to display and edit a **Description** and **Location** string describing the EnOcean device. These strings can also be found as data points under the respective EnOcean device folder and appear as parameters in LWEB-900. A click on the device name link will lead you to that folder location in the data point Web interface.

To clear device assignments check one or more check boxes at the end of each line, choose the **Decommission** option in the **Action on selected** drop-down and click **Execute**. The selected devices will then be unassigned and appear as uncommissioned again. Devices can also be temporarily disabled. When disabled, no further data is processed from the respective devices until they are enabled again later.

11.3.4 Configure a Transmission ID

Certain EnOcean actuator devices require different sender's EnOcean IDs in the teach-in process in order to distinguish between the senders. An example are lamp actuator devices that need to learn EnOcean IDs of rocker switches using broadcasts only. In this case the LOYTEC device needs to simulate a sending rocker switch and a unique ID must be sent out per rocker switch. The EnOcean transmission ID can be configured in this scenario.

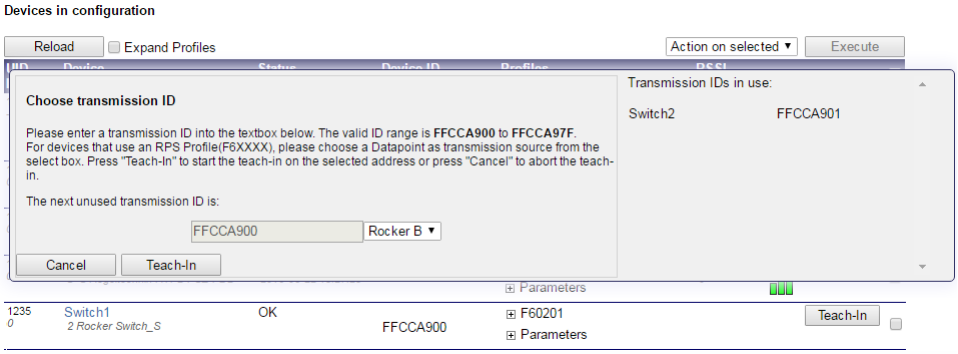


Figure 177: Teach-in using a transmission ID.

To Teach In a Device with Transmission ID

1. Bring the EnOcean actuator device into teach-in mode, e.g. in the lamp actuator device.

2. On the EnOcean commission Web interface click the teach-in button for the respective transmission device, e.g. a rocker switch. A dialog opens as shown in Figure 177 that prompts for a transmission ID.

3. Choose the proposed ID as the next unused ID on the LOYTEC device. Note that this must not be used by other LOYTEC devices that send to a different actuator.

4. Optionally, choose rocker plate A or B for teach-in.

5. Then click the teach-in button in the window. This sends a message using the chosen transmission ID to the EnOcean actuator to complete the process.

11.3.5 Statistics

Figure 178 shows a typical output of the statistics information which can be displayed for the EnOcean ports. For each port available one statistics tab is displayed. The statistics can be cleared for each EnOcean port separately by pressing the **Clear EnOcean statistics** button. A refresh of the statistics is done automatically. To stop automatic update, deselect the **Live update** checkbox. For manual update press **Update EnOcean statistics**.

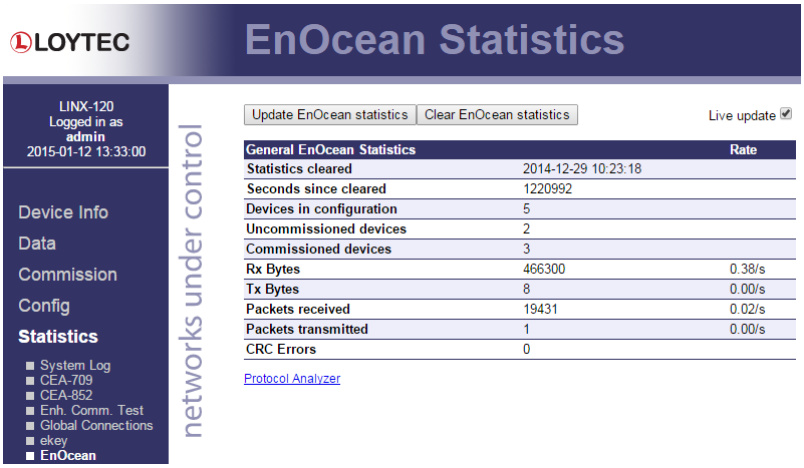


Figure 178: Statistics of the EnOcean port.

The following information is available:

- Statistics cleared: last time of statistics reset,
- Devices in configuration: Total EnOcean devices in data point configuration,
- Uncommissioned devices: Devices that need teach-in,
- Commissioned devices: Devices with teach-in completed,
- Rx Bytes: number of bytes received,
- Tx Bytes: number of bytes sent,
- Packets received: number of EnOcean packets received,
- Packets transmitted: number of EnOcean packets transmitted,
- CRC errors: number of communication errors with wrong CRC.

11.3.6 Protocol analyzer

By activating the link **Protocol Analyzer** (available in all EnOcean statistics tabs), the protocol analyzer page is shown as displayed in Figure 179.

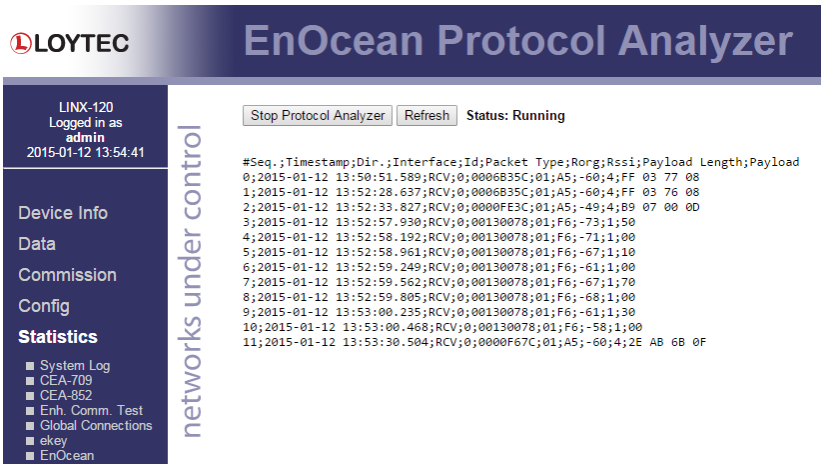


Figure 179: EnOcean protocol analyzer.

Next to the button the status of the protocol analyzer is shown. If the analyzer is started, an automatic refresh is performed every 60 seconds. By pressing the button **Start Protocol Analyzer** / **Stop Protocol Analyzer** the protocol analyzer can be started / stopped.

For every frame sent or received a line is presented using comma separated values. The page refreshes automatically with a given interval. Press the **Refresh** button to get the latest updates immediately. When stopped click on **Save Log** to store the protocol log as a CSV file. **Clear Log** clears the log data.

12 MP-Bus

12.1 Introduction

The MP-Bus is the Belimo master/slave bus, which can be used to connect Belimo MP-Bus devices. On a regular bus up to 8 slaves can be connected to the MP-Bus port of the LOYTEC device, which acts as the master, e.g., damper actuators, valve actuators, MP fire damper actuators or MP VAV devices. MP-Bus devices are bus-powered over a 3-wire cable (24V, GND, MP) and follow no specific restriction of network topology; bus, star, tree and mixed topologies are possible.

The LOYTEC MP-Bus master supports the following two basic addressing modes:

- Point-to-Point Mode (PP mode): In this mode only one MP-Bus device is attached. It supports full auto-commission and is the default mode.

- Multi-Point Mode (MP mode): In this mode up to 8 MP-Bus slaves devices can be connected. The devices need to be commissioned by assigning a serial number or by pressing a button. A short address is automatically assigned to each device.

The number of 8 slave devices can be extended to 16 MP-Bus light (MPL) devices. These devices have a limited set of functions and put less burden on the bus. In this setup mode, MPL and non-MPL devices cannot be mixed.

12.2 Hardware Installation

12.2.1 Built-In MP-Bus Port

MP-Bus devices can be connected to LOYTEC devices with a dedicated MP-Bus port only. It is not possible to connect to an RS-485 or EXT port. MP-Bus devices are connected using an unshielded 3-wire cable. There are LOYTEC MP-Bus ports that provide only the communication signals BUS, GND (LROC-40x). These models require the connection of an external power supply as depicted in Figure 180.

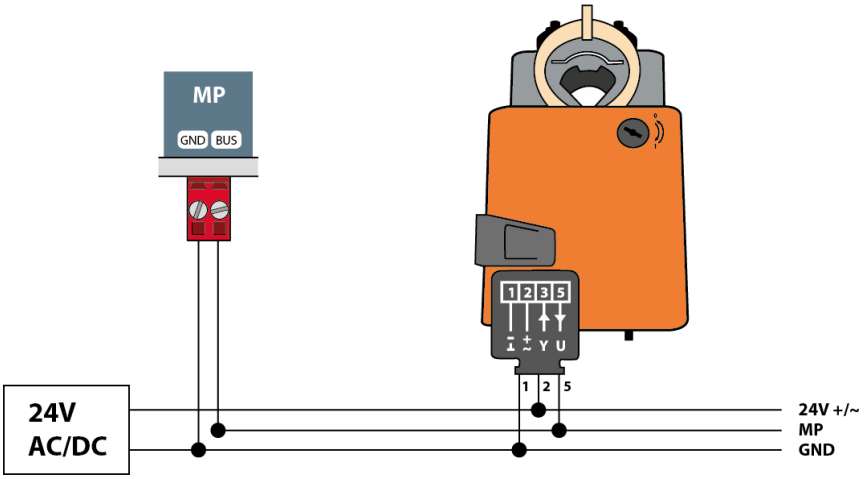


Figure 180: MP-Bus port connector with external bus-power.

Other LOYTEC device models also provide the MP-Bus power 24V (LIOB-AIRx). The port connection to MP-Bus devices is depicted in Figure 181. Note, that some LIOB-AIR models already come pre-cabled with a Belimo MPL device.

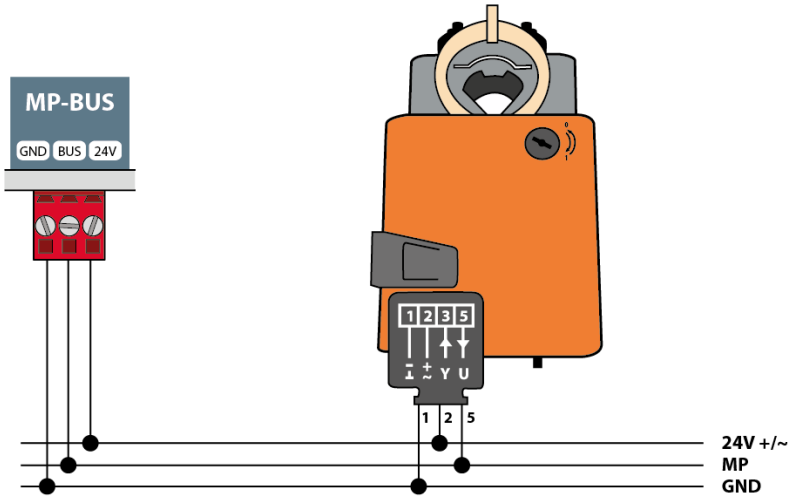


Figure 181: MP-Bus port connector with integrated bus-power.

12.2.2 LMPBUS-804

Other LOYTEC devices with no built-in MP-Bus port can be extended by the LMPBUS-804 interface, which is connected via USB to the LOYTEC device. This interface supports up to four MP-Bus channels. The port connection to MP-Bus devices is depicted in Figure 182.

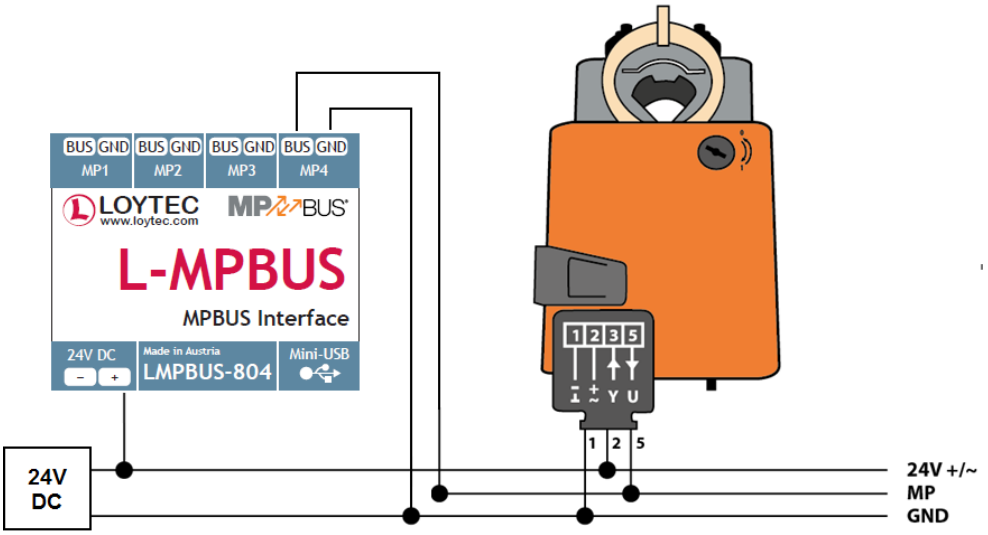


Figure 182: LMPBUS-804 interface with external bus power.

Depending on the LOYTEC device model, up to two LMPBUS-804 interfaces can be connected to the two built-in USB ports.

Important!	***The LMPBUS-804 interface can be operated on the built-in USB ports only. External USB hubs are not supported.***

12.3 Web Interface

12.3.1 Configuration

To enable the MP-Bus protocol on the dedicated MP-Bus port, use the port configuration Web interface. The settings for enabling the MP-Bus protocol are shown in Figure 183. Normally, a LOYTEC device comes with the MP-Bus port enabled as a default. The protocol information area shows communication speed and the MP-Bus mode.

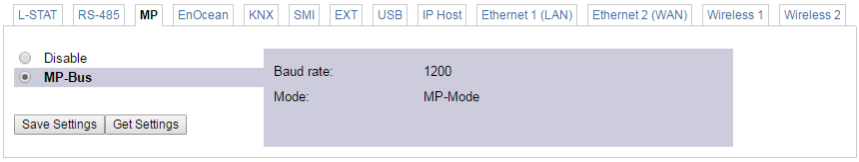


Figure 183: Enabling the MP-Bus protocol.

To enable the MP-Bus protocol on the USB port using the LMPBUS-804 interface, use the port configuration Web interface. The settings for enabling the MP-Bus protocol are shown in Figure 184. The protocol information area shows whether the LMPBUS-804 interface has been connected and provides some details on that interface such as the serial number.

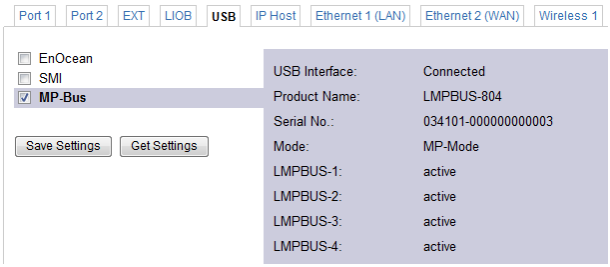


Figure 184: Enabling the MP-Bus protocol on the USB port.

12.3.2 Data Points

MP-Bus data points can be accessed through the Web UI as described in Section 3.3.1.

12.3.3 Auto-Commission in PP Mode

A data point configuration with only one MP-Bus device activates the PP mode on the LOYTEC device automatically. In this case the MP-Bus port is pre-enabled and the MP-Bus device is auto-commissioned after configuration download.

The **Commission** Web interface shows the operation status 'OK' and 'PP' as the point-to-point MP-Bus ID, the serial number of the connected device and the current position. There are no additional steps required to get the MP-Bus device online. An example is shown in Figure 185.

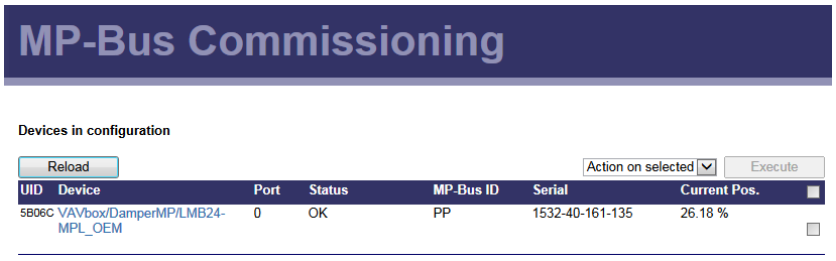


Figure 185: MP-Bus Commission Web interface in PP mode.

12.3.4 Commissioning in MP Mode

A data point configuration with more than one MP-Bus device activates the MP mode on the LOYTEC device. No auto-commission is possible in this mode. The **Commission** Web interface provides a page for managing and commissioning MP-Bus devices.

This page lists all MP-Bus devices, which have been created in the data point configuration as shown in Figure 186. The list shows device names as created in the configuration. The device **Status** can be one of the following:

- OK for a configured, online and working MP-Bus device,
- Offline: The device is configured for communication but appears offline,
- Uncommissioned for an unlinked MP-Bus device that needs assignment,
- Disabled for a temporarily disabled MP-Bus device.

The **MP-Bus ID** column shows the MP-Bus short addresses assigned to the devices. In the **Serial** number column, the serial numbers of the MP-Bus devices to be installed can be pre-configured. It can also be left empty, in which case the serial numbers of attached MP-Bus devices can be assigned by a button press method. For an online device the column **Current Pos** shows the current actuator position of the MP-Bus device.

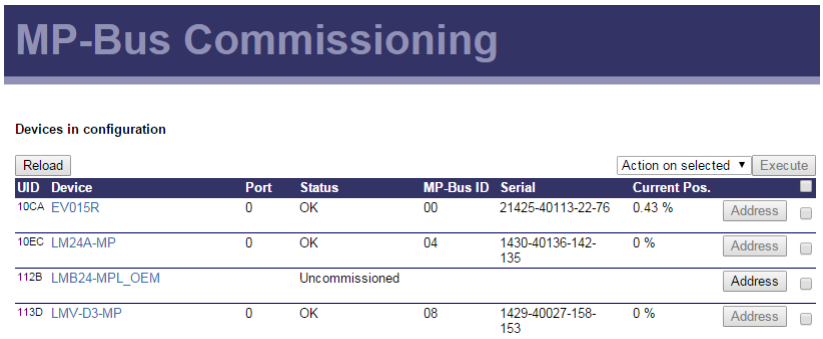


Figure 186: MP-Bus Commission Web interface in MP mode.

In order to execute an action on devices, select the checkbox at the end of the line. Then choose an action in the drop-down **Action on selected** and click on the **Execute** button. Actions that can be executed on all devices are enable, disable, decommission and replace.

The assignment of MP-Bus devices to uncommissioned devices in the configuration is typically done by scanning for attached devices. Select the port to be scanned in the **Scan options** drop-down list. If **Scan all** is selected, the scan will produce a list of devices attached to any of the available MP-Bus ports. Then select **Auto** scan mode. This scan shows all MP-Bus devices with an MP address in the list **Scanned devices not in configuration** as depicted in Figure 187. Devices that support PPX addressing are automatically assigned an MP address.

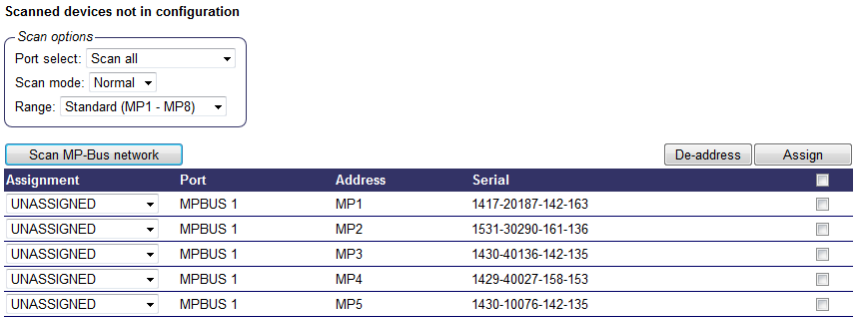


Figure 187: Result of the MP-Bus scan on the Web interface

To assign a scanned device to an uncommissioned device in the configuration, select the corresponding device name from the drop-down box in the **Assignment** column. Repeat that for all other devices and then click the button **Assign**.

If the MP-Bus scan does not show the expected MP-Bus devices, they may not have an MP address and have no PPX addressing capability. In this case there are the following ways to assign those MP-Bus devices:

- Manual assignment: The **Serial** number and **Port** are entered manually into the respective columns of an uncommissioned device. Once the serial number has been entered, the device is contacted and assigned the next available MP-Bus ID automatically.

- Button press: Click on the **Address** button. This activates the auto-address mode. Then press the button on the corresponding MP-Bus device. The serial number is then fetched and the port and MP-Bus ID are assigned automatically.

The scan also reveals any addressing conflicts of MP-Bus devices on the network. In this case the conflict is displayed and identifies the MP address causing the conflict (see Figure 188).

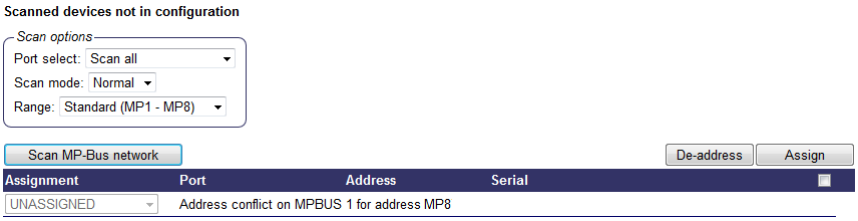


Figure 188: Address conflict after a normal MP-Bus scan

To resolve the conflict, identify the physical MP-Bus devices (they are not yet assigned). Then execute the serial number assignment workflow or the address button workflow as described above.

12.3.5 Statistics

Figure 189 shows a typical output of the statistics information which can be displayed for the MP-Bus port. The statistics can be cleared for the MP-Bus port by pressing the **Clear MP-Bus statistics** button. A refresh of the statistics is done automatically. To stop automatic update, deselect the **Live update** checkbox. For manual update press **Update MP-Bus statistics**.

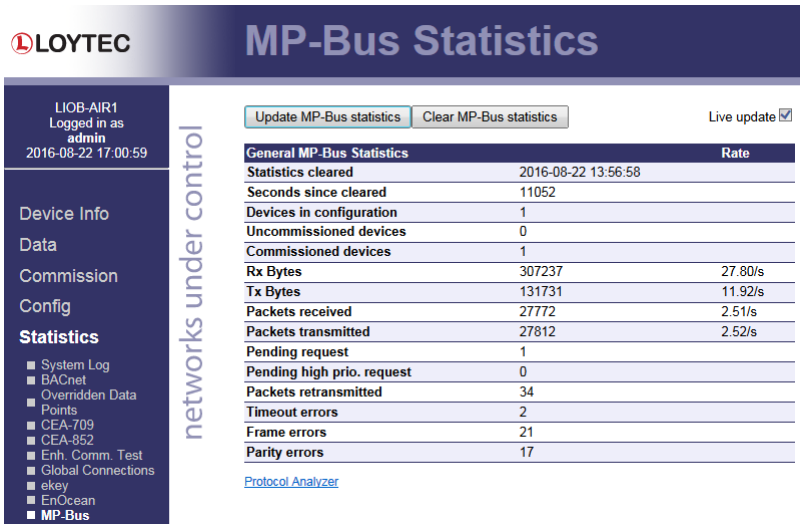


Figure 189: Statistics of the MP-Bus port.

The following information is available:

- Statistics cleared: last time of statistics reset,
- Devices in configuration: Total MP-Bus devices in data point configuration,
- Uncommissioned devices: Devices that need to be assigned,
- Commissioned devices: Devices that are fully assigned,
- Rx Bytes: number of bytes received,
- Tx Bytes: number of bytes sent,
- Packets received: number of MP-Bus packets received,
- Packets transmitted: number of MP-Bus packets transmitted,
- Pending request: Number of pending requests in the low-priority queue. Examples for low-priority requests are status requests.
- Pending high prio request: Number of pending requests in the high-priority queue. These requests are sent for time-critical information such as position set point data.

- Packets retransmitted: number of packets re-transmitted due to an error,
- Timeout errors: number of requests that timed out,
- Frame errors: number of packets with frame errors,
- Parity errors: number of packets with parity errors.

12.3.6 Protocol Analyzer

By activating the link **Protocol Analyzer** (available in the MP-Bus statistics page), the protocol analyzer page is shown as displayed in Figure 190.

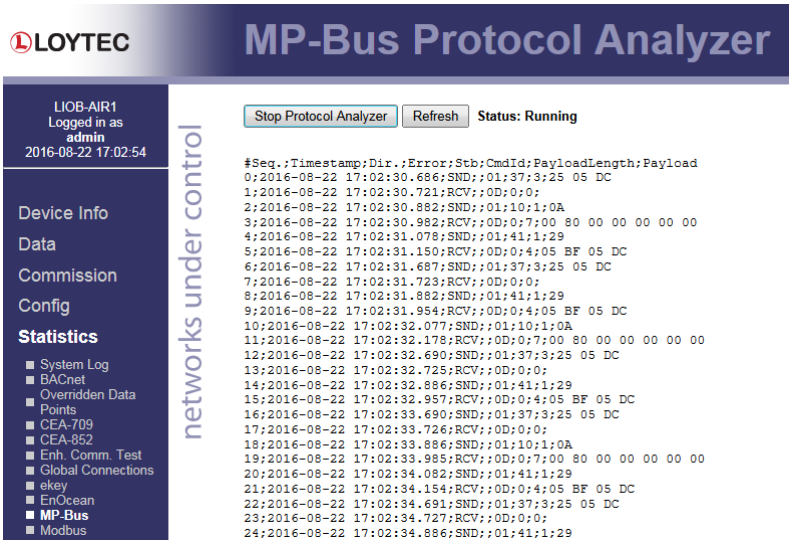


Figure 190: MP-Bus protocol analyzer.

Next to the button the status of the protocol analyzer is shown. If the analyzer is started, an automatic refresh is performed every 60 seconds. By pressing the button **Start Protocol Analyzer** / **Stop Protocol Analyzer** the protocol analyzer can be started / stopped.

For every frame sent or received a line is presented using comma separated values. The page refreshes automatically with a given interval. Press the **Refresh** button to get the latest updates immediately. When stopped click on **Save Log** to store the protocol log as a CSV file. **Clear Log** clears the log data.

13 OPC Client

13.1 Introduction

LOYTEC devices that support the OPC XML-DA standard as a client can integrate compatible OPC server implementations, for example L-INX or L-DALI devices or an LWEB-900 server running on a PC. The OPC tags of these OPC servers are added as data points to the device. An OPC server is represented by an OPC device in the OPC client. The OPC device address information consists of a URL to the Web service, including the IP address or hostname, port, username/password and secure service option.

The OPC client function in the Configurator can directly integrate OPC tags from other device configurations or import OPC tags lists. These tags lists can also be used to integrate third-party OPC servers. It is also possible, to assign OPC server URLs and username/password tokens later in the commission Web UI.

To support environments, where a single OPC client configuration shall be used on the local network (LAN) and from an external (public) network, a secondary address and port can be specified for an OPC device. This secondary address will be tried by the client in case the server is not reachable via the primary address. This can be used in NATed environments, where different addresses need to be used depending on the location of the client.

13.2 Web UI

13.2.1 Data Points

OPC client data points can be accessed through the Web UI as described in Section 3.3.1. The native info on the data point details page shows the effective tag path on the OPC server and the OPC server timestamp of the tag value.

13.2.2 Commissioning

The **Commission** Web interface provides a page for managing and commissioning OPC devices used by the OPC client technology. This page lists all OPC devices, which have been created in the data point configuration as shown in Figure 191. The list shows device names as created in the configuration. The device **Status** can be one of the following:

- Running for a working OPC device,
- Stopped if the OPC device communication is halted,
- Disabled if the OPC device has been disabled,
- Unreachable if the OPC device is commissioned but cannot be contacted at the moment,
- Auth Error if the user authentication failed on this OPC device,

- Uncommissioned for an OPC device that needs to be commissioned.

To commission an OPC device, enter the IP address of the OPC server (or the entire Web service URL) and the operator password. The default password is 'operator'. Then click on the save icon. The OPC device stats should change to Stopped and Running, if successful. Otherwise, the status goes to an error state.

Optionally, a **Replacement Path** can be entered. This relocates the tag path of an OPC device to another path. This option is only available, if the OPC tag list has been generated with a path offset. See Chapter „OPC Client" in the LINX Configurator User Manual [1].

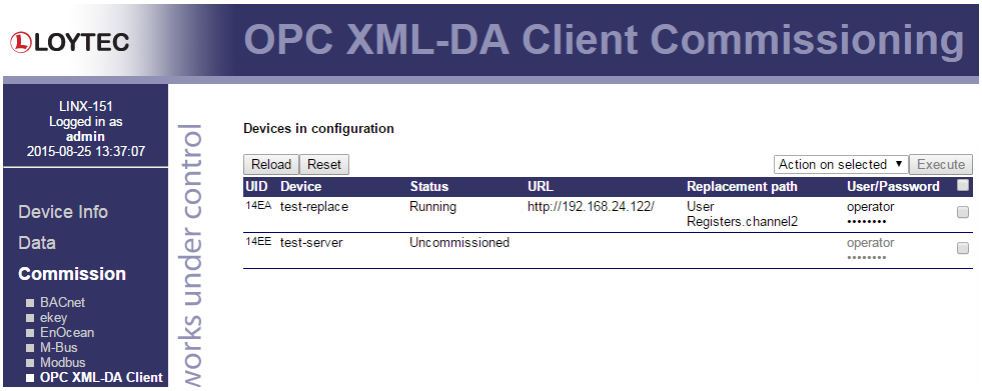


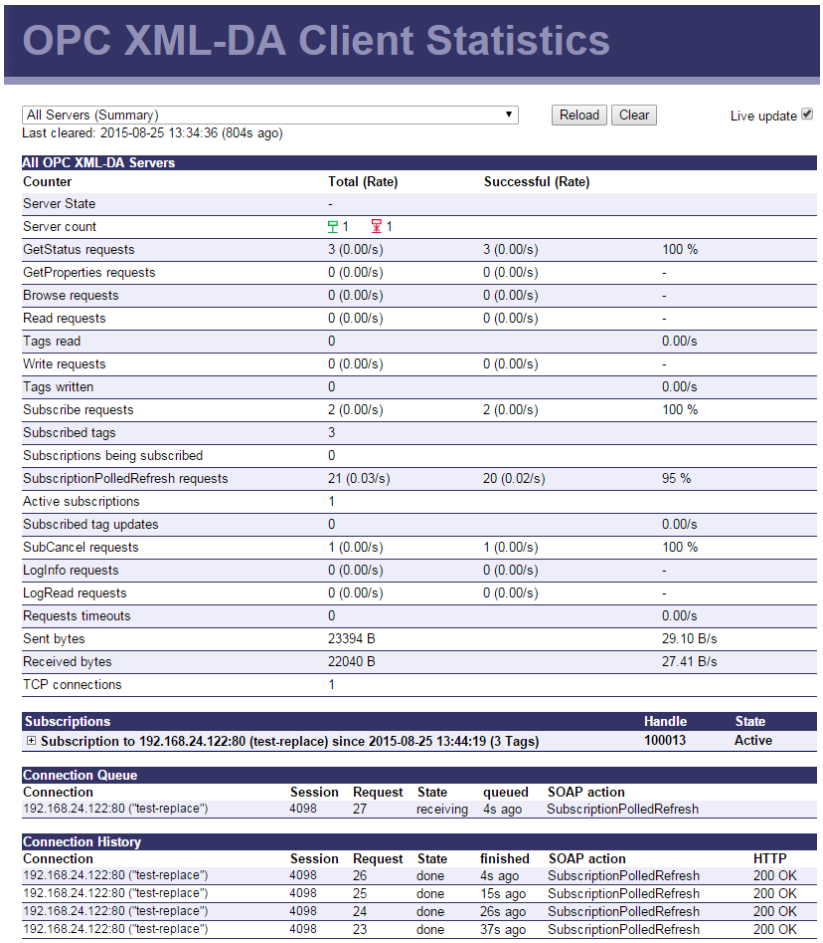
Figure 191: Commission OPC devices

To clear device assignments check one or more check boxes at the end of each line, choose the **Decommission** option in the **Action on selected** drop-down and click **Execute**. The selected devices will then be unassigned and appear as uncommissioned again. Devices can also be temporarily disabled. When disabled, no further data is processed from the respective devices until they are enabled again later.

13.2.3 Statistics

The OPC XML-DA Client Statistics page provides OPC client side communication statistics. For each OPC server defined in the project, there is a separate box of information regarding this server. At the top of this list is an additional box, showing a summary of all servers. An example of this page is shown in Figure 192.

Each box contains a list of statistic items, such as requests sent, OPC tags read or written, subscriptions made, the number of subscribed OPC tags, and so on. For each entry in this list, there are four columns. The first one describes the counted item, the second is the total count since the statistics were cleared the last time, and the last two columns show the number of successful operations, if applicable.



OPC XML-DA Client Statistics

All Servers (Summary) Reload Clear Live update

Last cleared: 2015-08-25 13:34:36 (804s ago)

All OPC XML-DA Servers

Counter	Total (Rate)	Successful (Rate)	
Server State	-		
Server count	1 1		
GetStatus requests	3 (0.00/s)	3 (0.00/s)	100 %
GetProperties requests	0 (0.00/s)	0 (0.00/s)	-
Browse requests	0 (0.00/s)	0 (0.00/s)	-
Read requests	0 (0.00/s)	0 (0.00/s)	-
Tags read	0		0.00/s
Write requests	0 (0.00/s)	0 (0.00/s)	-
Tags written	0		0.00/s
Subscribe requests	2 (0.00/s)	2 (0.00/s)	100 %
Subscribed tags	3		
Subscriptions being subscribed	0		
SubscriptionPolledRefresh requests	21 (0.03/s)	20 (0.02/s)	95 %
Active subscriptions	1		
Subscribed tag updates	0		0.00/s
SubCancel requests	1 (0.00/s)	1 (0.00/s)	100 %
LogInfo requests	0 (0.00/s)	0 (0.00/s)	-
LogRead requests	0 (0.00/s)	0 (0.00/s)	-
Requests timeouts	0		0.00/s
Sent bytes	23394 B		29.10 B/s
Received bytes	22040 B		27.41 B/s
TCP connections	1		

Subscriptions	Handle	State
⊞ Subscription to 192.168.24.122:80 (test-replace) since 2015-08-25 13:44:19 (3 Tags)	100013	Active

Connection Queue

Connection	Session	Request	State	queued	SOAP action
192.168.24.122:80 ("test-replace")	4098	27	receiving	4s ago	SubscriptionPolledRefresh

Connection History

Connection	Session	Request	State	finished	SOAP action	HTTP
192.168.24.122:80 ("test-replace")	4098	26	done	4s ago	SubscriptionPolledRefresh	200 OK
192.168.24.122:80 ("test-replace")	4098	25	done	15s ago	SubscriptionPolledRefresh	200 OK
192.168.24.122:80 ("test-replace")	4098	24	done	26s ago	SubscriptionPolledRefresh	200 OK
192.168.24.122:80 ("test-replace")	4098	23	done	37s ago	SubscriptionPolledRefresh	200 OK

Figure 192: OPC Client Statistics Page.

Below a **Subscriptions** list of all active subscriptions for the selected OPC server is shown. Each subscription can be expanded to list the subscribed OPC tags and their last updated values. The **Connection Queue** and **Connection History** shows the next queued request on active connections and the history of completed requests, respectively.

14 ekey

14.1 Introduction

The ekey function allows adding fingerprint readers to LOYTEC devices and building applications where access restrictions using biometric measures are required. ekey fingerprint readers must be purchased separately and can be attached to the RS-485 port. Up to 16 fingerprint readers are supported in a bus topology. Communication to reader devices on the RS-485 bus is encrypted.

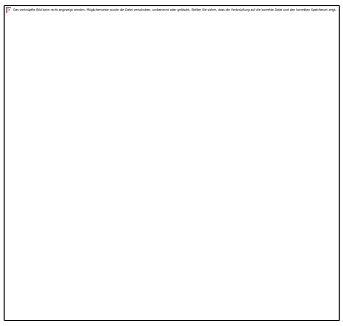


Figure 193: Example ekey fingerprint reader device

The reader devices are operated in active mode. In this mode each device is required to be polled in a timely fashion in order to be online. Reader devices indicate whether they are online as shown in Figure 193. The following color codes are in use:

- Blue permanent: The reader is online.
- Orange flashing: The reader is offline and cannot be contacted by the LOYTEC device.
- Orange permanent: The reader is waiting for a finger to be enrolled.
- Green flash on: A user has been authenticated.
- Red flash on: A user has been rejected.

The primary function of a fingerprint reader device it to authenticate a user, who has been enrolled for that device. One or more fingerprints can be used for the enrollment. The user is identified by a user string.

LOYTEC products that have the ekey function can be used for:

- Building access control using biometric measures (fingerprints),
- Creating users and enrolling fingerprints,
- Distributing users over several fingerprint sensors,

- Controlling data points each time a user is authenticated.

14.1.1 Supported ekey models

Table 7 lists the ekey models supported by LOYTEC devices.

Supported ekey model	Note
ekey module FS UP	
ekey module FS UP RFID REL	RFID not supported
ekey FSX UP E REL	
ekey FSX UP E RFID	
ekey FSX UP E RFID REL	
ekey FSX UP E	
ekey FSX IN	
ekey FSX IN RFID	
ekey FSX AP	
ekey FSX AP RFID	
ekey FSX AP REL	
ekey FSX AP RFID REL	
ekey FSX UP I	
ekey FSX UP I RFID	
ekey FSX UP I REL	
ekey FSX UP I RFID REL	

Table 7: Supported ekey models

14.2 Web UI

14.2.1 Data Points

The ekey data points can be accessed through the Web UI as described in Section 3.3.1.

14.2.2 Commissioning

The **Commission** Web interface provides a page for managing and commissioning ekey reader devices. It allows scanning for devices and assigning them to reader device instances in the data point configuration. An example is shown in Figure 194.

The **Devices in configuration** section lists the ekey reader instances found in the data point configuration. Each line allows editing the device settings and user configuration on that device by clicking the icons at the end of the line. Edit the device description below the device

name in the **Device** column. The **Status** column shows the reader state. It can be one of the following:

- OK for a working reader device,
- Uncommissioned for an unassigned reader device,
- Disabled for an ekey device that has been disabled,
- Offline for a reader that does not respond within 6 seconds,
- Busy for a reader with an ongoing data transfer,
- Encryption error for a reader that uses different encryption keys than the host device,
- Error if any other error occurred, e.g., the commissioning data has been corrupted.

The **Data** column shows enrolled users and fingers on the reader devices. **Encryption** is indicated if active.

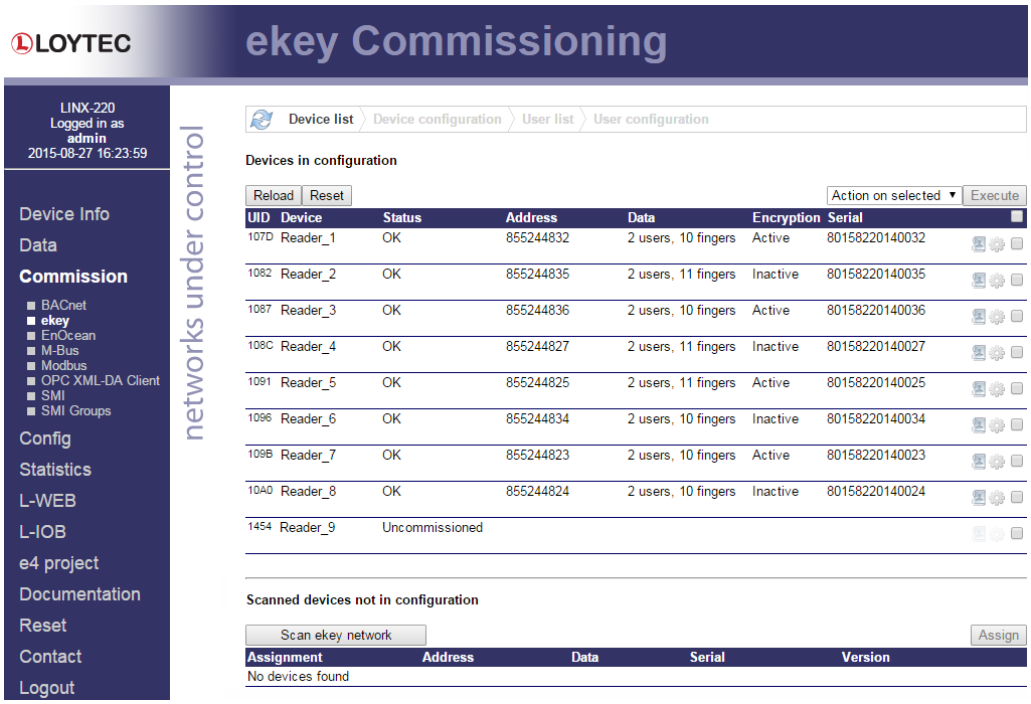


Figure 194: ekey Commissioning Web page.

To clear reader device assignments check one or more check boxes at the end of each line, choose the **Decommission** option in the **Action on selected** drop-down and click **Execute**. The selected devices will then be unassigned and appear as uncommissioned again. Devices can also be temporarily disabled. When disabled, no further data is processed from the respective devices until they are enabled again later.

By clicking the **Scan ekey network** button a device scan can be started. The scan searches for connected reader devices and puts them in the scanned devices list. For devices found that have not yet been assigned to devices in the data point configuration, the user can select a reader device in a drop-down box and click on the **Assign** button.

15 Bluetooth

15.1 Introduction

Bluetooth Low Energy is a technology for short range radio transmission of small data packages. It operates in the license-free ISM band between 2.402 and 2.480 GHz. It may interact and be disturbed by other technologies using this frequency range like WLAN or radio emitting sources like microwave-ovens.

Bluetooth Low Energy has been introduced in the Bluetooth 4.0 specification in 2010. By defining transmit and receive timeslots for a connection between two devices, the energy-consumption for radio-communication has been dramatically reduced since the radio has to be turned on only during these slots. While the Generic Access Profile (GAP) controls connections and advertising in Bluetooth, the Generic Attribute Profile (GATT) defines the way how BLE-devices transfer data back and forth by services and characteristics.

Bluetooth Low Energy enables several features, the most important ones are mentioned here:

- Beaconing: advertising of Bluetooth beacons that can be used as identifiers
- Connections: services are used to provide device specific data
- Asset Tracking: scanning for available Bluetooth beacons and determine a location based on the RSSI

Nevertheless BLE is still a point-to-point (connection) or point-to-mulipoint (broadcast) communication.

15.1.1 Bluetooth Mesh Basics

In 2017 the Bluetooth SIG introduced Bluetooth Mesh on top of the Bluetooth 4.2 specification. It allows many-to-many connections by using advertising channels only and introducing a forwarding-mechanism (relay-function) and a publish/subscribe method for data exchange.

LOYTEC controllers support Bluetooth SIG qualified mesh only.

Note:	***No support for proprietary bluetooth mesh solutions (e.g. Casambi, Wirepas, CSRmesh, Mindtree, MeshTek, Estimote etc.)***

The basic concepts to allow multipoint-to-multipoint communication in BLE-based systems are simple:

- Use **advertising channels 37, 38 & 39** only (any device can listen). A further advantage of these channels is that they do not interfere with WLAN-signals.

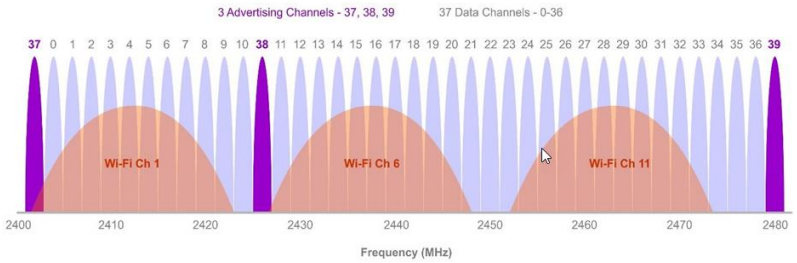


Figure 195: BLE Channels.

- **Managed Flooding** approach, which means that any message in the network can be forwarded multiple times (defined by the TTL-parameter). The target device is subscribed to the target address. Most important methods and parameters:
  - TTL (Time To Live, Number of Hops),
  - Message Cache (Withdraw messages, that have already been received)
  - Publish/Subscribe (Process only messages you are subscribed to)

- Each node (device in the mesh network) comes with a set of the following device capabilities and features, none of them is mandatory, but finally all will be required in different situations:
  - **Relay Feature**: capability of forwarding mesh-messages based on network key and TTL
  - **Proxy Feature**: service to access the mesh-network via a GATT-connection, typically via a mobile device
  - **Low Power Feature**: required for battery powered devices, so that they can be inactive most of the time to save energy
  - **Friend Feature**: required for support of devices with low power feature. A friend has the capability to store configuration commands for a low power device when it is in sleep mode

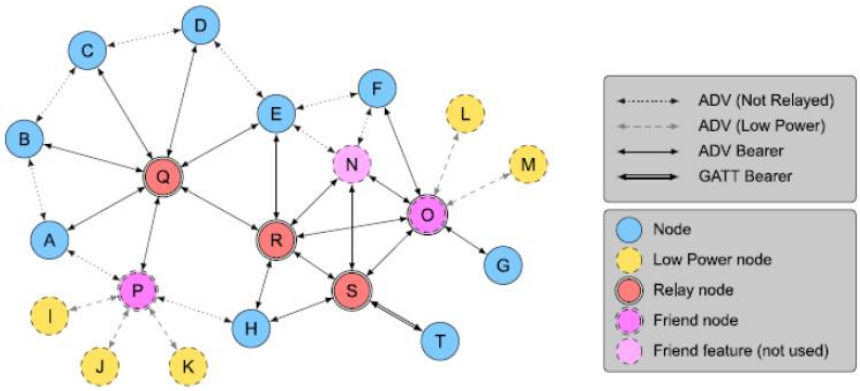


Figure 196: Bluetooth Mesh ecosystem with all features.

- **Security is mandatory** in bluetooth mesh and is provided by the following methods:
  - multi-level encryption (network key, application key, device key)
  - key refresh procedure
  - replay protection (IV index, sequence)
  - trashcan protection (node blacklisting)
  - authentication during provisioning (out of band)

- The **application** in Bluetooth mesh ecosystems is built on so called **models**. Each model describes a set of features represented by states and interacted with a defined command set. There are mandatory models (so called foundation models, which are used to setup the mesh and the basic functions) and optional application specific models (some generic, sensors or lighting specific) and vendor models.

For a more detailed description on Bluetooth mesh operation and models refer to Bluetooth SIG Mesh Profile v 1.0.1 and Mesh Model v1.0.1 specifications.

15.1.2 Bluetooth Mesh Network Limitations

There are several limitations in a bluetooth mesh network that have to be considered:

- Maximum number of nodes in a network is limited by the maximum number of elements which is 16384.
- Maximum number of group addresses is 16384 (of which 4096 are reserved)
- Forwarding is limited by TTL-parameter (Time To Live), the theoretical maximum is 126 hops
- The size of message cache effects the efficiency of relaying (suppression of circular relaying)
- Sequence Number & IV–index are not a limitation per se, but can result in unprovisioned devices (after a device has been offline for more than 48 weeks the it can happen that the values cannot be recovered anymore)
- Length of Subscription List – this parameter limits the number of addresses a device can listen to (or groups a device can be a member of)
- The CRPL parameter defines the length of the list of element addresses which are processed by a device (thus the parameter limits the number of nodes a device can interact with)
- The latency in a bluetooth mesh network is heavily depending on mesh size and payload as well as on message size (segmented and unsegmented messages)
- Turning unprovisioned mesh beacons into a node by a provisioning process requires a direct connection and is limiting the range between provisioner and mesh device

15.1.3 Bluetooth on LOYTEC controller

LOYTEC products support the Bluetooth standard (5.1 or higher) as well as Bluetooth Mesh and provide the following features based on these technologies:

- Bluetooth based features:
    - Beaconing: advertising of Bluetooth beacons that can be used as identifiers or for location services.
    - Asset Tracking: scanning for available Bluetooth beacons and determine a location based on the RSSI.
- Features for operating Bluetooth Mesh networks:
    - Comissioning Web-UI: Scan for devices and Add devices to or Remove devices from a Bluetooth-Mesh network.
    - Commissioning Web-UI for signal strength and basic function test.
    - Easy device replacement on the Comissioning Web UI.
    - Configurable through device templates using the Configurator software.

- Friend Feature to support Low Power Nodes.
- Integration of EnOcean Based Bluetooth Button Modules (PTM215B) in a Bluetooth Mesh Ecosystem.
- Protocol Analyzer for Decoded Messages of Mesh Application.

Additional Bluetooth Mesh related limitations in a LOYTEC system:

- Maximum Number of Nodes in a network: 16384 elements, a LOYTEC mesh network allows to add up to 100 nodes, which implicitly limits the number of elements.
- Dynamic Grouping – maximum number of groups: 16384 (of which 4096 are reserved).
- Low Power Device – responsiveness is limited to defined intervals.
- Provisioning is limited by the range of a direct connection, with the help of remote provisioning methods and devices supporting those the range can be extended (e.g. LOYBT-CALIB1).

15.1.3.1 Bluetooth Based Functions

A LOYTEC Controller with Bluetooth support can scan for beacons in its radio range. A maximum of 100 active beacons (Eddystone UID+TLM or iBeacon) can be managed by the device. A license LIC-ASSET is required to activate this function.

The asset data of a sensor is available on data point level. There is a data point *AssetCount* representing the number of active assets nearby the scanning device[2] and the *AssetData* data point. For more details about the datapoints refer to 16.3.5.

[2] The controller separates in near and far assets based on the strength of the radio signal (RSSI-limit is -75dBm)

15.2 Bluetooth Mesh Device Types

This chapter deals with the datapoint representations for different types of devices. The datapoint structure is type dependent, but provides support for several optional functions of a device type (e.g. color control). As a result not all datapoints provided by the templates are useful for every single application, in practice only a subset of the datapoints will be used.

15.2.1 Templates for Bluetooth Generic Devices

Device templates for generic bluetooth devices are available for the following types:

- Lamp.btmesh – for bluetooth mesh lamps (real and virtual)
- LOYBT-MSx.btmesh – for bluetooth sensors for occupancy, illuminance, temperature, humidity; additionally Bluetooth-mesh to DALI gateway is supported (e.g. for D4i luminaires).
- LOYBT-TEMPx.btmesh - 1 static instance, others optional
- BluetoothSwitch.btmesh – for integration of EnOcean based Bluetooth switches (PTM215B)
- Network.btmesh -> 1 static instance only

15.2.1.1 Template for BT-Mesh Lamps

Figure 197 shows the datapoints of the template for bluetooth mesh lamp actuator.

ROOT › Bluetooth › Lamp

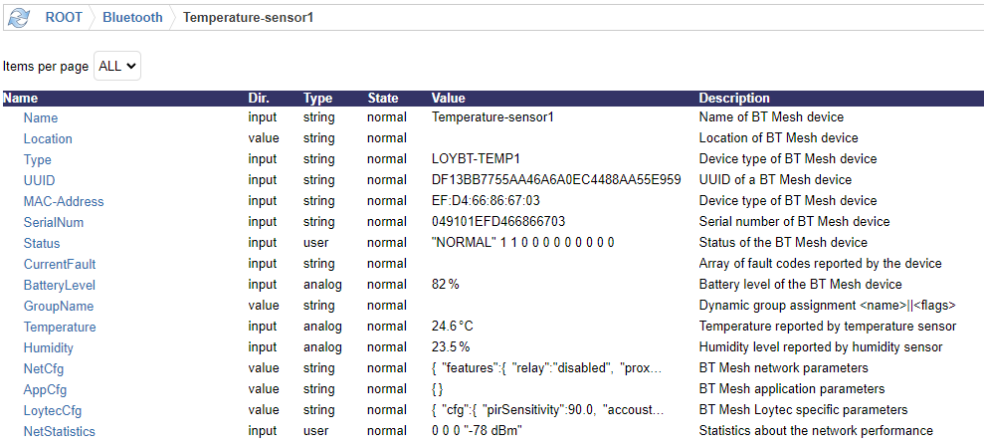
Items per page ALL

Name	Dir.	Type	State	Value	Description
Name	input	string	normal	Lamp	Name of BT Mesh device
Location	value	string	normal		Location of BT Mesh device
Type	input	string	normal	OSRAM OTi QBM NFC S	Device type of BT Mesh device
UUID	input	string	normal	A5C67FB3B6BB0F3D04BB48FFAE8A282E	UUID of a BT Mesh device
MAC-Address	input	string	normal	C7:24:DD:7E:E8:F9	Device type of BT Mesh device
SerialNum	input	string	invalid value	--	Serial number of BT Mesh device
DimLevel	output	analog	normal	50 %	Set a new target dim level for a lamp
DimLevelFb	input	analog	normal	50 %	Feedback of the dim level for a lamp
ColorTemperature	output	analog	invalid value	-- K	Set a new target temperature value for a lamp
ColorTemperatureFb	input	analog	invalid value	-- K	Feedback of the temperature value for a lamp
⊞ ColorHSL	output	user	invalid value	--	Set new target Hue and Saturation values for a lamp
⊞ ColorHSLFb	input	user	invalid value	--	Feedback of Hue and Saturation values for a lamp
⊞ ColorXY	output	user	invalid value	--	Set new target x and y values for a lamp
⊞ ColorXYFb	input	user	invalid value	--	Feedback of x and y values for a lamp
FadeTime	value	analog	normal	1 s	Transition time for a dim level command
FadeRate	value	analog	normal	10 %/s	Transition rate for UP and DOWN commands
MaxLevel	value	analog	normal	100 %	Maximum dim level for device
MinLevel	value	analog	normal	0 %	Minimum dim level for device
DefaultLevel	value	analog	normal	10 %	Default dim level for device
PowerUpBehavior	value	multistate	normal	Restore (2)	Behavior of the lamp after power up
Command	output	multistate	normal	NO_COMMAND (1)	Data point for issuing commands to the lamp
Status	input	user	normal	"ERROR" 1 1 0 0 0 0 0 0 0 1 0	Status of the BT Mesh device
CurrentFault	input	string	normal	[0x82]	Array of fault codes reported by the device
BatteryLevel	input	analog	normal	100 %	Battery level of the BT Mesh device
NominalPower	value	analog	normal	20 W	Nominal power of the lamp
Energy	input	analog	normal	8.61111e-06 kWh	Energy consumption of the lamp based on nominal power
RunHours	input	analog	normal	0.0097222 h	Time for which lamp has been turned on
GroupName	value	string	normal		Dynamic group assignment <name>||<flags>
NetCfg	value	string	normal	{ "features":{ "relay":"enabled", "prox...	BT Mesh network parameters
AppCfg	value	string	normal	{ "defaultTransitionTime":1.0, "power...	BT Mesh application parameters
LoytecCfg	value	string	normal	{}	BT Mesh Loytec specific parameters
NetStatistics	input	user	normal	0 0 0 "-62 dBm"	Statistics about the network performance

Figure 197: Datapoints Lamp.btmesh template.

15.2.1.2 Template for BT-Mesh Temperature-Sensors

Figure 198 shows the datapoints of the template for bluetooth mesh temperature sensor.


ROOT › Bluetooth › Temperature-sensor1

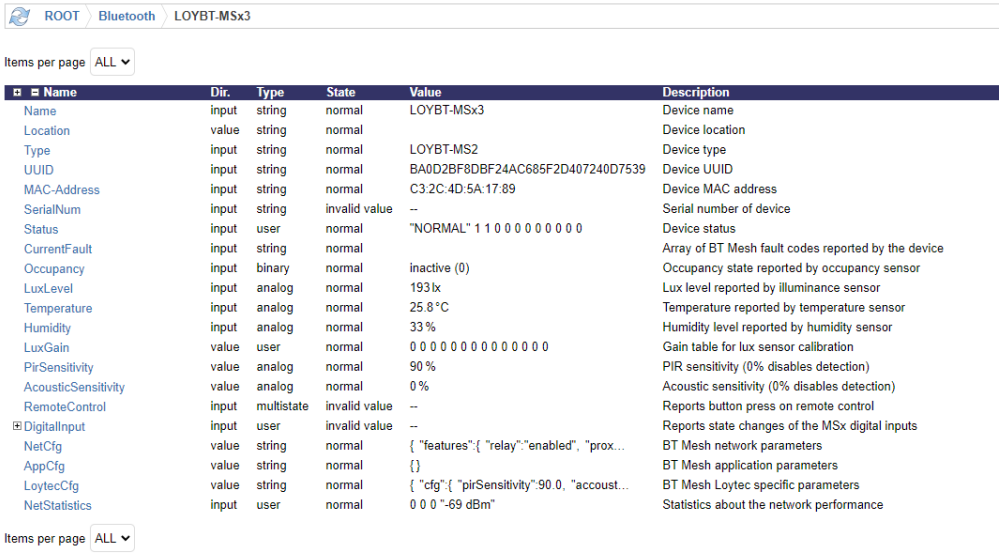
Items per page ALL

Name	Dir.	Type	State	Value	Description
Name	input	string	normal	Temperature-sensor1	Name of BT Mesh device
Location	value	string	normal		Location of BT Mesh device
Type	input	string	normal	LOYBT-TEMP1	Device type of BT Mesh device
UUID	input	string	normal	DF13BB7755AA46A6A0EC4488AA55E959	UUID of a BT Mesh device
MAC-Address	input	string	normal	EF:D4:66:86:67:03	Device type of BT Mesh device
SerialNum	input	string	normal	049101EFD466866703	Serial number of BT Mesh device
Status	input	user	normal	"NORMAL" 1 1 0 0 0 0 0 0 0 0 0 0	Status of the BT Mesh device
CurrentFault	input	string	normal		Array of fault codes reported by the device
BatteryLevel	input	analog	normal	82 %	Battery level of the BT Mesh device
GroupName	value	string	normal		Dynamic group assignment <name>||<flags>
Temperature	input	analog	normal	24.6 °C	Temperature reported by temperature sensor
Humidity	input	analog	normal	23.5 %	Humidity level reported by humidity sensor
NetCfg	value	string	normal	{ "features":{ "relay":"disabled", "prox...	BT Mesh network parameters
AppCfg	value	string	normal	{}	BT Mesh application parameters
LoytecCfg	value	string	normal	{ "cfg":{ "pirSensitivity":90.0, "accoust...	BT Mesh Loytec specific parameters
NetStatistics	input	user	normal	0 0 0 "-78 dBm"	Statistics about the network performance

Figure 198: Datapoints LOYBT-TEMPx.btmesh template.

15.2.1.3 Template for BT-Mesh Multisensors

Figure 199 shows the datapoints of the template for bluetooth mesh multisensor.


ROOT › Bluetooth › LOYBT-MSx3

Items per page ALL

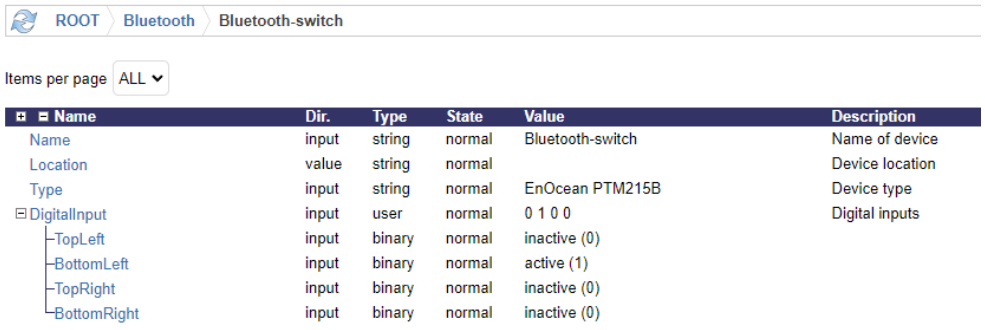
Name	Dir.	Type	State	Value	Description
Name	input	string	normal	LOYBT-MSx3	Device name
Location	value	string	normal		Device location
Type	input	string	normal	LOYBT-MS2	Device type
UUID	input	string	normal	BA0D2BF8DBF24AC685F2D407240D7539	Device UUID
MAC-Address	input	string	normal	C3:2C:4D:5A:17:89	Device MAC address
SerialNum	input	string	invalid value	--	Serial number of device
Status	input	user	normal	"NORMAL" 1 1 0 0 0 0 0 0 0 0 0 0	Device status
CurrentFault	input	string	normal		Array of BT Mesh fault codes reported by the device
Occupancy	input	binary	normal	inactive (0)	Occupancy state reported by occupancy sensor
LuxLevel	input	analog	normal	193 lx	Lux level reported by illuminance sensor
Temperature	input	analog	normal	25.8 °C	Temperature reported by temperature sensor
Humidity	input	analog	normal	33 %	Humidity level reported by humidity sensor
LuxGain	value	user	normal	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Gain table for lux sensor calibration
PirSensitivity	value	analog	normal	90 %	PIR sensitivity (0% disables detection)
AcousticSensitivity	value	analog	normal	0 %	Acoustic sensitivity (0% disables detection)
RemoteControl	input	multistate	invalid value	--	Reports button press on remote control
⊞ DigitalInput	input	user	invalid value	--	Reports state changes of the MSx digital inputs
NetCfg	value	string	normal	{ "features":{ "relay":"enabled", "prox...	BT Mesh network parameters
AppCfg	value	string	normal	{}	BT Mesh application parameters
LoytecCfg	value	string	normal	{ "cfg":{ "pirSensitivity":90.0, "accoust...	BT Mesh Loytec specific parameters
NetStatistics	input	user	normal	0 0 0 "-69 dBm"	Statistics about the network performance

Items per page ALL

Figure 199: Datapoints LOYBT-MSx.btmesh template.

15.2.1.4 Template for EnOcean Bluetooth Switch

Figure 200 shows the datapoints of the template for an EnOcean Bluetooth switch based on the PTM215B module.


ROOT › Bluetooth › Bluetooth-switch

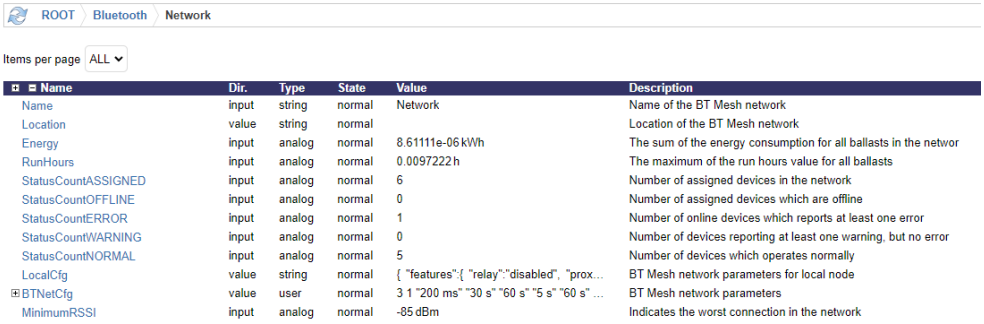
Items per page ALL

Name	Dir.	Type	State	Value	Description
Name	input	string	normal	Bluetooth-switch	Name of device
Location	value	string	normal		Device location
Type	input	string	normal	EnOcean PTM215B	Device type
⊟ DigitalInput	input	user	normal	0 1 0 0	Digital inputs
TopLeft	input	binary	normal	inactive (0)	
BottomLeft	input	binary	normal	active (1)	
TopRight	input	binary	normal	inactive (0)	
BottomRight	input	binary	normal	inactive (0)	

Figure 200: Datapoints BluetoothSwitch.btmesh template.

15.2.1.5 Template for the BT-Mesh Network

Figure 201 shows the datapoints of the template for bluetooth mesh network actuator.



Name	Dir.	Type	State	Value	Description
Name	input	string	normal	Network	Name of the BT Mesh network
Location	value	string	normal		Location of the BT Mesh network
Energy	input	analog	normal	8.61111e-06 kWh	The sum of the energy consumption for all ballasts in the networ
RunHours	input	analog	normal	0.0097222 h	The maximum of the run hours value for all ballasts
StatusCountASSIGNED	input	analog	normal	6	Number of assigned devices in the network
StatusCountOFFLINE	input	analog	normal	0	Number of assigned devices which are offline
StatusCountERROR	input	analog	normal	1	Number of online devices which reports at least one error
StatusCountWARNING	input	analog	normal	0	Number of devices reporting at least one warning, but no error
StatusCountNORMAL	input	analog	normal	5	Number of devices which operates normally
LocalCfg	value	string	normal	{ "features":{ "relay":"disabled", "prox...	BT Mesh network parameters for local node
⊞ BTNetCfg	value	user	normal	3 1 "200 ms" "30 s" "60 s" "5 s" "60 s" ...	BT Mesh network parameters
MinimumRSSI	input	analog	normal	-85 dBm	Indicates the worst connection in the network

Figure 201: Datapoints Network.btmesh template.

15.2.2 Datapoint Description

Object Name Suffix	Object Type	Lamp	Sensor	Temp	PTM215B	Network	Description
Name	String	✓	✓	✓	✓	✓	Name of the device
Location	String	✓	✓	✓	✓	✓	Location of the device
Type	String	✓	✓	✓	✓		Device type of the device (delivered in scan response)
UUID	String	✓	✓	✓			UUID of the device (128bit)
MAC-Address	String	✓	✓	✓			MAC-address of the device (6 Byte)
SerialNum	String	✓	✓	✓			Serial number of the device
DimLevel	Analog	✓					Set new target dim level for a lamp in %
DimLevelFb	Analog	✓					Feedback of the dim level for a lamp in %
ColorTemperature	Analog	✓					Set new target color temperature for a lamp in K
ColorTemperatureFb	Analog	✓					Feedback of the color temperature for a lamp in K
ColorHSL	User	✓					Set new target value of Hue in ° and Saturation in % for a lamp
ColorHSLFb	User	✓					Feedback of Hue in ° and Saturation in % for a lamp
ColorXY	User	✓					Set new targer for X and Y for a lamp
ColorXYFb	User	✓					Feedback of X and Y for a lamp
FadeTime	Analog	✓					Transition time for a dim level or color command (Default transition time)
FadeRate	Analog	✓					Transition Rate for UP and DOWN commands
MaxLevel	Analog	✓					Maximum dim level for device
MinLevel	Analog	✓					Minimum dim level for device
DefaultLevel	Analog	✓					Default dim level for device
PowerUpBehavior	Multistate	✓					Behavior of the lamp after power up (Off / Restore / Default)

Object Name Suffix	Object Type	Lamp	Sensor	Temp	PTM215B	Network	Description
Command	Multistate	✓					Command to control a device: • NO COMMAND • RECALL SCENE 1-25 • STORE SCENE 1-25 • DELETE SCENE 1-25 • RESET RUN HOURS • RESET ENERGY COUNT • UP • DOWN • COOLER • WARMER • STOP
Status	User	✓	✓	✓			Status Reported by the device: • Status: UNASSIGNED, OFFLINE, ERROR, WARNING, NORMAL • Present • StatusValid • ComFailure • LampFailure • BallastFailure • ThermalOverload • BatteryWarningOrError • SupplyVoltageWarningOrError • InternalBusWarningOrError • OtherWarningOrError • DynGrpSlave
CurrentFault	String	✓	✓	✓			Array of Fault codes reported by the device
BatteryLevel	Analog	✓		✓			Battery level of the device
NominalPower	Analog	✓					Nominal power of the lamp
Energy	Analog	✓				✓	Energy consumption of the lamp based on nominal power
RunHours	Analog	✓				✓	Lamp total On-Time
GroupName	String	✓		✓			Dynamic group assignment “<name>||<flag>”
NetCfg	String	✓	✓	✓			BT-mesh network parameters
AppCfg	String	✓	✓	✓			BT-mesh application paramters
LoytecCfg	String	✓	✓	✓			BT-mesh Loytec specific parameters (vendor models)
NetStatistics	User	✓	✓	✓			Statistic about network performance using Heartbeat
Occupancy	Binary		✓				Occupancy state reported by occupancy sensor
LuxLevel	Analog		✓				Lux level reported by illuminance sensor
LuxGain	User		✓				Gaintable for light sensor calibration
Temperature	Analog		✓	✓			Temperature reported by temperature sensor

Object Name Suffix	Object Type	Lamp	Sensor	Temp	PTM215B	Network	Description
Humidity	Analog		✓	✓			Humidity level reported by humidity sensor
Remote Control	MultiState		✓				Reports button pressed/released from L-RC1 remote control
DigitalInput	User		✓	✓			State of digital input
PirSensitivity	Analog		✓				PIR sensitivity (0% disables detection)
AcousticSensitivity	Analog		✓				Acoustic sensitivity (0% disables detection)
StatusCountASSIGNED	Analog					✓	Number of Assigned devices in the network
StatusCountOFFLINE	Analog					✓	Number of Assigned devices which are offline
StatusCountERROR	Analog					✓	Number of Online devices which report at least one error
StatusCountWARNING	Analog					✓	Number of Online device which report at least one warning, but no error
StatusCountNORMAL	Analog					✓	Number of deices which operate normal
LocalCfg	String					✓	Network parameters for the local node
BTNetCfg	User					✓	Common network parameters
MinimumRSSI	Analog					✓	Indicated the worst connection in the network

15.2.3 LOYTEC Controller with Bluetooth interface

The LPAD-7 comes with a Bluetooth Low Energy interface. The interface can be enabled/disabled in the Bluetooth tab of the Port Configuration via the WebUI of the device (see Figure 202, which also shows the recommended default settings for the mesh network). This tab also allows to export the key-file (network, application and device keys).

Note: ***For asset tracking "Bluetooth Mesh" has to be activated in the port config as well.***

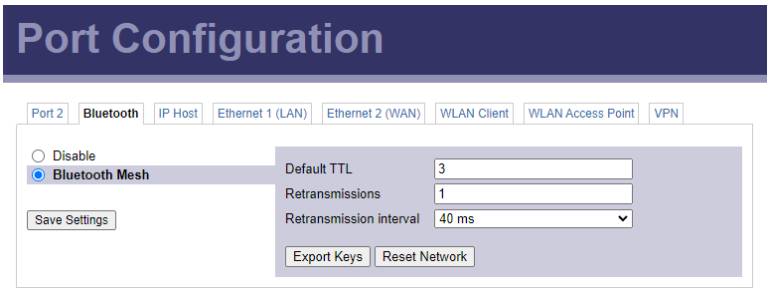


Figure 202: Port Configuration – Bluetooth Tab.

The LPAD-7 is intended to act as provisioner in a LOYTEC environment, i.e. the device is used to setup the bluetooth mesh ecoysystem (see Section 15.3.2). For interaction with physical bluetooth devices each device which has been added to the mesh must be assigned to a datapoint structure based on a bluetooth generic device template.

Based on the datapoints used in the generic device templates the LPAD-7 represents the client part for serveral models (generic, sensor, lighting). Furthermore it provides network-statistics, protocol-analyzer and also support the integration of EnOcean Bluetooth switches based on the PTM215B (see Web UI descritpion in Section 15.3).

15.2.4 LOYTEC bluetooth mesh system overview

A LOYBT bluetooth mesh system allows the integration of native Bluetooth mesh lamps and sensors. In addition the LOYBT-MSx can also act as gateway to a DALI-subsystem. The DALI-lamps are exposed to the Bluetooth ecosystem and can be individually controlled.

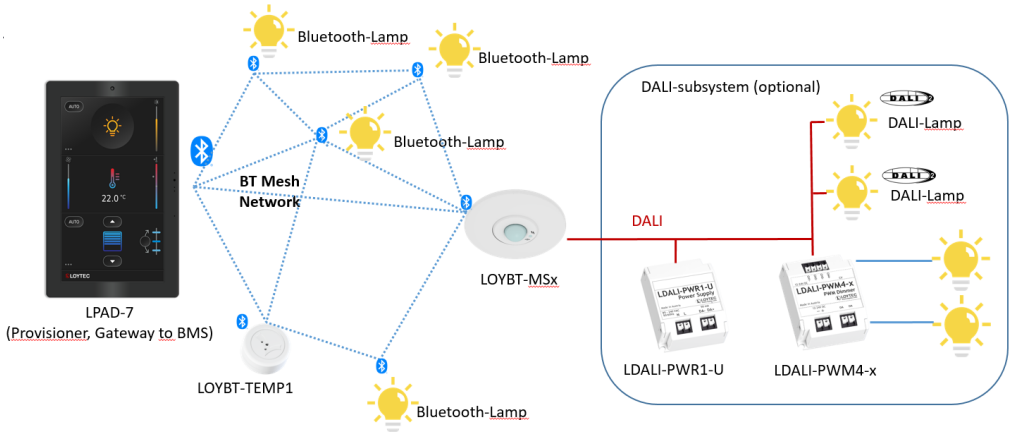


Figure 203: LOYBT Bluetooth mesh ecosystem with DALI-subsystem

15.3 Web UI

15.3.1 Data Points

The datapoints can be accessed through the Web UI as described in Section 3.3.1.

15.3.2 Commissioning

The **Commission** Web interface provides a page for managing and commissioning bluetooth mesh devices. It allows scanning for devices and assigning them to bluetooth mesh device instances in the data point configuration. An example is shown in Figure 207.

To use a LOYBT-TEMP1 for system registers *Room Temp* and *Humidity*, the lower power node has to be assigned to the static *Temperature-sensor* device. A proper scan process can be initiated by pressing the **Add**-Button on the top of the Bluetooth Mesh Comissioning page (see Figure 204) followed by to the assignment procedure with the help of an assignment wizard (see also Section 15.3.2.1). After device assignement the sensor values are visible (Figure 205) and are automatically used for system registers *Room Temp* and *Humidity* instead of the internal sensors.



Figure 204: Assign a LOYBT-TEMP1 to be used for values in system registers.



Figure 205: Assigned LOYBT-TEMP1 used for values in system registers.

The device can be simply removed by pressing the “Remove”-button and following the instruction in the upcoming wizard.

The **Devices in Datapoint Configuration** section lists the bluetooth mesh device instances found in the datapoint configuration. Each entry provides access to the corresponding datapoints and information about already assigned physical bluetooth mesh devices. Furthermore it gives access to settings and options and user configuration of that device. Left

to the Device Column the WebUI offers several actions (Wink, On, Off) for the corresponding device. The checkboxes at the very left combined with the **Action on Selected** menu and **Execute** button on top allows muliselect for the following actions:

- On
- Off
- Unassign
- Update Firmware

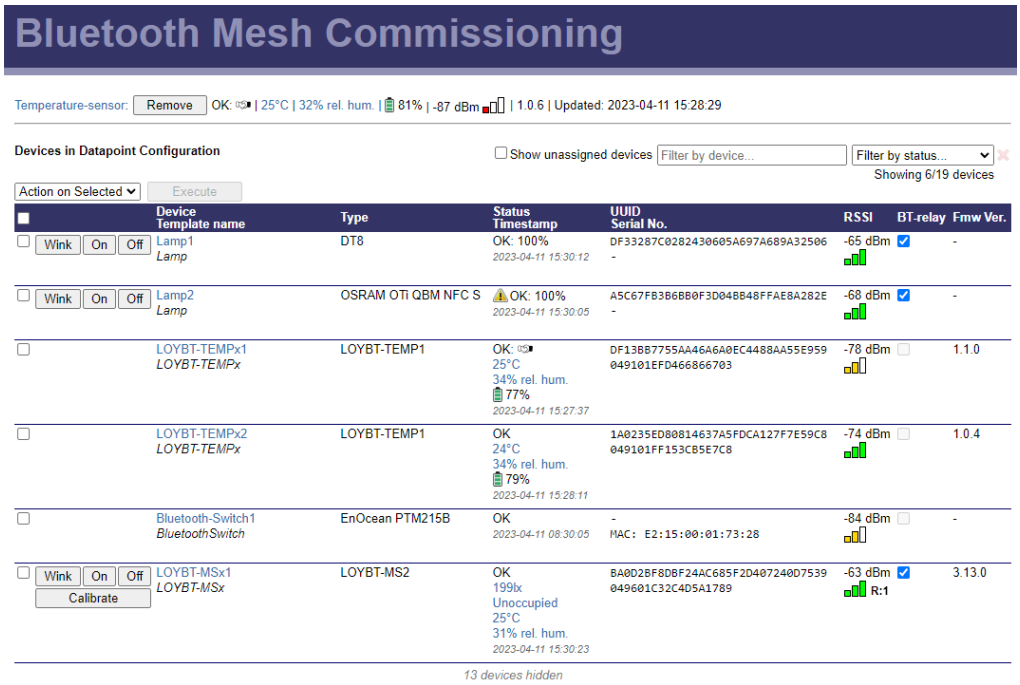


Figure 206: Assigned Bluetooth Devices.

The **Device** column shows the name of the instance, the template name and the location, the location can be edited directly on the device entry on the commissioning web-ui.

The **Type** column shows the device type reported in the scan response of the device, if the type is not provided by the physical device the name property of the object is shown.

The **Status** column shows the device state and additional values like dimlevel for lamps or measurement values for sensors and the timestamp of the last update. The status is always one of the following:

- **OK** for working device, including additional infos like dim value or sensor values
- **Unassigned** if no physical device has been assigned
- **Error** reported by the device, see also datapoint *CurrentFault*
- **Offline** in case of failed communication with device
- **Warning Symbol** in addition to OK indicated that there is a manufacturer specific error or warning of the device (meaning to be checked with device manufacturer), see also datapoint *CurrentFault*
- Friendship established – indicates the friendship state of the LOYBT-TEMP1.

The **UUID/Serial No.** column shows unique identifiers of the device. These are the UUID provided by a physical device in the unprovisioned beacon and the serial number. The serial number …

The **RSSI** column provided the information about the last RSSI of this device received by the controller. In addition a small graphical symbol indicated the signal strength and the information if the last message has been relayed (including the number of hops), indicated by “R:” and the number of hops.

RSSI > -75dBm

-75dBm >= RSSI > -85dBm

-85dBM >= RSSI

Note: ***In a mesh network a message received by the controller must not necessarily have been emitted by the message originator, but may instead have been forwarded by a node with relay functionality. The RSSI-value only represents the signal strength seen by the controller, it does not provide complete info in case of forwarded frames.***

The **BT-relay** column allows activation/deactivation the message forwarding of mesh-nodes.

The **Fmw Ver.** column indicates the firmware version of the device.

To remove devices from the configuration check one or more check boxes at the beginning of each line, choose the **Unassign** option in the **Action on selected** drop-down and click **Execute**. The selected devices will then be unassigned and appear in the Scanned devices list. Additional actions are **On**, **Off** and **Update Firmware**.

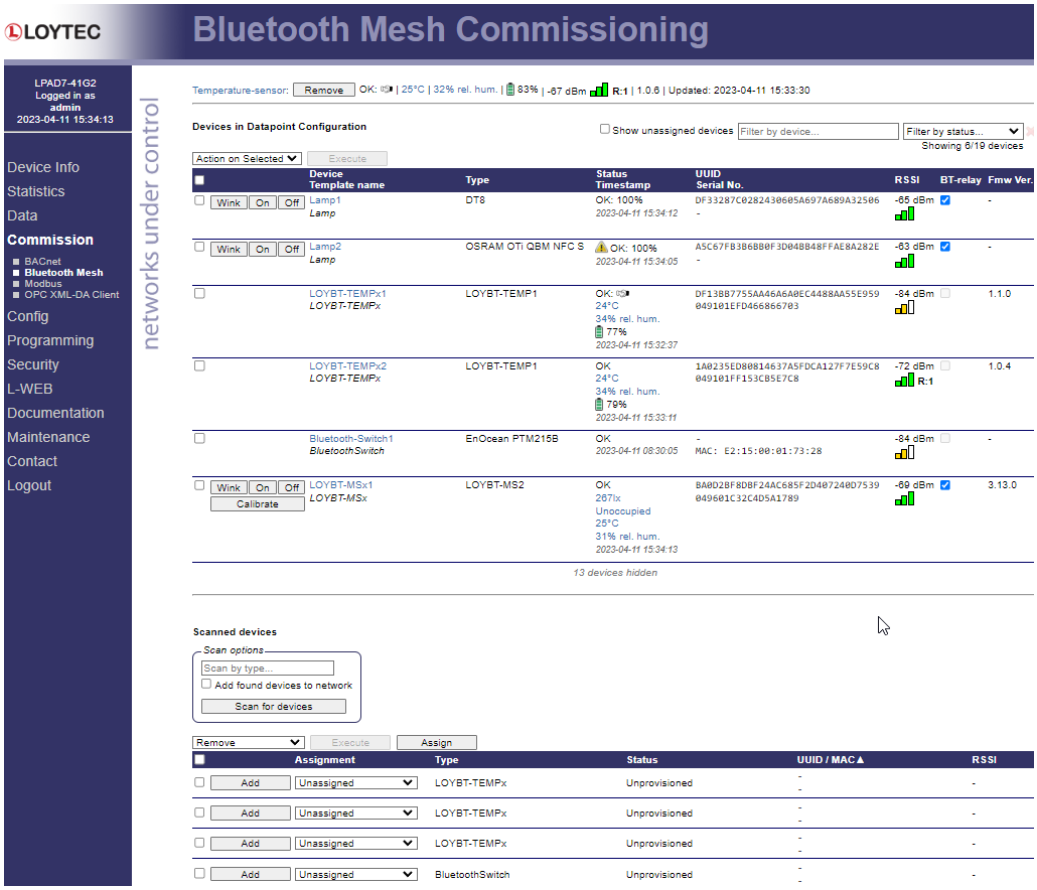


Figure 207: Bluetooth Mesh Commissioning Web page.

The **Scanned devices** section allows to setup a Bluetooth Mesh network and to connect added devices to the datapoint configuration. Most devices can be integrated more or less automatically, whereas some devices need manual interaction.

Low power nodes like LOYBT-TEMPx or Bluetooth Switch require a button press. If such devices are included in the configuration they are represented by a placeholder in the scanned devices table. The "Add" button allows to add those devices to the mesh with the help of an assignment wizard (see also 15.3.2.1 and 15.3.2.2).

The process for the devices that can be added automatically is structured in 3 parts:

- scan for unprovisioned mesh devices
- add unprovisioned devices to a bluetooth mesh network
- assign provisioned devices to a bluetooth mesh instance in the datapoint configuration

The checkbox **"Add found devices to network"** allows to add found devices to the network automatically and therefore combines the first two steps. This option removes the need for adding each device to the network manually but instead it maybe will add unprovisioned devices which shall not belong to the network and have to be removed from the network afterwards.

The **Scan for devices** button initiates a scan for devices that are broadcasting an unprovisioned mesh beacon. Found devices are put in the devices list (see Figure 208). The columns are similar to the columns in the Devices in Datapoint Configuration table (Type, RSSI, UUID/MAC (MAC instead of serial since it is unknown in this point in time). The Assignment-column is greyed out, because the device has to be added to the mesh before it can be assigned, by using the **"Add"**-Button.

If a device in the mesh is not reachable any more it is shown as **Offline** – it can than either be removed from the list using the **"Delete"**-button or the user can try to connect again using the **"Recover"**-button.

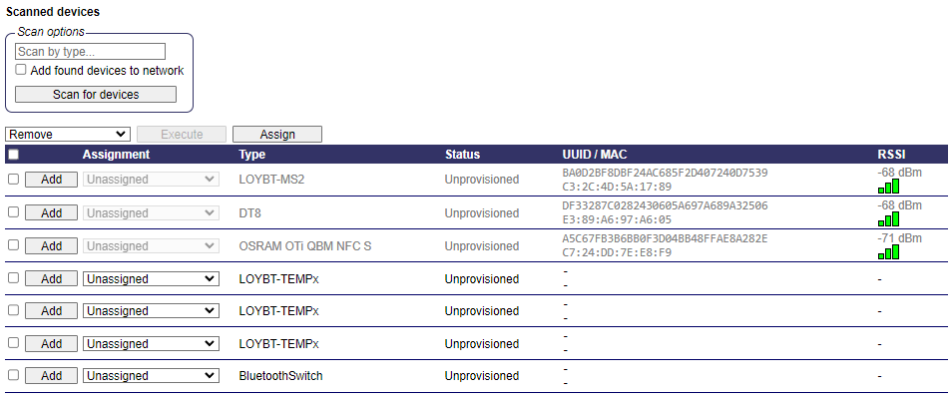


Figure 208: Scan Result showing unprovisioned devices and placeholders for devices that require manual interacton.

After adding the devices to the mesh, the status turns to OK and the assignment options and buttons for testing the communication to the device become available. Since supporting the **Wink**-function is optional in bluetooth mesh, **On** and **Off** buttons are also available.

Note: ***If nodes are changing the bluetooth MAC-address during mesh operation for security reasons the source of the received messages cannot be determined directly. This will result in outdated RSSI-values shown in italic letters (=last known RSSI).***

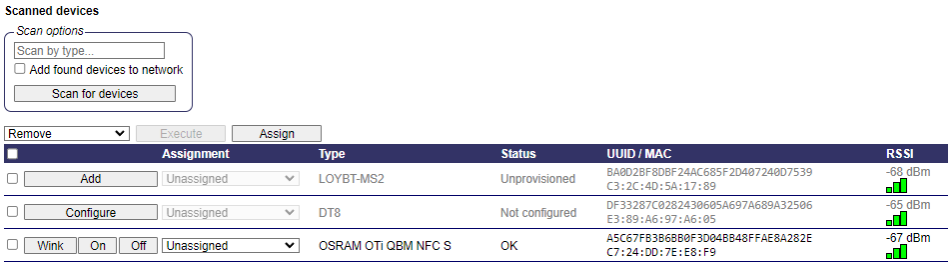


Figure 209: Scan Table with nodes in different states.

To remove devices from the network check one or more check boxes at the beginning of each line, choose the **Remove** option in the **Action on selected** drop-down and click **Execute**. The selected devices will be removed from the network and list. They will appear again in a scan as unprovisioned mesh devices.

Devices showing status “OK”, can be assigned to devices in the data point configuration, the user can select the Bluetooth device in a drop-down box and click on the **Assign** button.

The Status column can indicate the following states of the device:

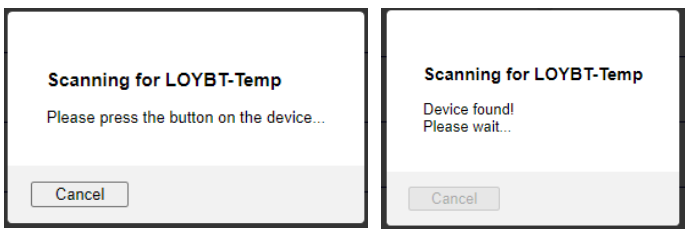
- **Unprovisioned** - if the device is in unprovisioned state
- **Adding / Configuring …** - transient states while the device is added to the network and gets it basic network parameter settings
- **Not Configured** – if the device has been added to the mesh and configuration failed
- **OK** – device in the mesh network
- **Assigning …** - transient state while device is assigned to a device in datapoint configuration
- **Offline** – if a node (already provisioned device) does not respond anymore

15.3.2.1 Integration of LOYTEC LOYBT-TEMP1

The LOYTEC LOYBT-TEMP1 is a low power node and therefore is in sleep mode most of the time. To communicate with the device it has to wake-up before, which can be enforced by a button press (manual user interaction).

A LOYBT-TEMP1 can either be assigned to the static Temperature-sensor template or it can be assigned to any LOYBT-TEMPx template used in the configuration.

The provisioning procedure is similar and can be initiated by pressing the “Add”-button. The wizard guides the user through the process (Figure 210). The provisioning procedure typically requires a single button press only to wake up the sleepy device.



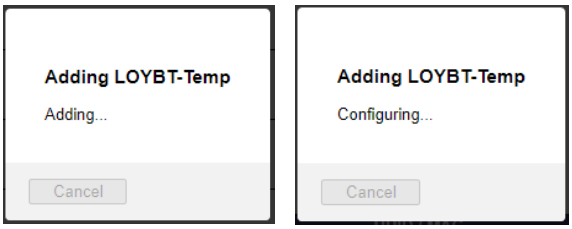


Figure 210: Assignment Wizard.

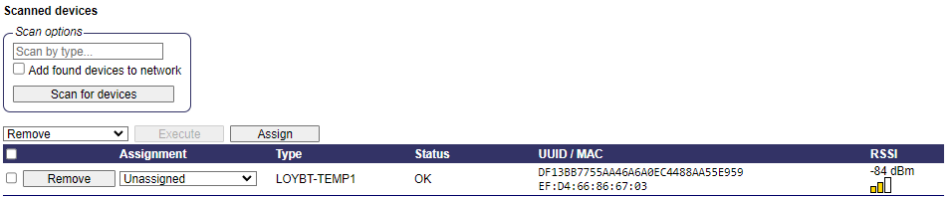


Figure 211: LOYBT-Temp1 has been added to the mesh.

The assignment can be done by selecting a LOYBT-TEMPx from the configuration via the dropdown menu and press the “Assign”-button. This selection can already be made before pressing the “Add”-button.

The LOYBT-TEMP1 can be removed in the same way: Simply press the “Remove”-button and follow the instructions in the wizard, which again typically requires a single button press (Figure 212).

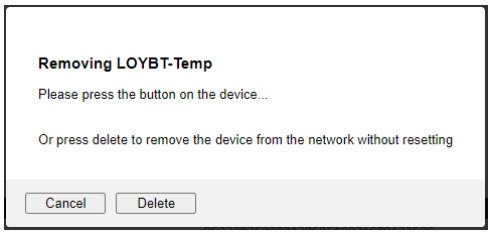


Figure 212: Wizard for Removing LOYBT-Temp.

Finally the LOYBT-TEMP1 will be available as sensor in the configuration and sensor data are available via the corresponding data points.

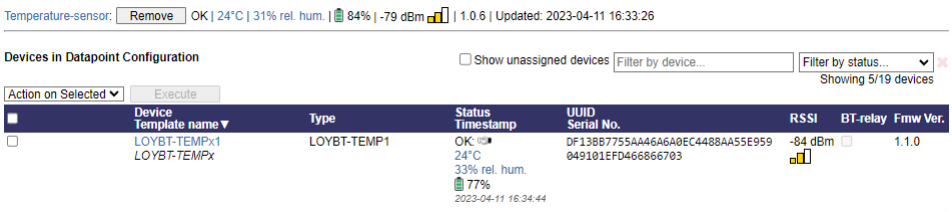


Figure 213: Assigned LOYBT-TEMP1s in datapoint configuration and for system register use.

15.3.2.2 Integration of EnOcean Bluetooth Switch PTM215B

The LOYTEC Bluetooth-Mesh ecosystem supports the integration of Bluetooth Switches based on the PTM215B module. This device uses EnOcean energy harvesting technology to transmit Bluetooth beacons on button press and button release.

A button module based on the EnOcean switch template has to be added to the datapoint configuration. Afterwards a placeholder for the Bluetooth Switch appears in the Scanned devices sections as shown in Figure 214.

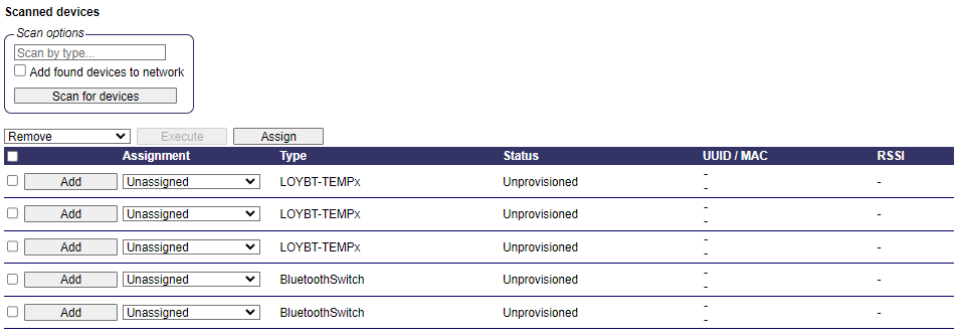


Figure 214: Entries for EnOcean-switches in scanned devices.

After pressing the "**Add**"-button a wizard appears asking for pressing a button on the Bluetooth Switch. If the LPAD receives a proper frame the Bluetooth Switch is added to the configuration immediately (see Figure 215).

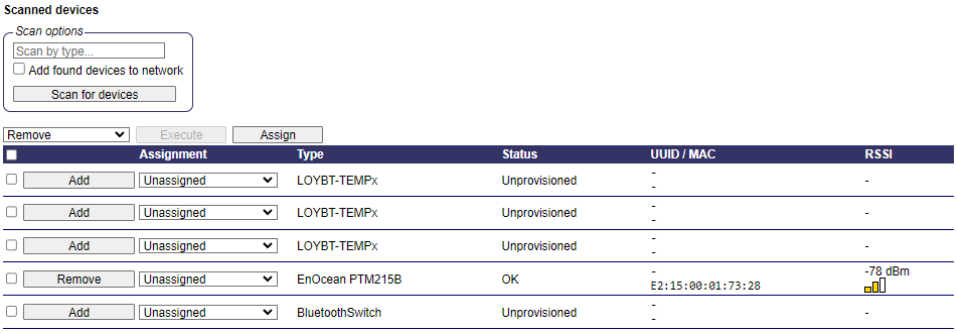


Figure 215: Bluetooth Switch after Teach-In.

The MAC-address of the device is shown as identifier. This can also be found on the label on the backside of the module.

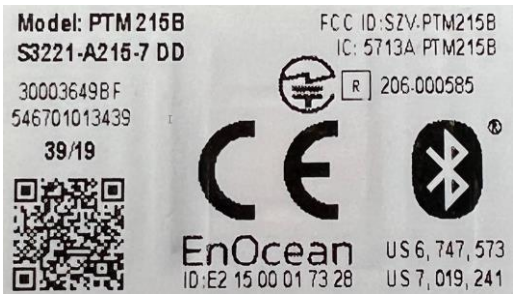


Figure 216: PTM215B label with ID (MAC-address) and QR-code.

The assignment via the dropdown menu can either be done before or after the Teach-In (Assigned Bluetooth Switch see Figure 217).

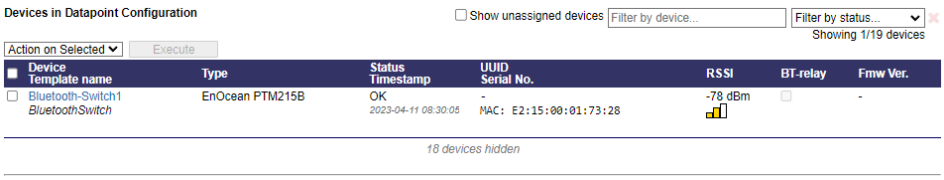


Figure 217: Assigned Bluetooth Switch PTM215B.

To remove the added physical device simply use the "**Unassign**"-option as for other devices.

15.3.3 Groups

Grouping of Bluetooth Mesh devices allows the simultaneous control of the devices. The grouping is done by using the datapoint **GroupName**. The name of the group automatically assigns the device to a group with the corresponding Name.

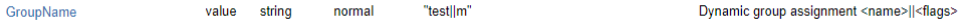


Figure 218: Data point: GroupName.

The name represents the name of the group, the flags are used for setup of a proper control flow. The general behavior using only a name (without flags) is that the device can be controlled via its own datapoints or via the group master.

Flags:

- m … master, the datapoints of this device are used to control all other devices with the same name-tag, there can be multiple masters for the same group
- s … slave, the device is a pure slave, it can only be controlled via a master

Note:	*If no master is defined for a group the controller will choose the master by itself so that the logic has a group master to interact with.*

15.3.4 Scenes

Not yet supported.

15.3.5 Statistics

The Bluetooth Mesh statistics page displays the statistics data of the Bluetooth mesh network. To reset all statistics counters to zero, click on the button **Clear Statistics**. The field **Statistics cleared** will reflect the time of the last reset.

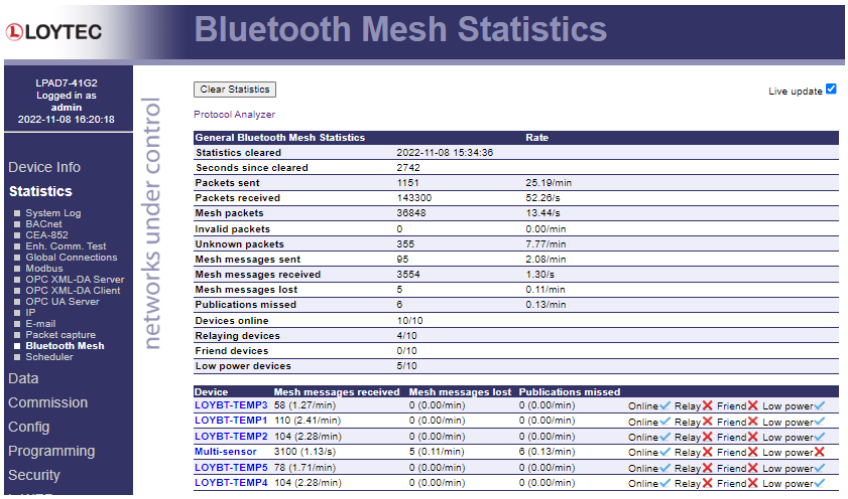


Figure 219: Bluetooth Mesh Statistics.

Statistical values:

- **Statistics cleared:** Timestamp of last clear/powerup
- **Seconds since cleared:** period of current statistic values
- **Packets sent:** Number of Bluetooth frames sent
- **Packets received:** Number of Bluetooth frames received
- **Mesh packets:** Number of Bluetooth mesh packets
- **Invalid packets:** Number of invalid packets
- **Unknown packets:** Number of unknown packets
- **Mesh messages sent:** Number of mesh messages sent by the controller
- **Mesh messages received:** Number of mehs messages received by the controller
- **Mesh messages lost:** Number of messages that have not been acknowledged although a reply was expected
- **Publication missed:** Number of expected publication messages that have not been received
- **Devices online:** Number of online devices
- **Relaying devices:** Number of devices with relay feature enabled
- **Friend devices:** Number of devices with friend feature enabled
- **Low power devices:** Number of devices with low power feature enabled

In addition per device statistics provide more detailed information.

15.3.6 Protocol Analyzer

By activating the link **Protocol Analyzer** (available in Bluetooth Mesh statistics), the protocol analyzer page is shown as displayed in Figure 220.

Start protocol analyzer | Clear Log | Save Log | Status: **Stopped** | Filter text... | Hide report messages ☐ | Automatic Scrolling ☐ | Live update ☑

Timestamp	Source	Destination	Message type	Values	Raw data
2022-09-26 15:27:35.430	LPAD7-41G2 (0x0001)	Lamp5 (0x0290)	Light Lightness Set Unacknowledged (0x824D)	Transaction ID: 8 Transition time: 1.0s Delay: 0ms	0xFFFF080A00
2022-09-26 15:27:35.520	Lamp5 (0x0290)	REPORT (0xF010)	Light Lightness Status (0x824E)	Present: 2% Target: 100% Remaining time: 0.9s	0x1F05FFFF09
2022-09-26 15:27:35.790	Lamp5 (0x0290)	REPORT (0xF010)	Light Lightness Status (0x824E)	Present: 2% Target: 100% Remaining time: 0.9s	0x1F05FFFF09
2022-09-26 15:27:36.490	Lamp5 (0x0290)	REPORT (0xF010)	Light Lightness Status (0x824E)	Present: 100%	0xFFFF
2022-09-26 15:27:36.710	Lamp5 (0x0290)	REPORT (0xF010)	Light Lightness Status (0x824E)	Present: 100%	0xFFFF
2022-09-26 15:27:37.390	LPAD7-41G2 (0x0001)	Lamp5 (0x0290)	Light Lightness Set Unacknowledged (0x824D)	Lightness: 0% Transaction ID: 9 Transition time: 1.0s Delay: 0ms	0x0000090A00
2022-09-26 15:27:37.510	Lamp5 (0x0290)	REPORT (0xF010)	Light Lightness Status (0x824E)	Present: 94% Target: 0% Remaining time: 0.9s	0xE5F0000009
2022-09-26 15:27:37.720	Lamp5 (0x0290)	REPORT (0xF010)	Light Lightness Status (0x824E)	Present: 94% Target: 0% Remaining time: 0.9s	0xE5F0000009
2022-09-26 15:27:38.480	Lamp5 (0x0290)	REPORT (0xF010)	Light Lightness Status (0x824E)	Present: 0%	0x0000
2022-09-26 15:27:38.690	Lamp5 (0x0290)	REPORT (0xF010)	Light Lightness Status (0x824E)	Present: 0%	0x0000
2022-09-26 15:28:18.230	LOYBT-TEMP1 (0x02CE)	REPORT (0xF010)	Sensor Status (0x52)	Rel. Hum.: 41% Temperature: 25°C	0xA20EE209C20E0410
2022-09-26 15:28:18.340	LOYBT-TEMP1 (0x02CE)	REPORT (0xF010)	Generic Battery Status (0x8224)	Battery level: 93% Time to discharge: unknown Time to charge: unknown Flags: Presence: 1 Indicator: 2 Charging: 0 Serviceability: 1	0x5DFFFFFFFFFFFF49
2022-09-26 15:28:18.460	LOYBT-TEMP1 (0x02CE)	REPORT (0xF010)	Loytec CFG Status (0xC20AA0)	Property ID: 0x0001 Firmware version	0x010003010100
2022-09-26 15:28:18.590	LOYBT-TEMP1 (0x02CE)	REPORT (0xF010)	Loytec CFG Status (0xC20AA0)	Property ID: 0x0002 Build time stamp	0x02000423DD2963
2022-09-26 15:28:18.680	LOYBT-TEMP1 (0x02CE)	REPORT (0xF010)	Loytec CFG Status (0xC20AA0)	Property ID: 0x000D Server flags	0x0D000400000000
2022-09-26 15:28:18.800	LOYBT-TEMP1 (0x02CE)	REPORT (0xF010)	Sensor Status (0x52)	Rel. Hum.: 41% Temperature: 25°C	0xA20EE209C20E0410
2022-09-26 15:28:18.930	LOYBT-TEMP1 (0x02CE)	REPORT (0xF010)	Generic Battery Status (0x8224)	Battery level: 93% Time to discharge: unknown Time to charge: unknown Flags: Presence: 1 Indicator: 2 Charging: 0 Serviceability: 1	0x5DFFFFFFFFFFFF49

Figure 220: Bluetooth Mesh Protocol Analyzer.

With the **filter** window the number of logged frames can be reduced by configuring a filter to logging only certain frames containing the filter text. By pressing the button **Start** or **Stop** the protocol analyzer can be started and stopped respectively. When stopped click on **Save** to store the protocol log as a CSV file. **Clear Log** clears the log data. Check **Automatic Scrolling** to always show the newest frames by automatically scrolling to stay at the end of the page.

Each line contains the following information:

- **Timestamp** (Example: “2022-09-26 15:27:35.430”): Local time on the device when the frame was received (end of frame).
- **Source** (Examples: “LOYBT-TEMP1 (0x02CE)”, “LPAD7-41G2(0x0001)”): Originator of the mesh message incl. element address.
- **Destination** (Examples: “REPORT (0xF010)”, “Lamp1 (0x0290)”): Destination of the mesh message incl. element address. All report messages in a LOYTEC-bluetooth mesh network report to the same group (REPORT). Messages from the controller typically directly control lamps or groups.
- **Message type** (Examples: “Light Lightness Set Unacknowledged”) explains the meaning behind the message
- **Values** (Examples: Lightness 0%, Transcation ID: 9, Transition Time 1.0s, Delay 0ms) contains the encoded message data
- **Raw Data** (Example: “0x0000090A00”): contains the raw payload of the message of the current type

15.4 Troubleshooting

15.4.1 Device Recovery

To remove a device from a mesh system it has to be unprovisioned which typically is the same as bringing it to factory default state. There are several actions to reset a device:

- Node Reset command (mesh command, in the WebUI this command is sent when performing the “Remove”-action (see also Section 15.3.2).
- Manufacturer specific action: dependent on the device and described in the datasheets. For LOYTEC devices the following applies:
  - LOYBT-TEMP1: 20 second button press
  - LOYBT-MSx: short-circuit DI2 and DI3 or use LOYBT-CALIB1 reset feature

Hint:	***Due to an improper removal (without a node-reset) the device can end up in a state where it must be manually reset.***

16 DALI

16.1 Introduction

DALI stands for “Digital Addressable Lighting Interface” and is the name commonly used for the communication protocol defined in the international standard IEC 62386[3]. It is used to dim and switch luminaries from most leading manufacturers. DALI also supports devices like multi-sensors (e.g. for illuminance, occupancy, etc.) and intelligent switches. For further information regarding DALI please refer to https://www.digitalilluminationinterface.org.

To ensure device interoperability, DALI-2 compliant devices – bus power supplies, input devices and ballasts – can be certified by the Digital Illumination Interface Association (DiiA). Only certified devices may bear the DALI-2 logo shown in Figure 221 and are listed in the product database on the DiiA website (https://www.digitalilluminationinterface.org).



Figure 221: DALI-2 Logo.

Important: ***LOYTEC recommends using only DALI-2 certified devices wherever possible.***

16.1.1 DALI Wiring

DALI wiring is typically run together with the mains wiring using normal mains rated wire (2 wires). Table 8 shows the recommended conductor size depending on the length of the DALI wires. A total length of 300 m must not be exceeded.

DALI cable length	Recommended min. conductor size
< 100 m	0.5 mm^2
100-150 m	0.75 mm^2
150-300 m	1.5 mm^2

Table 8: Recommended minimum conductor size for DALI wiring

[3] Previous versions of the DALI standard were defined in IEC 60929 Annex E.

Though the signal is only 16 V (typical), DALI is not SELV rated and should therefore treated as mains voltage wiring[4].

DALI connections are not polarity sensitive[5].

16.1.2 DALI Interface and DALI Bus Power Consumption

Each DALI-interface connected to the DALI-line typically draws a current of a few mA from the DALI-line. The power drawn by the devices via the DALI line must be provided by a DALI bus power supply. The maximum current on a DALI-line which can be provided either by a single or by multiple bus-power supplies is 250mA.

The bus-current consumption of DALI-devices as well as the *guaranteed current* and *maximum current* provided by bus-power supplies has to be taken into account for DALI system design.

Bus Power Supply:

While for power supplies the *maximum supply current* has to be taken into account when operating multiple bus power supplies in parallel, the *guaranteed supply current* represents the value that is provided by the bus power supply under any operating conditions.

The sum of maximum supply currents of DALI bus power supplies on a DALI-line must not exceed 250mA.

The sum of the guaranteed current consumptions of DALI bus power supplies on a DALI-line is the current which must not exceeded by the current consumption of the DALI-devices connected to this line.

Bus Power Consumption:

The maximum bus-current consumption of externally powered DALI-devices is limited by 2mA as defined in IEC62368-101.

For bus-powered devices there is no limit given by the DALI-standard, but the *maximum current* (typically the inrush current) has to be stated in the datasheet. Furthermore for certified devices it is listed in the DiiA database.

While the maximum current is representing the theoretically worst case, the *idle current* (often provided in the datasheet) reflects the best case with respect to current consumption. The actual current during operation (with DALI communication and different states or operating modes of the bus-powered device) will at least sometimes result in a current consumption somewhere between the idle and the maximum current.

The DALI-Alliance introduced a rule of thumb[6] to consider the times no power is available on the DALI bus due to communication. The power consumption of the DALI devices (idle current) must be multiplied by the **factor 1.2** when calculating the required DALI bus power supply current:

[4] Basic insulation only required between DALI and mains voltage.

[5] Except for the bus power supply, in case more than one bus power supply is connected to the channel.

[6] This rule will work in most cases, but may fail sometimes.

$$\sum I_{DALI\ devices} \leq \frac{I_{Power\ Supply}}{1.2}$$

For LOYTEC devices Table 9 applies and shows the typical power drawn via the DALI line depending on device types. It represents the worst-case during operation and is much more accurate compared to rule of thumb.

For DALI devices not listed in the table see the corresponding datasheet or contact the device vendor on the power drawn via the DALI line.

Device type	bus-current consumption (typical)
externally powered DALI devices	2 mA
LOYTEC LDALI-RM8 relay module (ext. powered)	2 mA
LOYTEC LDALI-PWM4-x (ext. powered)	2mA
LOYTEC LDALI-PWM8-x (ext. powered)	2mA
LOYTEC LDALI-MS2 multi-sensor	3.5 mA
LOYTEC LDALI-MS2/MS4-BT multi-sensor	6mA / 10mA[7]
LOYTEC LDALI-BM2 button coupler	3 mA
LOYTEC LDALI-RM5/RM6	6 mA
LOY-DALI-SBM1 sunblind module	6 mA
LOYTEC LDALI-PD1 phase-cut dimmer module	6 mA
LOYTEC LDALI-RM1 relay module (EOL)	2.6 mA
LOYTEC LDALI-RM2 1-10V interface (EOL)	4.2 mA
LOYTEC LDALI-RM3/RM4 (EOL)	3.4 mA
LOYTEC LDALI-BM1 button coupler (EOL)	3.1 mA
LOYTEC LDALI-MS1 multi-sensor (EOL)	4.1 mA

Table 9: DALI bus power usage for different device types (@16 V DC)

16.1.3 Multi-Master Operation

The LOYTEC DALI interface is capable of multi-master operation. Thus it can be installed in parallel to one or more other DALI master controllers on the same DALI network. However, all other DALI master controllers must be multi-master capable in order to render a working DALI system. Other DALI masters may be DALI-2 input devices (sensors,

[7] the higher current applies if bluetooth-based functions are enabled

buttons), multi-sensors with built in constant light or occupancy controller functionality, DALI switches, buttons, and touch panels, as well as other DALI controllers.

16.2 DALI Device Types

Figure 222 shows the typical structure of a DALI system.

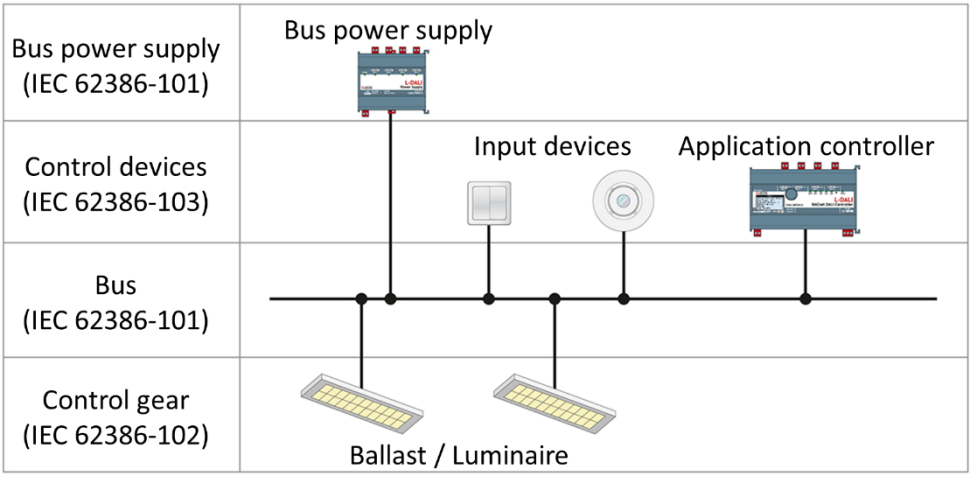


Figure 222: Typical structure of a DALI system.

It consists of the following components:

Bus power supply

Each DALI channel must contain at least one bus power supply. Bus power supplies are defined in IEC 62386-101. For more information on the DALI bus power supplies see Section 16.1.2 (Power consumption), for LOYTEC bus power supplies refer to the LOYTEC LDALI devices user manual [11].

DALI Ballasts

DALI ballasts are specified in the IEC 62386-102 part of the DALI standard and the DALI device types are specified in parts IEC 62386-201 to 209 (see Table 10). For LOYTEC ballasts refert to the LOYTEC LDALI devices user manual [11]. See AN011E L-DALI Compatibility List [9] for DALI ballasts tested with the LOYTEC DALI interface.

Control gear type	Standard
Fluorescent lamps	IEC 62386-201
Self-contained emergency lighting	IEC 62386-202
Discharge lamps	IEC 62386-203
Low voltage halogen lamps	IEC 62386-204
Incandescent lamps	IEC 62386-205
Converter Digital to DC voltage	IEC 62386-206

Control gear type	Standard
LED modules	IEC 62386-207
Switching function	IEC 62386-208
Colour control	IEC 62386-209

Table 10: DALI control gear types.

DALI Input Devices

The DALI-2 standard covers DALI input devices (sensors and buttons) in its part IEC 62386-103. The LOYTEC DALI controllers allow to integrate sensors and buttons based on the DALI-2 standard.

DALI-2 input devices provide their input values via one of its instances. Each device can have up to 32 instances. Figure 223 shows a typical example of a DALI-2 input device with its instances, representing a multi-sensor (occupancy and lux instances) which supports an IR-remote (push-button instances) and has two generic instances representing a built-in temperature and humidity sensor.

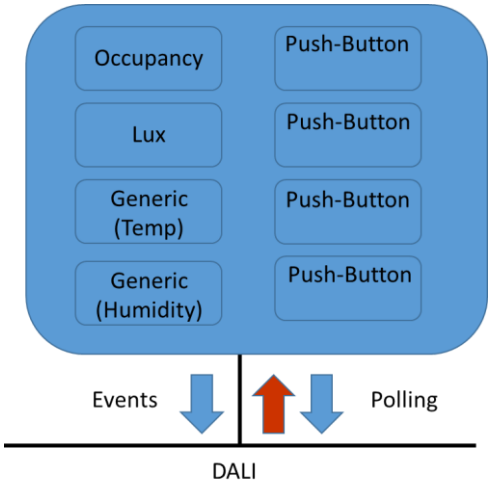


Figure 223: DALI-2 input device instances.

Different instance types are specified in the parts IEC 62386-301 to 304 of the DALI standard (62386-305 and306 in progress). Additional feature types which can be used in combination with instances are defined in IEC 62386-332 and 333.

Instance/Feature type	Standard	Device Class
Push-Button	IEC 62386-301	Button
Absolute Input	IEC 62386-302	Button
Occupancy Sensor	IEC 62386-303	Sensor
Light Sensor	IEC 62386-304	Sensor

Instance/Feature type	Standard	Device Class
Colour Sensor	*IEC 62386-305*[8]	*Sensor*
General Purpose Sensor	*IEC 62386-306*[9]	*Sensor*
Generic	IEC 62386-103	Sensor / Button
Input devices – Feedback (feature)	IEC 62386-332	Button

Table 11: Instance and Feature types defined in DALI-2.

For LOYTEC input devices, i.e. sensors and button modules, refer to the LOYTEC LDALI devices user manual [11]. See AN011E L-DALI Compatibility List [9] for DALI input devices tested with the LOYTEC DALI interface.

DALI Application controller

The DALI-2 standard covers DALI application controllers in its part IEC 62386-103. The application itself is not defined, only the command set and the behavior of the DALI-interface is defined.

The DALI application controllers are the brain of each DALI-system. Application controllers allow to use DALI sensor values or buttons as inputs in their fixed application program or program logic and control the ballasts on the DALI-line.

For the complete function of LOYTEC application controller refer to the LDALI User Manual [2].

16.3 LOYTEC DALI Interface

16.3.1 LOYTEC Controller Types and Features

LOYTEC controller with DALI interface can be separated in 2 different groups:

- Fixed application controller models
- Programmable controller models

The main difference is the light application, it is either fixed or programmable. Whereas fixed application controllers have a predefined number of various object-types (lamp-actuator, group-actuator, clc, sensor, etc.) per channel, for programmable controller the number can be tailored to the application.

DALI controllers allow to use DALI sensor values or button states as inputs in their fixed application program (e.g. for constant light controller in LDALI-ME20x-U, LDALI-3E10x-U) or as data points in the program logic of the programmable controller models (e.g. LDALI-PLC2/PLC4, LROC-400).

[8] Standardization in Progress

[9] Standardization in Progress

Depending on the model LOYTEC devices support up to 4 DALI channels. The following features are supported:

- Direct control of up to 64 DALI devices per DALI channel
- Direct control of up to 16 DALI groups per DALI channel
- Scene control for up to 16 groups and one broadcast scene per DALI channel
- Detect lamp and ballast failure on DALI luminaries and signals
- DALI Multi-Master capable
- Integration of up to 64 DALI-2 input devices (sensors and buttons)
- Simple replacement of (broken) DALI devices (no configuration tool required)
- Built-in DALI protocol analyzer

On the LOYTEC DALI controllers DALI-2 input devices are separated into device classes sensors and buttons depending on the instance type of their instances. Table 11 shows which instance types are available via which device class. All instances belonging to the sensor device class – if any – will appear as one DALI sensor device, all instances belonging to the button device class as one DALI button device. Sensor and button devices belonging to the same physical device will have identical short addresses and serial numbers.

In our multi-sensor example shown in Figure 224 the occupany, lux, temperature and humidity sensor values are available via the sensor device, while the push-button instances are available via the button device.

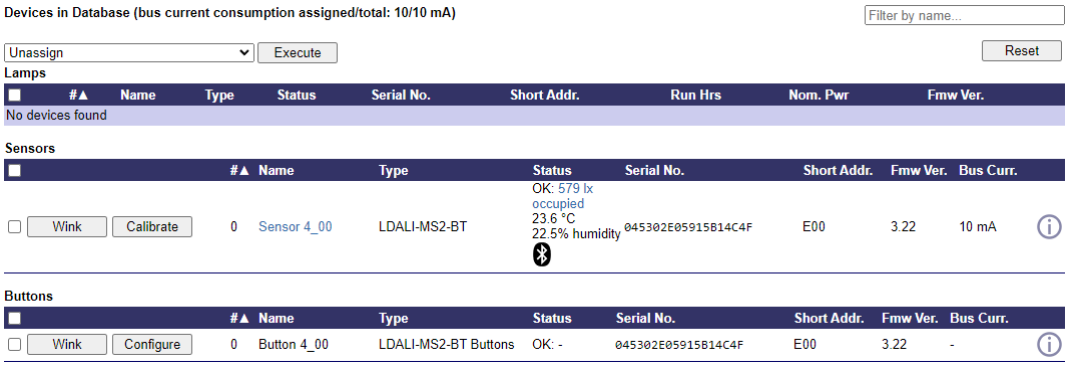


Figure 224: LDALI-MS2-BT represented by sensor and button instance with the same DALI-short address and serial number.

16.3.2 DALI Channel Limitations

The number of devices per channel is limited by the following aspects:

Limits of LOYTEC DALI master:

- The LOYTEC DALI controller supports a maximum of **64 ballasts** and **64 buttons** per DALI channel (which can be assigned).
- On **L-DALI controllers** a maximum of **16 sensors** per DALI channel is supported.
- On **programmable L-DALI controllers** up to **64 sensors** can be assigned.

Address-Limitations:

A maximum of **64 addresses** each for ballasts and input devices (sensors, buttons) are available per DALI channel, allowing a maximum of **64 ballasts and 64 input devices** per channel.

Each device (ballast, sensor, buttons) uses one DALI address with the following exceptions:

- The **LOYTEC DALI master** does not use a DALI address[10].
- Some **DALI ballasts with multiple channels** (e.g. RGB or warm and cool white) use one DALI address for each channel. Please refer to the manufacturer's documentation of the ballast or luminaire to determine the number of DALI addresses used.
- Some **pre-DALI-2 sensors** using proprietary extensions of the DALI protocol use ballast addresses, thus reducing the number of ballasts on a DALI channel. Please refer to the manufacturer's documentation of the sensor to determine the number of DALI addresses used. LOYTEC recommends using only DALI-2 certified devices wherever possible.

16.3.3 Device Class – Lamps

DALI ballasts can be used together with the LOYTEC DALI controllers in different ways:

Fixed application controller models (LDALI-ME20x-U/LDALI-3E10x-U):

- Dim level and Feedback values are mapped to datapoints and exposed to BACnet (ME20x-U) or CEA-709 (3E10x-U).
- Lamps can be grouped and groups can be bound to constant light control.
- Scenes can be set up for each lamp.
- A wide set of DALI-parameters can be set for each lamp, containing *Max_Pres_Value, Power_On_Level, System_Failure_Level, Fade_Time, Min_Level* etc.

Programmable controller models (LDALI-PLC2/4, LROC-400, LROC401):

- Lamp properties are available as datapoints in the program logic.
- Standard Lamp Actuator (LampActuatorStd.dali): provides data points for dimming (*DimLevel, DimLevelGrp* – the *Mode* property allows to select the dimming behavior*: Fading, Ramping or LinearFading*), commands (*Command, CommandGrp*), feedback (*Feedback* – the value is available on logarithmic or linear scale – *Value, ValueLinear*), status (*Status*), DALI-parameters (*DALI-Cfg*), grouping (*Group, GroupName*) as well as for device configuration (*DeviceCfg*) and LOYTEC specific configuration (*LoytecCfg*). In addition datapoints for Energy and RunHours are available.
- Colour Lamp Actuator (LampActuatorColourControl.dali): in addition to the standard lamp actuator this template provides colour support for Tc, XY, RGBW in DALI Format (*Colour*) as well as for hue (*Hue*) and saturation (*Saturation*).
- Colour Lamp Actuator (LampActuatorColourControl_XY_TC_HSV.dali): this template is very similar but with an optimized and reduced set of datapoints. For dimlevel, colour, command, hue and saturation only the datapoints for dynamic groups are supported (*DimLevelGrp, ColourGrp, CommandGrp, HueGrp, SaturationGrp)*.

[10] Theoretically, an external application controller can assign an address to a LDALI controller with DALI-2 compliant interface

- The LOY-DALI-SBM1 sunblind module is represented by a special set of datapoints defined in the template LOY-DALI-SBM1.dali: *UpDuration* and *DownDuration* can be used to move the sunblind up or down for the defined time in ms written to the corresponding datapoint. Please note that only values with a resolution of 10ms are supported. The *Feedback* reports the state of the module (STOPPED, UP, DOWN), but is updated only once per minute.

LOYTEC Devices represented by a Lamp-Actuator:

For a detailed description of LOYTEC devices acting as ballast refer to LOYTEC LDALI Devices User Manual [11]:

- Relay and converter modules:
  - LOYTEC LDALI-RM5/RM6 relay/converter module
  - LOYTEC LDALI-RM8 relay module
  - LOYTEC LDALI-RM3/RM4 relay/converter module (EOL)
- PWM-modules:
  - LOYTEC LDALI PWM4/PWM4-Tc/PWM4-RGBW
  - LOYTEC LDALI PWM8/PWM8-Tc/PWM8-RGBW
- Phase-Cut dimmer module:
  - LOYTEC LDALI-PD1
- Sunblind module:
  - LOYTEC LOY-DALI-SBM1

Note:	*The system failure and power-on behavior is always dependent on the DALI-device, especially if it is buspowered or externally powered. For the behavior of LOYTEC devices refer to the LOYTEC LDALI Devices User Manual [11].*

LOYTEC LDALI-RM5/RM6: Setup Mode of Operation

The LDALI-RM5/6 can be operated in ‘Switching Function’ or ‘Converter’ mode. The mode of the LDALI-RM5/6 defines whether a driver is connected to the 1-10V output. The mode is selected via DALI operating mode, which can be done by changing the operating mode either after scanning (see Figure 225) or via the drop down menu of an already assigned device (Figure 226).

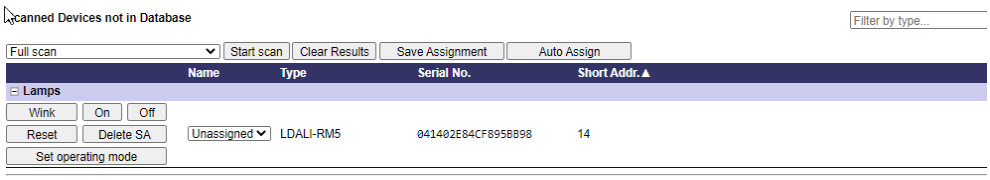


Figure 225: Press “Set operating mode” button for operating mode selection

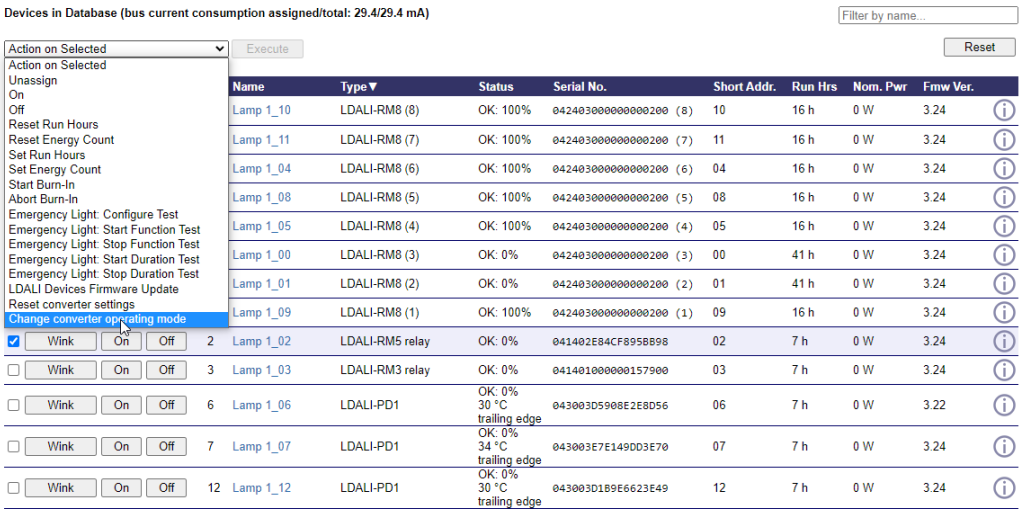


Figure 226: “Change converter operating mode” of an assigned device

Note:	*The info field of the LDALI RM5/6 on the DALI-Installation tab in the WebUI shows the number of switching cycles performed by the relay.*

Recommendation:	*For dimming a 1-10V lamp with a control element (dial, slider, ...) choose the ‘linear dimming curve’ and a fade time of 0.7 seconds for better dimming results.*

LOYTEC LDALI-RM8: Indication of DI-Override

The switching state can be controlled via DALI as long as the corresponding digital input is open. Closing the input will always switch on the relay (override). An override via DIx (digital input) will be inidcated in the WebUI (see Figure 227) of the LOYTEC DALI master devices and is available as property *Digital_Input_Override* of the channel analog input object or as SNVT *nvoDigitalInputOverride.*

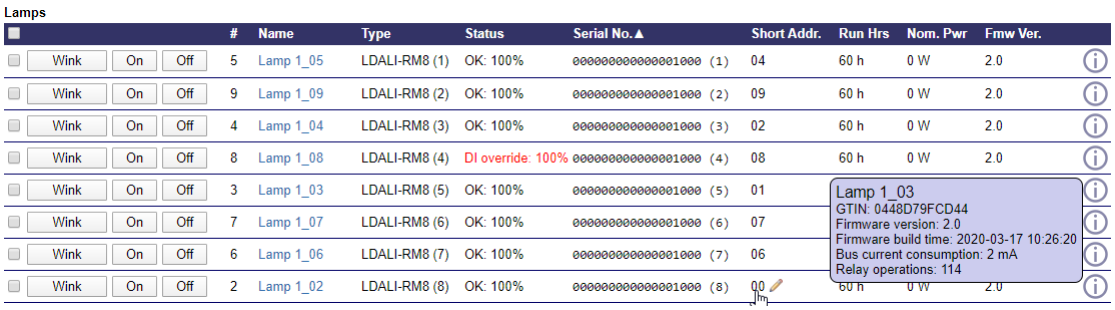


Figure 227: Web UI view LDALI-RM8

LOYTEC LOY-DALI-SBM1: Web UI representation

The Web-UI offers other control options for the the sunblind module. UP and DOWN button start to move the sunblind in the corresponding direction for 10 seconds. STOP stops the sunblind immediately. The WINK moves blind up and down alternately for 2 seconds.

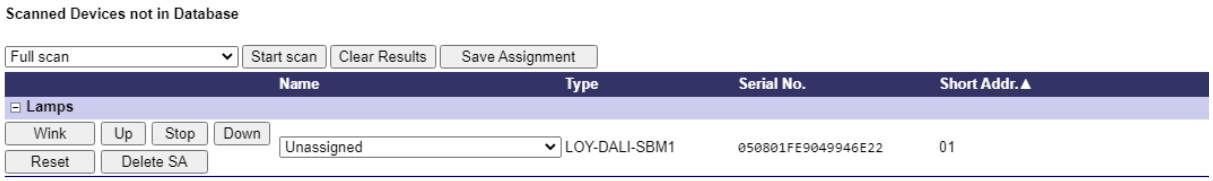


Figure 228: WebUI-view LOY-DALI-SBM1 after scan

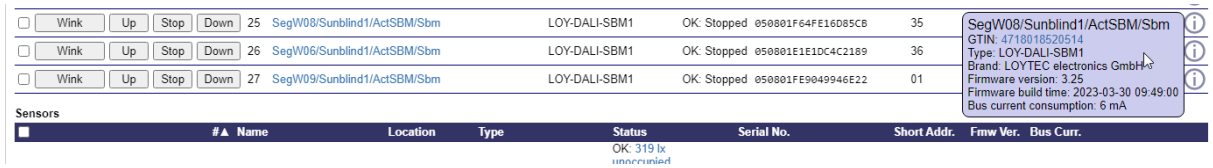


Figure 229: WebUI-view LOY-DALI-SBM1 after assignment

16.3.4 Device Class – Buttons

DALI buttons can be used together with the LOYTEC DALI controllers in different ways:

Fixed application controller models (LDALI-ME20X-U/LDALI-3E10X-U):

- Manual control of DALI groups (dimming lights, scene recall).
- Manual control of sublinds controlled via built-in sunblind controller application (up/down, open/close).
- Mapping DALI button inputs to data points (see L-INX Configurator User Manual [1] and L-DALI User Manual [8]).
- The feedback LEDs (if supported by the button input) can be configured to indicate the state of the group (On/Off) or it can be mapped to a datapoint.
- **Button Functions:** The button functions which can be assigned to a DALI-button are versatile. Access is not only given to lighting (dimming, recalling scenes), but also to sunblindcontrol, air condition and heating. The LDALI-controller supports all the functions and maps the button-input to the corresponding technology. See L-DALI User Manual [8] and the L-INX Configurator User Manual [1] on how to configure which button input performs which function.

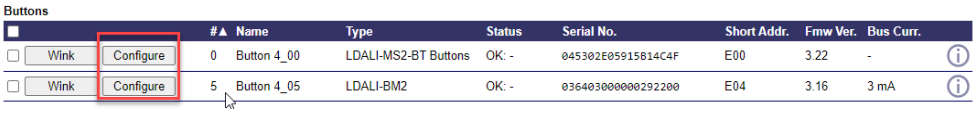


Figure 230: Configure button available on fixed application controller only.

Programmable controller models (LDALI-PLC2/4, LROC-400, LROC401):

- DALI button inputs are available as data points in the program logic.
- Feedback LEDs of button modules can be accessed via datapoints in the program logic
- Standard DALI push-button (ButtonDigital.dali): This template represents up to 32 instances of digital inputs. Each bit of the *Button* data point is representing the state of the corresponding input.

- **LDALI-MS2 buttons** (LDALI-MS2 Buttons.dali): This template is similar to the standard DALI push-button (ButtonDigital.dali) template. Other than this generic button template the 21 sub-data points of the *Button* data point are named according to the corresponding input (e.g. *DI1*, *Lights UP*, etc.) instead of having a generic name (*B1*, *B2*, etc.).

- **LDALI-BM2** (LDALI-BM2.dali): This template is similar to the standard DALI push-button (ButtonDigital.dali) template. The device folder contains four sub-data points – Button.*IN1* to Button.*IN4* and four datapoints *Feedback IN1 – Feedback IN4* – representing the four inputs and the four feedback LEDs if operated as digital inputs. For inputs 1 and 2, the data point *Mode INx* (x = 1-2) allows to select between different operating modes of the input:

    - **Generic**: In this mode the data point *GenericValue INx* represents the resistance measured at the input in Ohm (range: 0-65kOhm), this mode is also suitable to connect a NTC10k for temperature measurements.

    - **Push Button**: Use this mode if the input is operated in digital mode (e.g. connected to a standard switch or button). In this case the data point *Button.INx* represents the current state of the input, *FeedBack INx* represents the feedback LEDs.

    - **Absolute Input**: In this mode the data point *AbsoluteInput INx* represents the resistance measured at the input as a value between 0% and 100% of a 10k or 1k resistor. It must be used if a potentiometer or slider is connected to the input.

LOYTEC Devices with Button-Instances:

For a detailed description of LOYTEC devices with button instances refer to LOYTEC LDALI Devices User Manual [11]:

- LDALI-BM2 button module (4 digitals inputs)

- LDALI-MS2, LDALI-MS2-BT, LDALI-MS4-BT multisensors with 3 digital inputs and support for L-RC1 and Apple IR-remote control

16.3.5 Device Class – Sensors

DALI sensors can be used together with the LOYTEC DALI controllers in different ways:

Fixed application controller models (LDALI-ME20X-U/LDALI-3E10X-U):

- Occupancy and Illuminance measurements for constant light control (CLC).

- Occupancy and Illuminance are mapped to datapoints and can be exposed to other technologies.

- Temperature and Humidity of LOYTEC LDALI-MSx(-BT) sensor types are mapped to datapoints.

- Bluetooth features of For LOYTEC LDALI-MS2/MS4-BT are supported.

Programmable controller models (LDALI-PLC2/4, LROC-400, LROC401):

- Occupancy and Illuminance measurements are available as datapoints in the program logic.
- Temperature and Humidity of LOYTEC LDALI-MSx(-BT) sensor types are mapped to datapoints.
- Standard DALI-multisensor (SensorMulti.dali): This template represents one occupancy and 2 illuminance instances for DALI-2 multisensors.
- **LDALI-MS2** (LDALI-MS2.dali): This template is similar to the standard DALI multi-sensor (SensorMulti.dali) template. In addition it provides data points for temperature (*Temperature*) and humidity (*Humidity*). As the LDALI-MS2 only provides one lux sensor value, it only contains a single lux level data point (*Lux*) and one gain table data point (*Gain*). Furthermore the structured datapoints *iBeaconCfg* (*UUID*, *Major*, *Minor*), *Eddystone BeaconCfg* (*Name*, *Instance*), *LWebBeaconCfg* (*LocalName*, *ClientConfig*, *View1*, *View2*) are provided as well as the *AssetData* and *AssetCount*, since they are required for BLE-based features of LDALI-MSx-BT sensors.

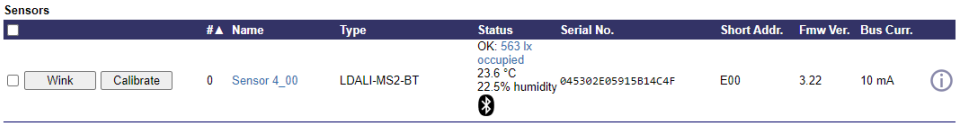


Figure 231: Commissioning Web UI: Sensor values provided by a LOYTEC LDALI-MS2-BT.

LOYTEC Devices with Sensor-Instances:

For a detailed description of LOYTEC devices with sensor instances refer to LOYTEC LDALI Devices User Manual [11]:

- LDALI-MS2 multi sensor (occupancy, illuminance, temperature, humidity).
- LDALI-MS2-BT, LDALI-MS4-BT multisensors: similar to LDALI-MS2 but with additional bluetooth enabled features.

Bluetooth Low Energy Based Functions

The LDALI-MS2-BT/LDALI-MS4-BT comes with Bluetooth Low Energy support. To be able to usethe Bluetooth based functions the related datapoints have to be enabled in the project settings (BacNet or CEA709 interface) in the LINX Configurator. The Bluetooth objects can then be found in the Bluetooth Sensors folder.

Bluetooth features:

- Asset Tracking: License LIC-ASSET required.
- Beaconing.

Bluetooth Beacons:

The LDALI-MS2-BT/LDALI-MS4-BT supports various beacon types (iBeacon, Eddystone-UID beacon or the LOYTEC-specific LWEB beacon), which can be individually configured.

- iBeacon and Eddystone-UID beacon can be used for indoor localization and indoor navigation systems.

- The LWEB beacon offers access to LWEB-802 views via the LWEB app on a mobile device (iOS/Android) and thus provides access to room control and monitoring functions.

The beacon parameters (see Table 12) are available as datapoints on LDALI controllers and LROC systems.

Type	Parameter	Description
iBeacon	UUID	Unique Identifier, 32 hexadecimal digits
iBeacon	Major	Major Number, 0-65535
iBeacon	Minor	Minor Number, 0-65535
EddyStone UID	Namespace	Unique Identifier, 20 hexadecimal digits
EddyStone UID	Instance	Instance Number, 12 hexadecimal digits
LWEB Beacon	LocalName	Beacon Name – used for Room or Segment identification, String (UTF8, 16 byte max)
LWEB Beacon	ClientConfig	defines how the LWEB app (client) shall react
LWEB Beacon	View1	Link to first LWEB view, string (UTF8, 250 byte max)
LWEB Beacon	View2	Link to second LWEB view, string (UTF8, 250 byte max)

Table 12: beacon types and parameter description

Asset Tracking and Asset Counting:

The LDALI-MS2-BT/LDALI-MS4-BT can scan for beacons in its radio range. A maximum of 32 active beacons (Eddystone UID+TLM or iBeacon) can be managed by the device. A license LIC-ASSET is required to activate this function.

The asset data of a sensor is available on data point level in LDALI and LROC controllers. The data point *AssetCount* is representing the number of active assets nearby the sensor[11] and the *AssetData* data point contains JSON-formatted data (see Figure 232, Figure 233).

[11] The sensor separates in near and far assets based on the strength of the radio signal (RSSI-limit is -75dBm)

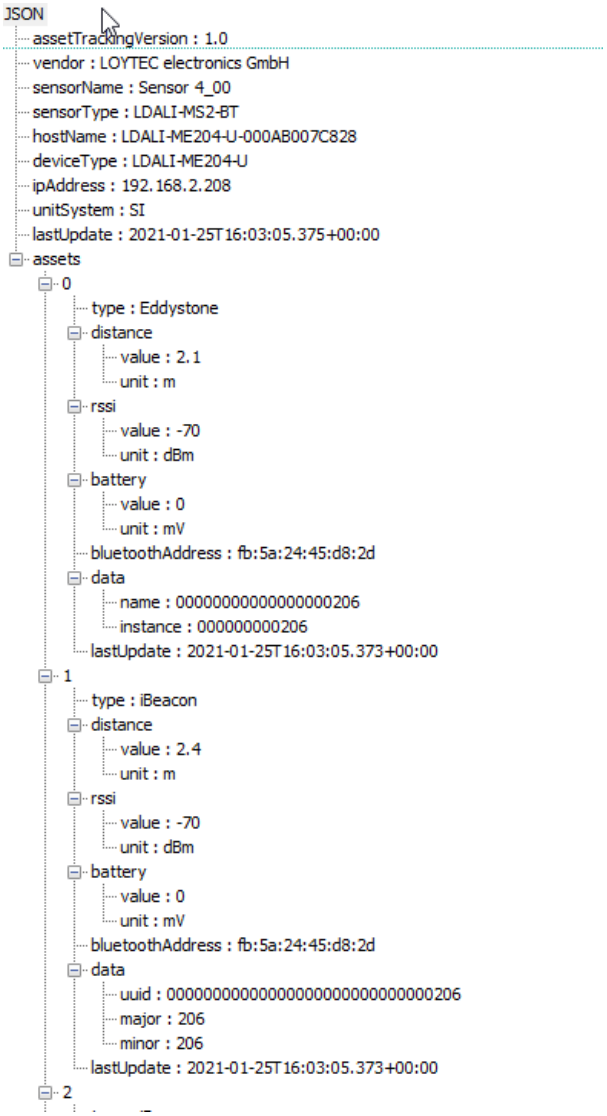


Figure 232: AssetData data point shown in JSON-Viewer

Parameter	Description
sensorName	Name of sensor
sensorType	Type of sensor
hostName	Name of the host system
deviceType	Type of the host system
ipAddress	IP address of the host system
unitSystem	Unit system used
lastUpdate	Timestamp of the last update
assets.type	Beacon type (iBeacon or Eddystone)
assets.distance	Distance to the assets

Parameter	Description
assets.rssi	Relative signal strength indicator
assets.battery	Battery voltage (only provided by Eddystone-TLM beacon, automatically linked to Eddystone-UID beacon)
assets.bluetoothAddress	Bluetooth address (6 Byte)
assets.data.UUID	UUID (iBeacon only), unique identifier, 32 hexadecimal digits
assets.data.Major	Major (iBeacon only), major number, 0-65535
assets.data.Minor	Minor (iBeacon only), minor number, 0-65535
assets.data.Namespace	Namespace (Eddystone-UID only), 20 hexadecimal digits
assets.data.Instance	Instance (Eddystone-UID only), 12 hexadecimal digits
assets.lastUpdate	Last time the beacon has been seen

Table 13: data available for each tracked asset

16.3.6 Proprietary DALI sensors and buttons

Prior to the introduction of DALI-2 input devices, different vendors were using proprietary extensions of the DALI protocol to be able to connect sensors and buttons to the DALI network. For historical reasons the following pre DALI-2 sensors using such proprietary extensions of the DALI protocol are supported[12]:

- LOYTEC LDALI-MS1

Typically these devices offer occupancy and light level sensor functionality. In addition they usually also offer occupancy and constant light controller functionality. When used with a LOYTEC DALI interface the sensor functionality can be utilized. If it is intended to also use the controller functionality the installation software of the devices vendor must be used to install and parameterize the device as this is not supported via the LOYTEC DALI interface.

The following pre DALI-2 buttons are supported[12]:

- LOYTEC LDALI-BM1
- LOYTEC LDALI-MS1 IRT

Different other proprietary pre DALI-2 devices are not supported. They cannot be commissioned or parameterized by the DALI interface of a LOYTEC DALI controller and they are not mapped to data points like DALI ballasts or supported DALI sensors and DALI buttons.

However, such devices may be operated in parallel to a LOYTEC DALI interface. In this case, they must be commissioned and parameterized using the installation software of the device's vendor.

[12] *LOYTEC electronics GmbH assumes no responsibility for any errors contained in this list. LOYTEC makes no representation and offers no warranty of any kind regarding any of the third-party components mentioned in this list. These components are suggested only as examples of usable devices. The use of these components or other alternatives is at the customer's sole discretion.*

16.3.7 Power Failure Recovery

If a ballast signals that it has come back from power failure the LOYTEC DALI master will restore the ballast's last known dim level. This behavior ensures that a consistent lighting situation is reestablished after a power failure.

16.3.8 DALI Channel Bridging

On LOYTEC DALI controllers with more than one DALI channel two or more physical DALI channels can be connected to one virtual DALI channel. This operation mode is called DALI bridging. It is used if a DALI group shall contain more than 64 ballasts, that is, more ballasts than it is possible to accommodate on one DALI channel.

In the DALI bridging mode any dim commands addressed to DALI groups and any DALI broadcasts received on one channel will be forwarded to the other bridged channels.

Note: *DALI bridging is only required if the large group shall be controlled by other DALI masters like DALI switches, buttons, or touch panels. If no such devices are used, it is recommended to use local or global connections, fan-out network variable bindings or similar methods to connect DALI groups across DALI channels instead of the bridging mode.*

16.3.9 Reducing ballast standby energy consumption

To reduce the standby energy consumed by DALI ballasts, the mains power of all ballasts on a DALI channel can be switched using an external relay, whenever they all have a dim level of 0% (OFF).

Important: ***Do not use this functionality in case the channel contains DALI emergency lights or HID lamps!***

Mains-Off handling: Local feedback

The relay must switch off power, whenever the channel feedback of that DALI channel is 0% and must switch power on otherwise. Depending on the devices interface the channel feedback is available via the following data points:

- **LDALI-10x models (CEA-709)**: *nvoCHValueFb* in the corresponding Channel Actuator object.
- **LDALI-20x models (BACnet)**: *Present_Value* of the channels feedback Analog Input object.

Note: *To use this feature on L-DALI models the mains power of all DALI ballasts on a DALI channel must be switchable via a relay controlled by a BACnet or LonMark IO-module (e.g. LOYTEC L-IOB, see Figure 233).*

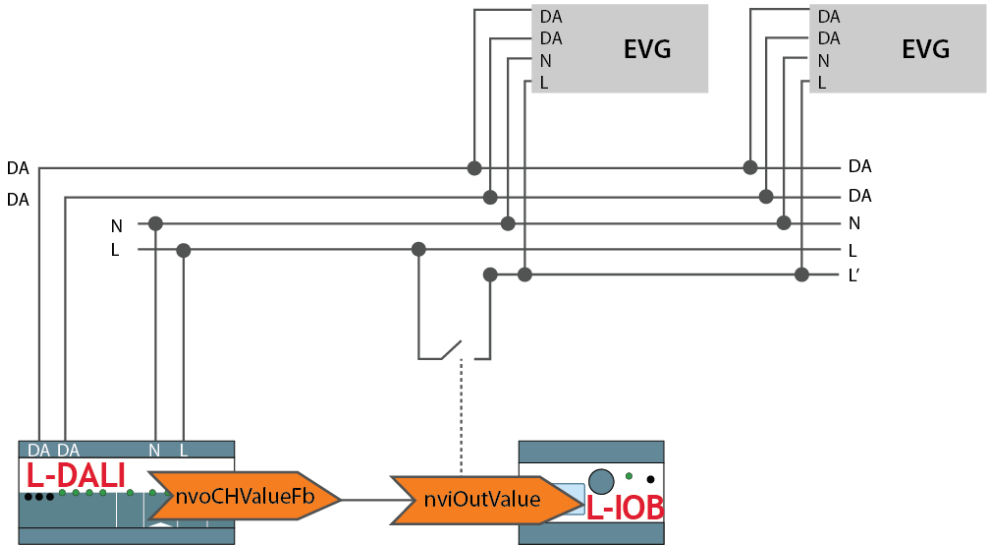


Figure 233: Wiring example for switching ballast mains using L-IOB relay output.

Important:	***The channels DALI bus power must not be switched off by the relay!***

The feature is enabled by setting the **Mains-Off handling** mode of the channel to **Local feedback** either using the LINX Configurator software (see L-INX Configurator User Manual [1]) or the Web-Interface (see Section 16.4.2.9).

Mains-Off handling: Local datapoint

In this mode additional Mains_On datapoints are used to reflect the state of the mains voltage. Thus, the channel-feedback datapoint always reflects the correct state and is not extended by the On/Off-delays. The relay must switch off power, whenever the Mains_On datapoint is "inactive" and switch on when it is "active". Depending on the device interface the following data points apply:

- **LDALI-10x models (CEA-709)**: *MainsOnx* for each channel x in the system registers DALI-folder.
- **LDALI-20x models (BACnet)**: *Mains_On* in the corresponding channel actuator object.

The feature is enabled by setting the **Mains-Off handling** mode of the channel to **Local data point** either using the LINX Configurator software (see L-INX Configurator User Manual [1]) or the Web-Interface (see Section 16.4.2.9).

On- and Off-Delay:

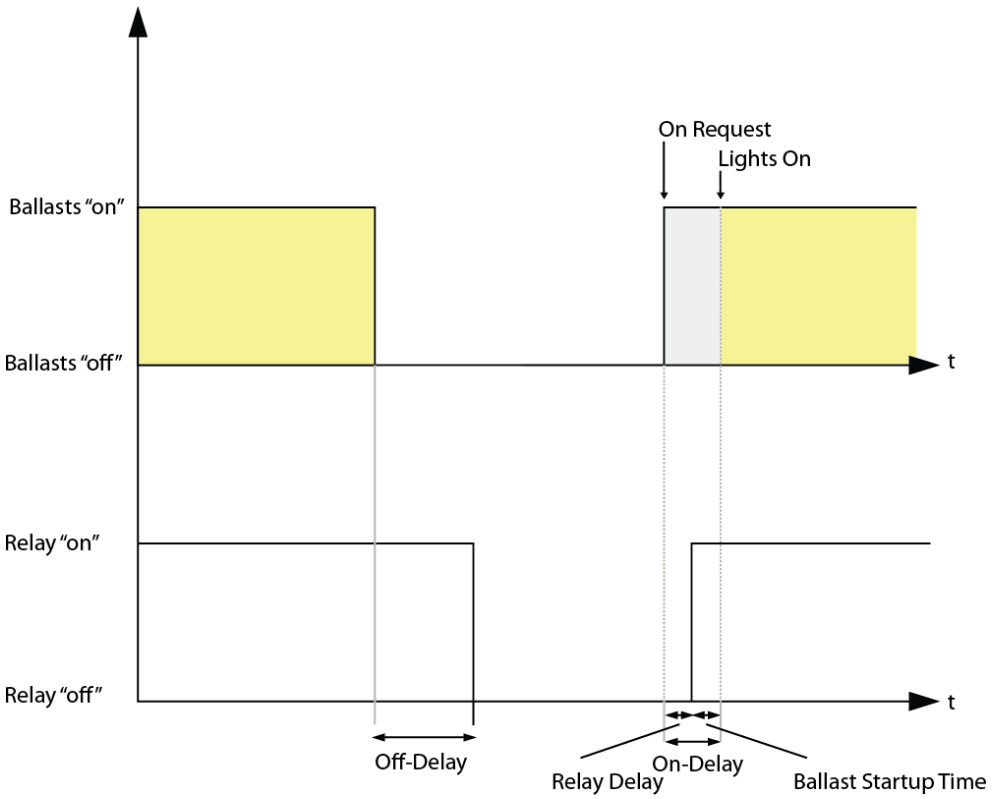


Figure 234: Timing parameters of Mains-Off handling function.

The function has two parameters (see Figure 234):

- **Off-Delay**: Delay between detection that all DALI ballasts are at 0% and entering standby mode (switching off mains). Using smaller value increases the energy saving potential, but might decrease ballast life-time.

- **On-Delay**: Typical delay between commanding the mains to be switched on (via the corresponding data point) and the time the ballast is powered up and reacting to dim commands. Modify this value if you observe all ballasts on the channel briefly switching on when mains are turned on.

Note: *The On-Delay includes the delay due to communication (e.g. via BACnet or CEA-709), the delay in the IO-module for switching the relay and the ballast startup time. The ballast startup time typically is below 500 ms (required by IEC 62386). If the On-Delay is too short, some ballasts might not be ready. They therefore will miss the startup sequence and will go to their POWER ON LEVEL. If the On-Delay is too long, switching on lights when returning from standby mode will be delayed longer than necessary.*

When **Mains-Off handling** is set to **Local feedback** or **Local data point** the current mains status is displayed on the Device Information page in the web interface together with the status of the DALI channel (see Table 14).

Symbol	Description
	Ballast mains switched on
	Ballast mains switched off

Table 14: Symbols representing ballast mains status.

Alternatively, the same functionality is offered by special DALI devices (e.g. Tridonic PS2 standby). Set the **Mains-Off handling** mode of the channel to **External** if using such a device.

Mains-Off handling: Mains_On_All

The datapoint *Mains_On_All* (ME20x-U: BACnet Port\Datapoints) or *MainsOnAll* (3E10x-U: System Register\DALI) represents the logical OR of all channel related *Mains_Onx* / *MainsOnx* datapoints on a controller which uses the local datapoint method. In other words, all individual *Mains_Onx / MainsOnx* datapoints must be inactive for the *Mains_On_All / MainsOnAll* to be set to inactive.

16.4 Web UI

16.4.1 DALI Groups

The DALI ballasts can be assigned to DALI groups as shown in Figure 235. Check the check box to add ballasts to groups, uncheck it to remove a ballast from a group. Commit changes by clicking on the **Save** button.

The lamp symbol shows whether the group is on or off. Clicking on it toggles the group between override to on, override to off and automatic mode. In the **Override** row a dim level override can be entered. Enter '--' to relinquish the override. In the **Feedback** row below the current average dim value (0%-100%) of the group is shown.

Click on the name to jump to the data point configuration page of the fieldbus object corresponding to the group. The name can be changed by editing the corresponding data point – e.g. *nciLocation* (LONMARK) or *Object_Name* (BACnet) property.

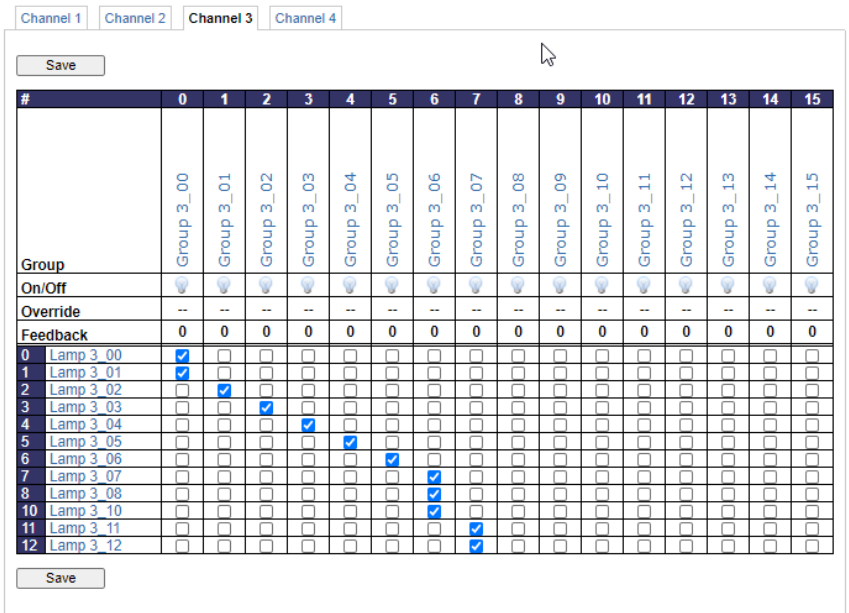


Figure 235: DALI Group Configuration.

16.4.2 DALI Installation

Figure 236 shows the initial DALI configuration page. If the device offers multiple DALI channels, the channel can be selected by clicking on the different tabs at the top of the page labeled **Channel 1**, **Channel 2**, etc.

If there is a problem with the DALI bus power on the selected channel, "**Bus supply failed**" will be displayed in the upper right corner of the tab.

The page is separated in three sections:

1. **Devices in Database**: Lists all devices on the DALI channel which were already commissioned (separated in **Lamp**s, **Sensors** and **Buttons)**.

2. **Scanned Devices not in Database**: Lists the uncommissioned DALI devices found during the last DALI scan.

3. **Unassigned Devices**: Lists the devices set up using the LINX Configurator PC software during an (optional) off-line preparation, which were not yet assigned to a physical DALI device.

The tables in each section can be sorted by clicking on the header of a column.

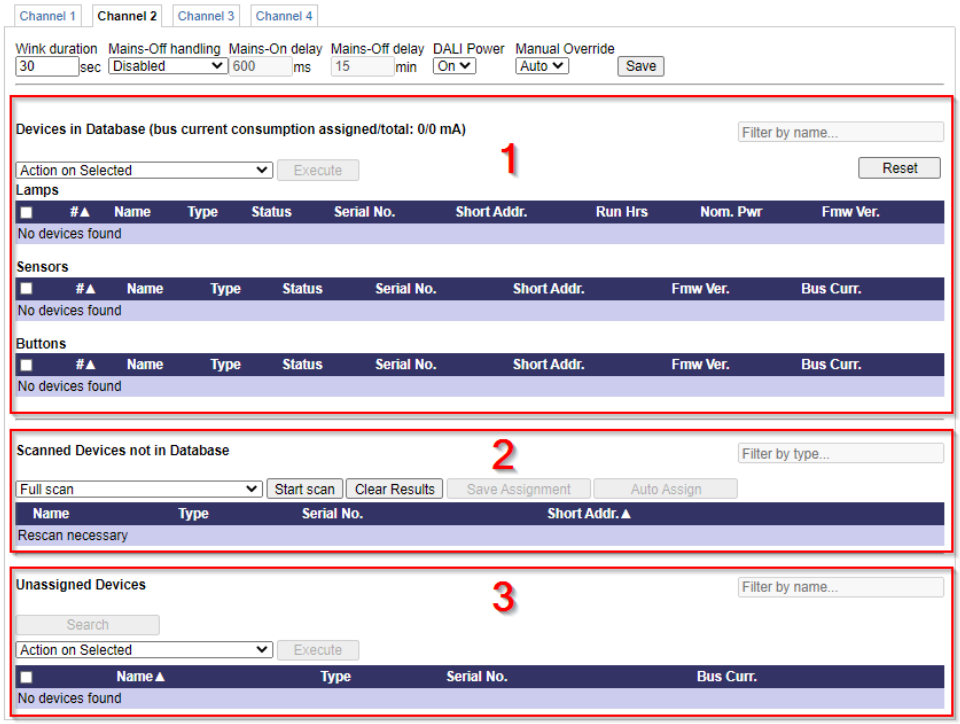


Figure 236: DALI Installation: Initial View

16.4.2.1 Installing DALI devices

To install DALI devices press the **Scan** button (select '**Full scan**' in the drop down menu). The DALI channel is scanned and the detected devices are listed under **Scanned Devices not in Database** in the middle of the page (see Figure 237). In case an error occurs see Section 16.7 for a description of the error codes and possible reasons.

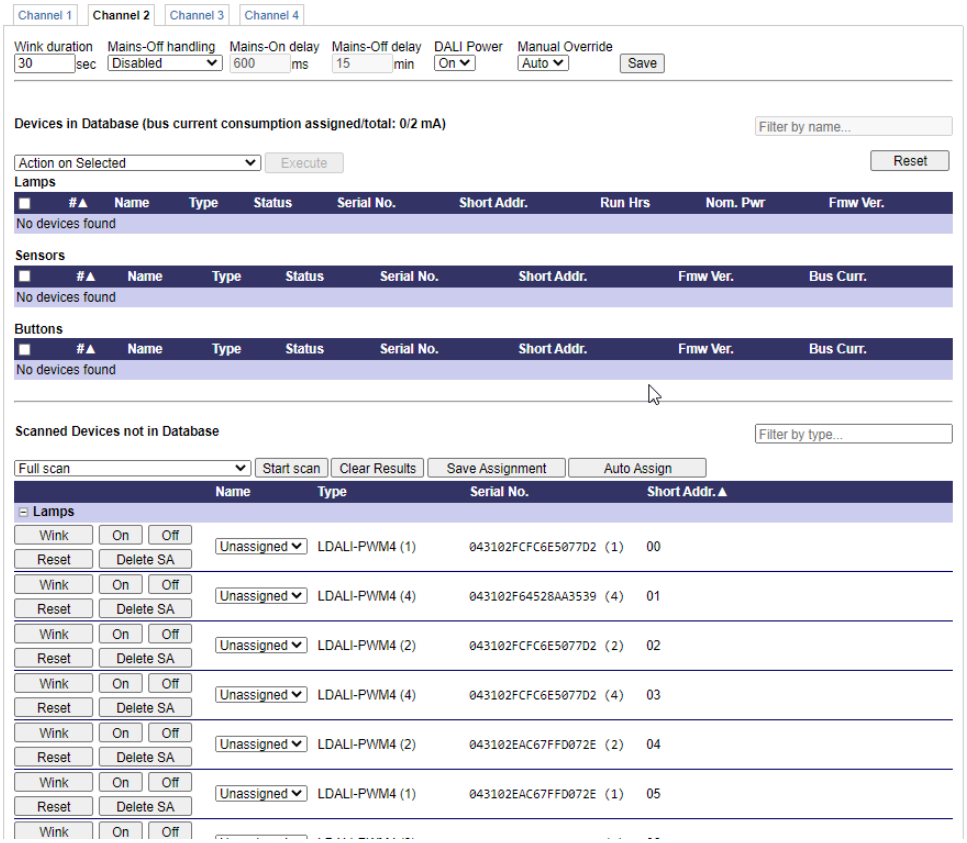


Figure 237: DALI Installation: Scan

Scan mode description:

- **Full scan:** Searching for addressed and unaddressed DALI devices
- **Partial scan (unaddressed only)**: Searching only for unaddressed DALI devices
- **Search for lost LDALI devices:** Scan and Recover LDALI devices that have been lost during or after a firmware update.

The scanned physical DALI devices have to be assigned to logical DALI devices which in turn are mapped to data points and – depending on the model – to LONMARK or BACnet objects. This can be done by one of the following ways:

- **Auto Assign**: Press the button **Auto Assign** to assign the scanned lamps, sensors and buttons randomly to the logical DALI devices.

- **Manual Assign**: For each detected DALI lamp/sensor/button a drop-down list of available objects is displayed. Select an object and press the button **Save Assignment**. To identify a DALI device press the **Wink** button. The duration for how long a device winks can be configured.

- **Assignment Wizard**: If the DALI devices have been set up during the off-line preparation steps of the LOYTEC device configuration, a search wizard can be used to locate and assign the DALI devices to the pre-configured objects in a convenient way (see Section 16.4.2.2).

If a DALI device type (e.g. emergency lighting) has been configured during the off-line preparation steps of the LOYTEC device configuration, this device type must match the device type of the assigned device. In case of **Manual Assign**, the drop-down list will only offer devices with matching device type.

Depending on the DALI devices type, devices can be identified by one or more of the following ways:

- **Wink**: Devices providing some means of visual feedback can be winked. Clicking on the **Wink** button will trigger this visual feedback. DALI ballasts are typically switched on and off for the wink process. DALI sensors and DALI emergency lights usually come with a status LED which starts blinking when the device gets winked. The duration of the wink process can be configured in the field **Wink Duration** in the upper left corner of the DALI Installation page. Once a new wink is triggered any other active wink is terminated. That is, only one device will wink at a time.

- **Physical selection**: Devices which can be physically selected can be identified by selection. A DALI button can be selected by pressing one of the buttons, an occupancy sensor can be selected by triggering occupancy. The last unassigned DALI button which was pressed is marked by a symbol, the last unassigned DALI sensor which detected occupancy is marked by a symbol.

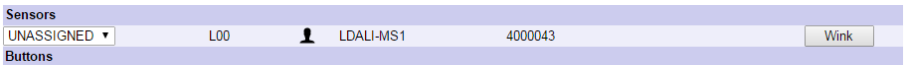


Figure 238: Sensor: Physical selection by occupancy.

If a single physical device is listed in different device type sections, because its different functions are represented as different device types (e.g. the LDALI-MS1 is listed as sensor and its IR receiver is listed as LDALI-MS1 IRT in the button section) all sub-devices are marked in case of physical selection.

- **Serial number**: Most DALI devices come equipped with a serial number. Specifically for sensors and buttons the serial number is a convenient way to identify the device. For devices, which do not allow physical selection and cannot provide visual feedback (e.g. DALI temperature sensors or relay modules) the serial number might even be the only way to identify the device. Therefore, it is highly recommended to document the serial number of a device – if known – when the device is physically installed together with the location of the installed device. For this purpose all LOYTEC DALI devices come with an additional sticker showing the serial number of the device in text and as a bar-code. This sticker can be attached to a plan or list as part of the installation process to mark the devices location in a convenient way.

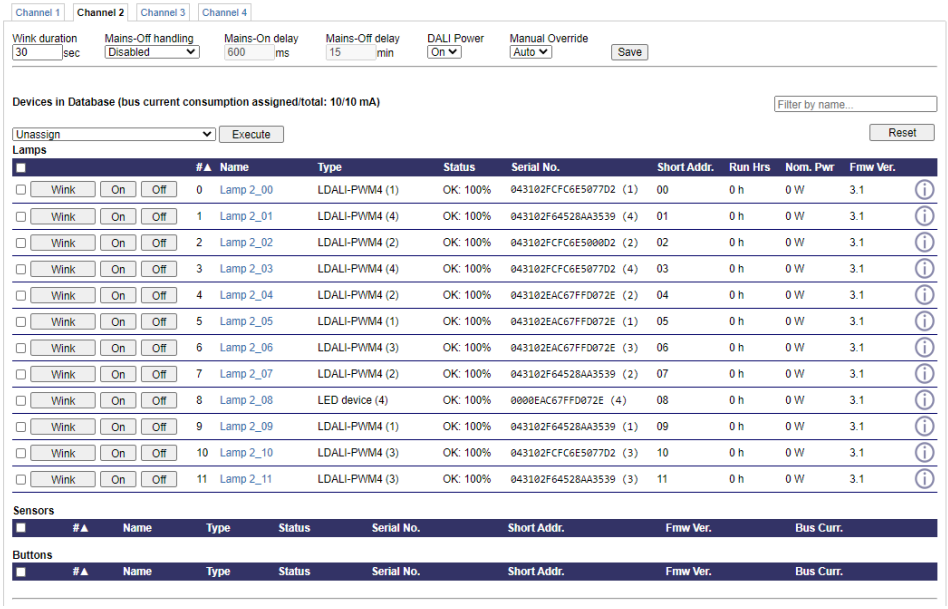


Figure 239: DALI Installation: Device Assignment

For scanned devices that are not yet assigned some additional operations are provided for troubleshooting (**Reset** and **Delete short address)**.

After the devices have been assigned, they are listed under **Devices in Database** in the upper half of the Web interface (see Figure 239). The table displays the following information:

- **Name**: This column displays the name of the DALI device. Click on the name to jump to the data point configuration page of the corresponding data point folder. The name can be changed by editing the data point containing the device name – e.g. *nciLocation* (LONMARK) or *Object_Name* (BACnet) property.

- **Type**: Displays the type of the DALI device (certified DALI-2 devices listed in the DiiA database are identified automatically).

- **Status**: This column displays the status of the DALI device and the current value. In addition the battery charge is displayed for self-contained emergency lights providing this information.

- **Bus Pwr**: Displays the bus power consumption of the device (if known). On the top of the page the sum of the bus power consumption of all devices on the channel is shown (**bus power usage assigned/total**). Make sure the bus power consumption of all devices on the channel is below 80% of the guaranteed supply current of the DALI bus power supply used. For more information on bus power consumption see Section 16.3.2 (Power consumption).

- **Nominal Power**: Displays the nominal power for DALI lamps. Some DALI ballasts report their nominal power. For DALI ballasts which do not support this feature the nominal power can be configured by the corresponding configuration property – e.g. *nciNominalPwr* (LONMARK) or *Nominal_Power* (BACnet) – of the corresponding fieldbus object.

- **Run Hrs**: Displays the run hours counter of DALI lamps. In case a lamp is replaced the run hours counter of a lamp can be reset by selecting the lamp, choosing **Reset Run Hours** from the **Action on Selected** drop down box and clicking on the **Execute** button (see Section 16.4.2.4).

- **Short Address**: DALI short address which was assigned to the device by the LOYTEC DALI master.

- **Serial Number**: This column displays the serial number of the DALI device if available. Not all DALI devices have a serial number.

- **Buttons**: Each DALI device providing some means of visual feedback can be winked. The wink duration can be configured. DALI lamps can be switched on/off manually. DALI light sensors can be calibrated (see Section 16.4.2.6).

16.4.2.2 DALI Device Search Wizard

If the DALI devices have been assigned a name using the LINX Configurator PC software during the (optional) off-line preparation and this configuration has been downloaded to the LOYTEC DALI controller a search wizard is available to assign physical DALI devices to the corresponding objects and therefore the prepared configuration:

1. Create a DALI configuration offline using the LINX Configurator software. Preconfigured DALI devices must be named to allow correct assignment once online.

2. Connect to the LOYTEC device and download the configuration (DALI configuration and Parameters).

3. Perform a network scan. In our example the result will look like in Figure 240.

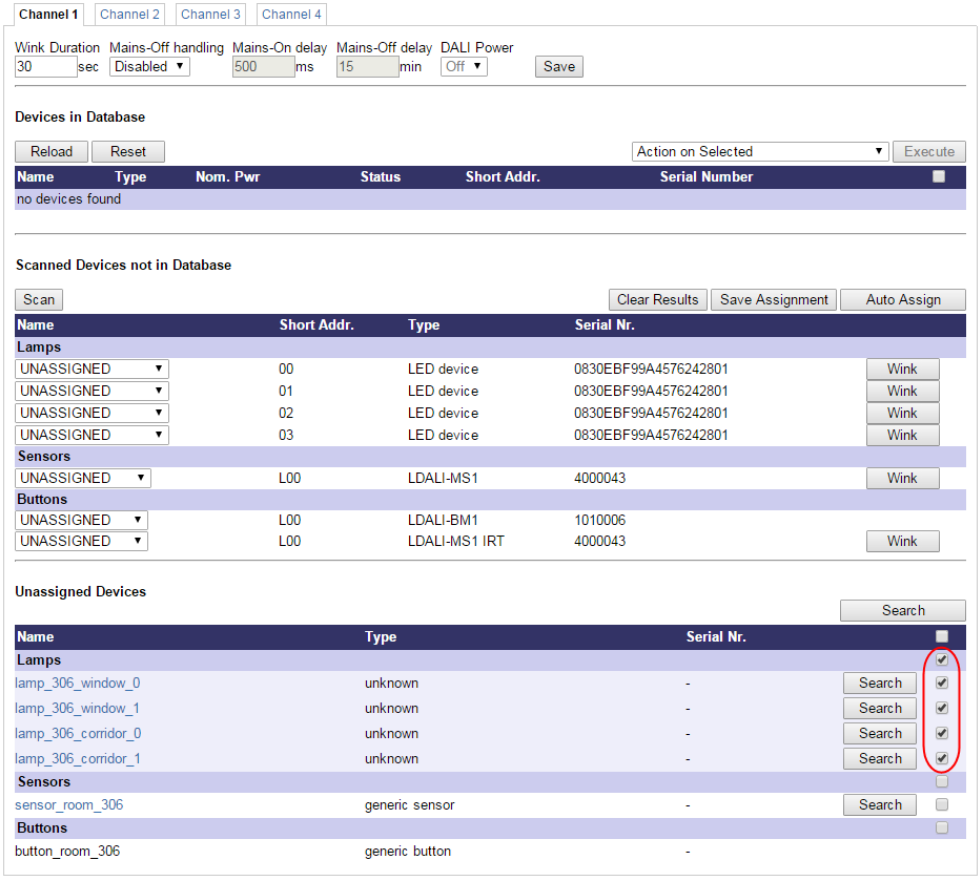


Figure 240: Scan results with unassigned devices.

4. Select the devices or device types to be identified and assigned by the search wizard by checking the check boxes on the left side of the list of unassigned devices. All devices which can provide visual feedback can be selected. And press the **Search** button on top

of the list. Alternatively the wizard can be started for a single device by pressing the **Search** button in the devices row.

5. This starts a binary search to identify the ballast(s). A dialog as shown in Figure 241 appears.

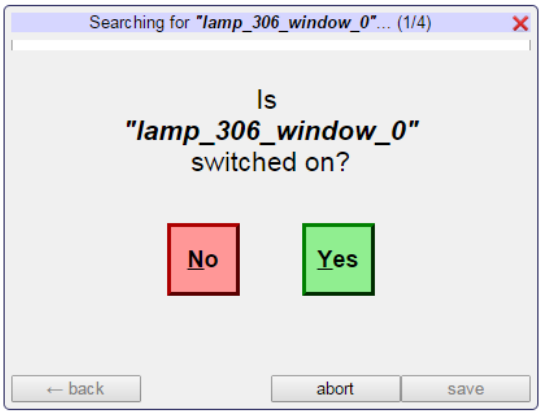


Figure 241: DALI Search Wizard.

6. Go to the luminaire/device, check whether the light is on or off and answer the question accordingly. The process is repeated until the device could be identified.

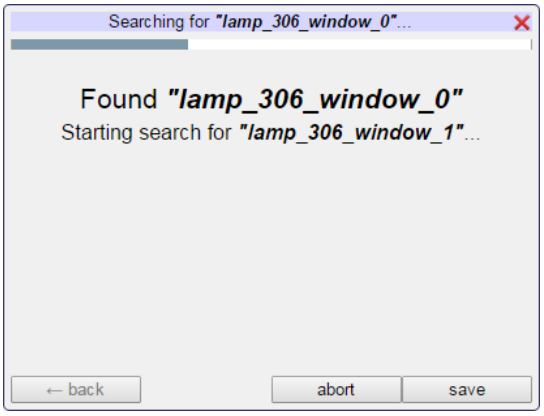


Figure 242: DALI Search Wizard: Device found.

7. A dialog as shown in Figure 242 is displayed. Then the wizard continues with the next device in the list of devices to be identified.

8. Once all DALI devices are identified press the **Save** button complete the assignment and commission the DALI devices.

For the identification during the search process DALI ballasts are switched on and off, all other devices (e.g. sensors) are winked.

16.4.2.3 Reset a DALI network

In case of a misconfigured DALI network, the **Reset** button can be used to reset the DALI configuration of all DALI devices in the network including their short address assignment. Note that if the DALI network is reset, all DALI related configuration data is lost.

16.4.2.4 Manage Devices

The devices listed under **Devices in Database** can be managed by checking the box at the right of the devices row. Then the desired function must be selected with the drop down box **Action on Selected**. Finally the **Execute** button must be pressed to perform the function. The following management functions are supported:

- **Unassign**: Clear the assignment to a logical DALI device, but keep the group assignment and the device name.
- **Wink**: Wink the selected devices (available as button only).
- **On**: Switch the selected devices on (applies only to lamps).
- **Off**: Switch the selected devices off (applies only to lamps).
- **Reset Run Hour**s, **Set Run Hours**: Reset or Set the run hours of the selected lamps (applies only to lamps).
- **Reset Energy Count, Set Energy Count**: Reset or Set the energy counter of the selected lamps (applies only to lamps).
- **Start Burn-In**: Start the burn-in mode. Some lamps require a burn-in time during which they must not be dimmed. The burn-in time is defined by the corresponding configuration property – e.g. *nciBurnInTime* (LONMARK) or *Burn_In_Time* (BACnet) – of the corresponding channel fieldbus object. During this time the lamps will only be switched to on (100%) or off (0%) but not dimmed. The remaining burn-in time is displayed in the status column (see Figure 243 for an example).
- **Abort Burn-In**: Abort burn-in mode.

	Name	Type	Nominal Pwr.	Status	Short Addr.	Serial Number		
Lamps								
0	Lamp 1_00	low voltage halogen lamp	0 W	Burn-In: 100 h 100%	00	-	Wink On Off	
1	Lamp 1_01	low voltage halogen lamp	0 W	Burn-In: 100 h 0%	02	-	Wink On Off	
2	Lamp 1_02	low voltage halogen lamp	0 W	OK: 0%	03	-	Wink On Off	
3	Lamp 1_03	low voltage halogen lamp	0 W	OK: 0%	04	-	Wink On Off	
Sensors								
0	Sensor 1_00	TRIDONIC sensor	-	OK: 52 lux, occupied	01 DIAL F	-	Wink Calibrate	

Figure 243: DALI Lamps in Burn-In Mode

- **Emergency Light: Configure Test**: Configure auto-test calendar of self-contained emergency lights. See Section for 16.4.2.7 details.
- **Emergency Light: Start Function Test**: Start function test of self-contained emergency lights supporting this function. Please refer to the documentation of the ballast vendor to determine whether the ballast supports execution of a function test. Whether the function test is executed, pending or failed is shown in the status of the selected devices. A test is pending if its execution is delayed as the current state does not permit the execution of the test (e.g. battery not fully charged, other test being performed, etc.). Test results will be stored in the appropriate emergency light test log (see Section 17.1.4).
- **Emergency Light: Stop Function Test**: Abort any function test currently executed or pending.
- **Emergency Light: Start Duration Test**: Start duration test of self-contained emergency lights supporting this function. Please refer to the documentation of the

ballast vendor to determine whether the ballast supports execution of a duration test. Whether the duration test is executed, pending or failed is shown in the status of the selected devices. A test is pending if its execution is delayed as the current state does not permit the execution of the test (e.g. battery not fully charged, other test being performed, etc.). Test results will be stored in the appropriate emergency light test log (see Section 17.1.4).

- **Emergency Light: Stop Duration Test**: Abort any duration test currently executed or pending.

- **LDALI devices firmware update**: Perform firmware update of the selected devices. The update can be performed parallel or sequential if multiple devices are selected. The unified firmware package for LOYTEC LDALI devices (LDALI RM3, RM4, RM8, BM2, MS2) is available on the website.

- **Reset converter settings**: special command to reset device type 5 specific settings (converters), e.g. LDALI RM3/4.

- **Change converter operating mode**: Change between switching and converter function (LDALI RM5/6)

- **Delete** (available in drop down menu for unassigned devices only): Delete the selected device(s) from the data base. This clears the DALI device, the group assignment, and the device name.

16.4.2.5 Replace a DALI device

If one or more broken DALI device must be replaced, the following steps must be performed:

1. Install the new device.

2. Press the **Scan** button to detect the newly installed and unconfigured device.

3. After the scan, the DALI configuration page should look similar to Figure 244. The broken device should be marked “Offline” in the Status field and the new device should be listed in the **Scanned Devices not in Database** section. Select the defective device in the drop-down list and press the **Save Assignment** button.

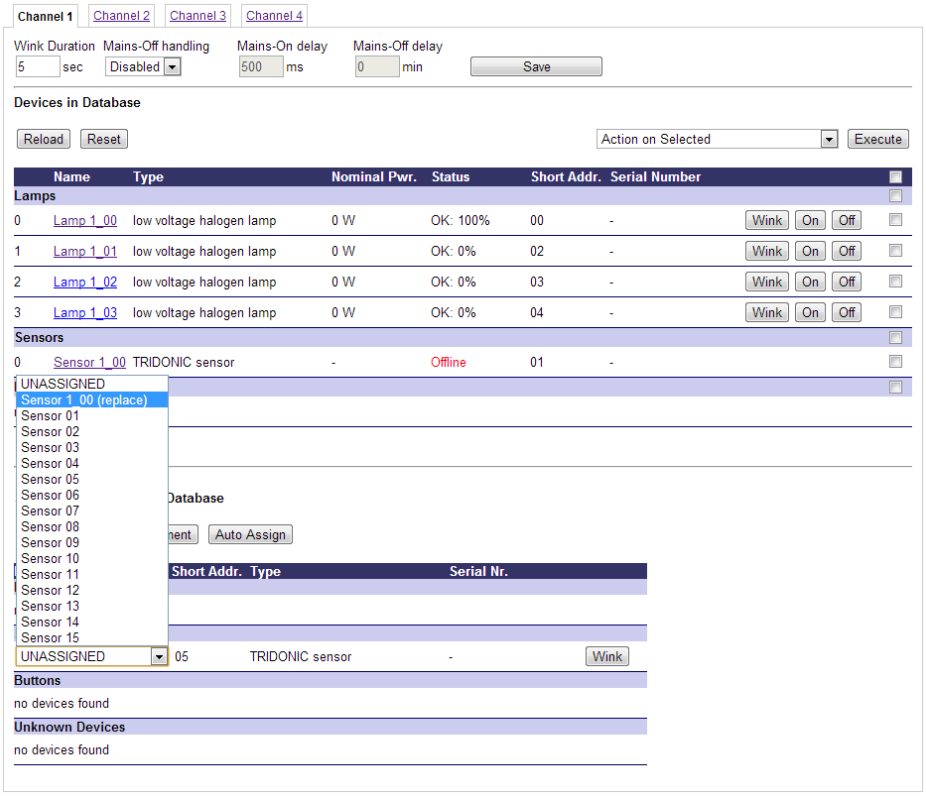


Figure 244: Replacing a defective DALI device

16.4.2.6 Sensor Calibration

CLC-applications can provide constant light behavior. To guarantee correct absolute values on reference areas like desks, workspaces etc. some teach-in is required.

Note:	*The minimum light requirements are typically prescribed by regional or national law.*

In the calibration routine the relation between a light on the ceiling (sensor) and the light on the reference area (luxmeter) has to be evaluated.

To calibrate a light sensor press the **Calibrate** button on the DALI Installation page. The DALI sensor calibration page is shown in Figure 245. The light sensor can be calibrated under up to seven different light conditions to counter any non-linearity of the sensor.

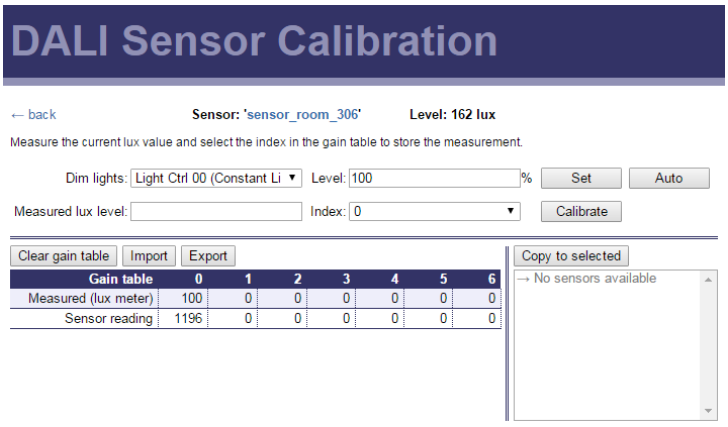


Figure 245: Sensor Calibration

To calibrate the sensor perform the following steps:

1. Measure the current lux level at the reference area (e.g. desk) using a luxmeter.

2. Optionally, the rooms light level can be adjusted. Select the appropriate DALI group or L-DALI Constant Light Controller instance located in the vicinity of the sensor in the **Dim lights** drop down box. Then enter a desired dim level in the **Level** input field and press the **Set** button. To resume normal operation press the **Auto** button.

3. Enter the measured lux level in the input field and select an unused index.

4. Press the **Calibrate** button.

5. To get the more accurate sensor reading, perform steps 1. – 3. With different light conditions.

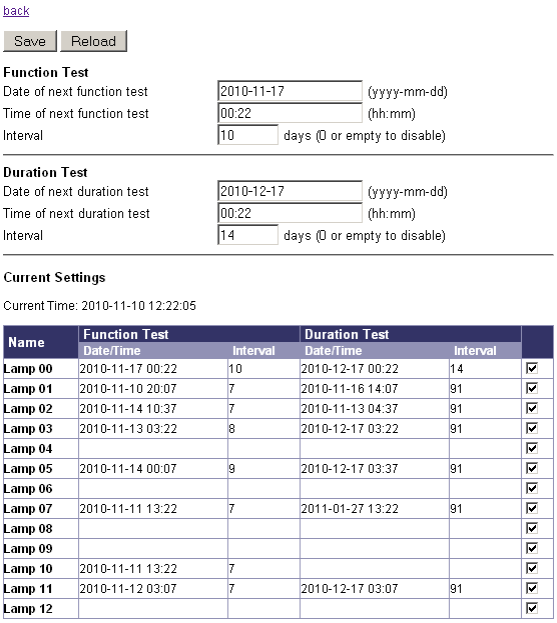
Note: *It is recommended to calibrate the sensor at least near the desired lux setpoint!*

If the sensor installation scenario is similar for multiple sensors, the calibration information can be applied to other sensor instances by selecting them in the box below the button **Copy to selected** and clicking the button. Similar the calibration information can be exported and imported by using the buttons **Import** and **Export** to transfer the data to other LOYTEC DALI controllers.

To reset the calibration table press the **Clear Gain Table** button.

16.4.2.7 Emergency Light Auto-Test Configuration

To configure the test calendar for the automatic function and duration tests of self-contained emergency lights supporting this function check the box at the right of the devices row of the DALI Installation page, choose **Emergency Light: Configure Test** from the **Action on Selected** drop-down box and click on the **Execute** button. Now the test calendar currently configured will be read from the selected devices. When done it will show a page similar to the one shown in Figure 246.


back

Save Reload

Function Test

Date of next function test 2010-11-17 (yyyy-mm-dd)
Time of next function test 00:22 (hh:mm)
Interval 10 days (0 or empty to disable)

Duration Test

Date of next duration test 2010-12-17 (yyyy-mm-dd)
Time of next duration test 00:22 (hh:mm)
Interval 14 days (0 or empty to disable)

Current Settings

Current Time: 2010-11-10 12:22:05

Name	Function Test		Duration Test		
	Date/Time	Interval	Date/Time	Interval	
Lamp 00	2010-11-17 00:22	10	2010-12-17 00:22	14	☑
Lamp 01	2010-11-10 20:07	7	2010-11-16 14:07	91	☑
Lamp 02	2010-11-14 10:37	7	2010-11-13 04:37	91	☑
Lamp 03	2010-11-13 03:22	8	2010-12-17 03:22	91	☑
Lamp 04					☑
Lamp 05	2010-11-14 00:07	9	2010-12-17 03:37	91	☑
Lamp 06					☑
Lamp 07	2010-11-11 13:22	7	2011-01-27 13:22	91	☑
Lamp 08					☑
Lamp 09					☑
Lamp 10	2010-11-11 13:22	7			☑
Lamp 11	2010-11-12 03:07	7	2010-12-17 03:07	91	☑
Lamp 12					☑

Figure 246: Emergency Light Auto-Test Configuration

For both tests – function and duration test – a test interval in days and the time and date of the next execution of the test can be specified. Click **Save** to store the new values in the devices selected by the check box at the right of the devices row.

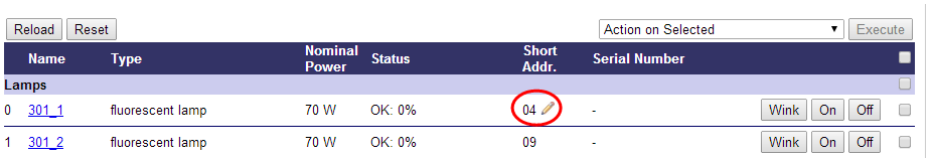
Note: *The resolution of the duration test interval is 7 days, the resolution of function test interval 1 day. Further, the time and date of the next test execution of both tests is converted to a delay with a resultion of 15 minutes[13]. The delay is calculated based on the system time and time zone of the LOYTEC DALI controller as configured in the System Configuration (see Section 3.5.1). In all cases the value entered will be rounded to the next appropriate value. For the time and date of the next test execution the result also depends on the current system time.*

Test results will be stored in the appropriate emergency light test log (see Section 17.1.4).

16.4.2.8 Changing the DALI Short Address of Devices

If required, the short address of a DALI device can be changed once it is assigned:

1. Click on the pencil, which appears next to the devices short address when moving the mouse over it.



2. Enter a valid short address in the text field that appears and press ENTER. A valid short address is in the range 0 to 63 and must be unique within one DALI channel.



Changing the short address has no effect to the assignment of the device in the LOYTEC DALI controller or any other function performed by the LOYTEC DALI controller.

16.4.2.9 Mains-Off Handling

When all ballasts on a channel are off the ballast mains can be switched. This function allows saving the standby energy consumed by the ballasts. The drop down box **Mains-Off handling** and the parameters **Mains-On delay** and **Mains-Off delay** allow configuring this function. For further details see Section 16.3.9.

16.4.2.10 Enable/Disable Internal DALI Bus Power Supply

LOYTEC DALI devices with internal DALI bus power supply show the status of the internal DALI bus power supply in the drop-down box **DALI Power** (see Figure 236). If supported by the device the internal DALI bus power supply can be enabled using the drop-down selection. Changes take effect when pressing the **Save** button to the right of the drop down box.

[13] According to the IEC 62386-202 standard the time and date of the next test execution and the test interval is stored in the emergency ballast. Thus, the ballast will execute the tests independently. As the ballast does not contain a real time clock, the time of the next test execution is stored as the delay from the current time. To facilitate entering the time and date of the next test execution, the L-DALI converts these delays to a time and date value based on the current system time.

16.4.2.11 Channel Override

By using the drop-down box **Manual Override** all lights on a channel can be overridden to **On** or **Off**. This function is very convenient to test the DALI installation. When selecting **Auto** the DALI lights are controlled via the data point interface and the controllers lighting application again. Changes take effect when pressing the **Save** button to the right of the drop down box.

16.4.2.12 Maintenance

For maintenance purposes several functions of the DALI Installation web-UI page are available for the user "operator" as well. These functions are:

- Replacing a broken DALI device (including scan).
- Reset Run Hours/Energy count.
- Start/stop burn in
- All Emergency Light functions.

All other functions are not available when logged in as "operator" user.

16.4.3 DALI Scene

Figure 247 shows the **DALI scene** page. It allows the manual configuration of DALI scenes. If the device offers multiple DALI channels, the channel can be selected by clicking on the different tabs at the top of the page labeled **Channel 1**, **Channel 2**, etc.

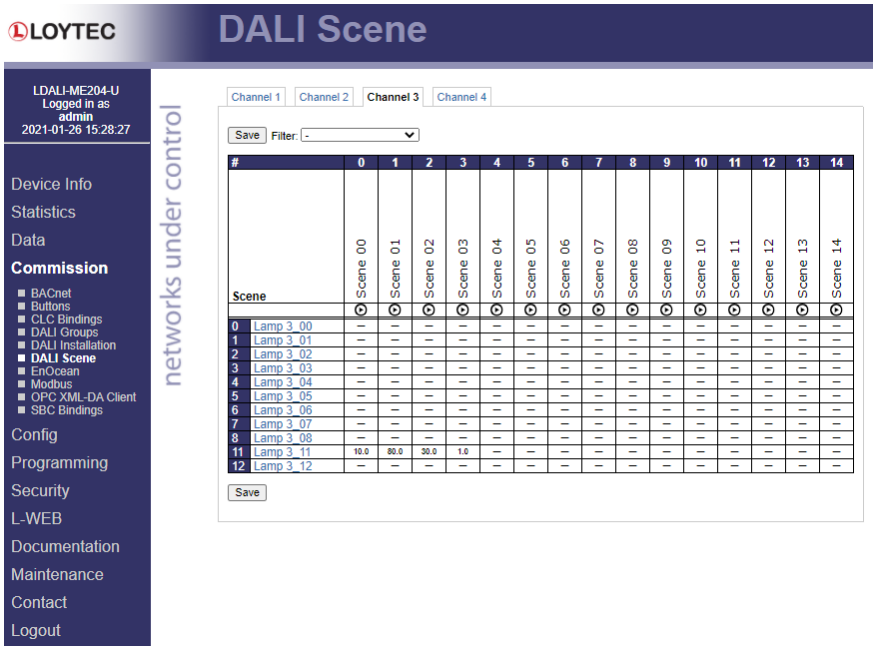


Figure 247: DALI Scene configuration.

Each DALI ballast allows to store up to 15 scenes[14]. For each scene a name can be configured. Click on the scene name to edit it. For each ballast a different dim level can be configured for each of its scenes. If recalling the scene shall not affect the ballast's dim level set the value to '--'. In addition a name can be assigned to each scene. Start editing by clicking on the name.

For ballasts supporting colour control (DALI device type 8, DT8) the scene can include colour information, too. The colour information stored with a scene is shown below the dim level. Like for the dim level a value of '--' results in no colour change if the scene is recalled.

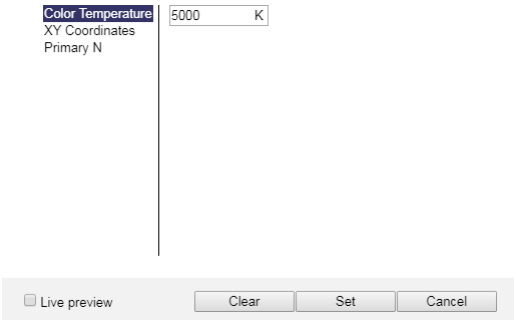


Figure 248: Scene colour selection for devices supporting colour type Tc Colour Temperature ("tunable white").

To configure the colour of a scene value click on the lower value to open the colour selection dialog (see Figure 248). The colour type(s) supported by the luminaire are displayed on the left side of the dialog. When the check box **Live preview** is checked the ballast will dim to the selected colour whenever a new value is selected.

Depending on the colour type(s) supported the colour information is configured as follows:

- **Colour Temperature**: For devices supporting *Colour Temperature* ("tunable white") only two values can be entered for each scene. The upper value is the dim level, the lower value is the colour temperature for the scene.

- **XY Coordinates**: For devices supporting *XY Coordinates* a colour picker dialog as shown in Figure 249 appears when clicking on the lower value. Either manually enter the x and y coordinate of the scene colour within CIE 1931 colour space or pick the colour by clicking in the colour diagram on the left side of the dialog. The last six colour values used are shown in the history below the colour diagram for quick reference.

[14] DALI ballasts support up to 16 scenes. Scene 15 is used by the LOYTEC DALI controller and the LOYTEC DALI buttons to store the last dim value when switching off and therefore is not available.

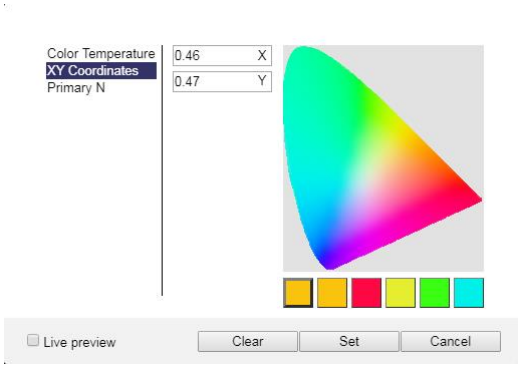


Figure 249: Scene colour selection for devices supporting colour type XY Coordinates.

- **RGBWAF**: For this type the resulting colour is composed by selecting a percentage value of 0% to 100% for the intensity of up to six predefined channels (red, green, blue, white, amber and free colour). Figure 250 shows the corresponding user interface. Note, that a specific ballasts supporting RGBWAF might only support a subset of those six channels (e.g. only red, green, blue).

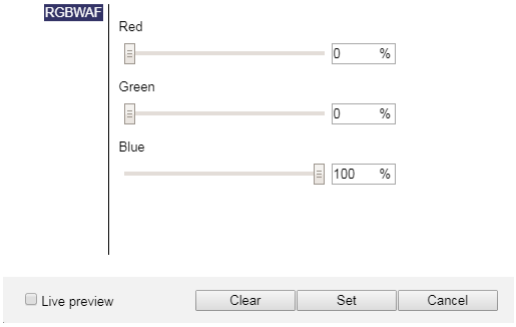


Figure 250: Scene colour selection for devices supporting colour type RGBWAF.

- **Primary N**: Similar to RGBWAF up to six colour channels are available for composing the resulting colour. However, in this case the colours represent the primary colours of the LEDs used on the luminaire. Similar to RGBWAF, a specific ballast might support less than six primary-N channels.

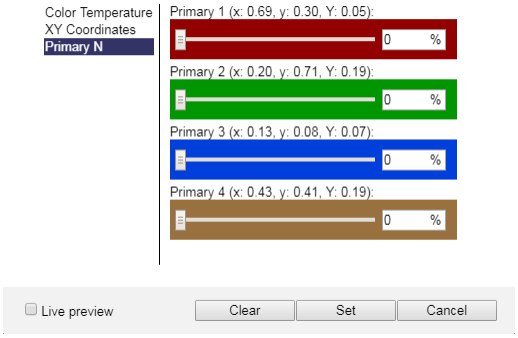


Figure 251: Scene colour selection for devices supporting colour type Primary N.

In all cases the enter '--' in the upper value if the dim level shall not be affected when the scene is recalled and enter '--' in the lower value if the colour shall not change when the scene is recalled.

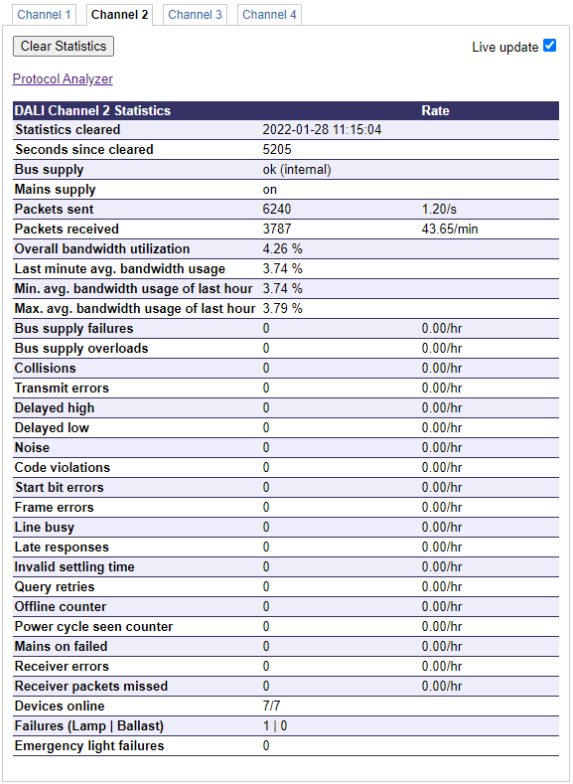
Scenes are stored for each ballast, but are typically recalled for a group. To show only the ballasts belonging to a certain group select the group in the **Filter** drop down box on the top of the page.

To test a scene configuration before saving it click on the ⊙ symbol. This will dim the ballasts selected by the current filter to the values configured for the scene.

Scenes can be recalled using DALI buttons or by the LOYTEC DALI controller via its data point interface.

16.4.4 Statistics

The DALI statistics page displays the statistics data of the DALI channels. If the device supports multiple DALI channels it is possible to switch between the channels using the tabs on the top (see Figure 252). To reset all statistics counters to zero, click on the button **Reset Channel Statistics**. The field **Date/Time of clear** will reflect the time of the last counter reset.


Channel 1 | Channel 2 | Channel 3 | Channel 4

Clear Statistics — Live update ☑

Protocol Analyzer

DALI Channel 2 Statistics		Rate
Statistics cleared	2022-01-28 11:15:04	
Seconds since cleared	5205	
Bus supply	ok (internal)	
Mains supply	on	
Packets sent	6240	1.20/s
Packets received	3787	43.65/min
Overall bandwidth utilization	4.26 %	
Last minute avg. bandwidth usage	3.74 %	
Min. avg. bandwidth usage of last hour	3.74 %	
Max. avg. bandwidth usage of last hour	3.79 %	
Bus supply failures	0	0.00/hr
Bus supply overloads	0	0.00/hr
Collisions	0	0.00/hr
Transmit errors	0	0.00/hr
Delayed high	0	0.00/hr
Delayed low	0	0.00/hr
Noise	0	0.00/hr
Code violations	0	0.00/hr
Start bit errors	0	0.00/hr
Frame errors	0	0.00/hr
Line busy	0	0.00/hr
Late responses	0	0.00/hr
Invalid settling time	0	0.00/hr
Query retries	0	0.00/hr
Offline counter	0	0.00/hr
Power cycle seen counter	0	0.00/hr
Mains on failed	0	0.00/hr
Receiver errors	0	0.00/hr
Receiver packets missed	0	0.00/hr
Devices online	7/7	
Failures (Lamp | Ballast)	1 | 0	
Emergency light failures	0	

Figure 252: DALI Statistics

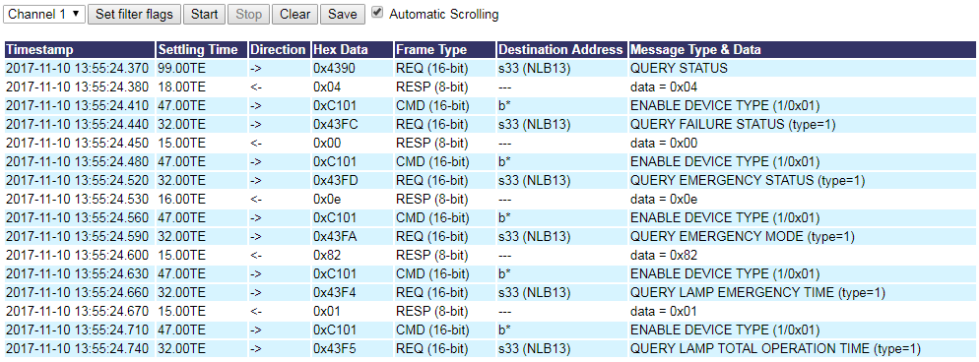
Statistics values:

- **Statistics cleared:** Timestamp of last clear/powerup
- **Seconds since cleared:** period of current statistic values
- **Bus supply:** shows the current state of the bus supply (internal/external; ok/failed/overload)
- **Mains supply:** mains supply state if mains-off handling is enabled
- **Packets sent:** Number of DALI-frames sent
- **Packets received:** Number of DALI-frames received
- **Overall bandwidth utilization:** Average bandwidth utilization since last clear/powerup
- **Last minute avg. bandwidth usage**: current bandwidth utilization (last minute)

- **Min. avg. bandwidth usage of last hour:** minimum 1 min. average in last hour
- **Max. avg. bandwidth usage of last hour**: maximum 1 min. average in last hour
- **Bus supply failures**: number of bus supply failures (>45ms bus outage, DALI "system failure")
- **Bus supply overloads:** current consumption on DALI-line is too high
- **Collisions:** number of DALI collisions (sending frame fails due collision are counted only)
- **Number of transmit errors:** sending frame fails due to error other than collision
- **Noise:** Short signal on DALI-line
- **Code violations:** Bit timing violation of receiving frames
- **Start bit errors:** start bit timing violation
- **Frame errors:** number of frame errors: invalid or not supported frame format
- **Line busy:** number of frame that could not be sent within 500ms
- **Late responses:** number of backward frames received after the max. settling time of 10.5ms
- **Invalid settling time:** number of settling time violations (settling time too short)
- **Query retries:** Number of query retries
- **Offline Counter:** Number of to-offline transitions of assigned devices
- **Power cycle seen counter:** number of power cycle seen for DALI-2 input devices
- **Mains-on failed**: number of times switching mains on failed
- **Receiver errors:** number of receiver errors due to heavy load
- **Receiver packets missed:** number of packets missed due to heavy load
- **Devices online:** number of assigned devices that are online
- **Failures (Lamp|Ballast):** number of lamp failures and control gear failures
- **Emergency light failures:** number of emergency light failures (battery or test failures)

16.4.5 Protocol Analyzer

By activating the link **Protocol Analyzer** (available in all DALI statistics tabs), the protocol analyzer page is shown as displayed in Figure 253.



Timestamp	Settling Time	Direction	Hex Data	Frame Type	Destination Address	Message Type & Data
2017-11-10 13:55:24.370	99.00TE	->	0x4390	REQ (16-bit)	s33 (NLB13)	QUERY STATUS
2017-11-10 13:55:24.380	18.00TE	<-	0x04	RESP (8-bit)	---	data = 0x04
2017-11-10 13:55:24.410	47.00TE	->	0xC101	CMD (16-bit)	b*	ENABLE DEVICE TYPE (1/0x01)
2017-11-10 13:55:24.440	32.00TE	->	0x43FC	REQ (16-bit)	s33 (NLB13)	QUERY FAILURE STATUS (type=1)
2017-11-10 13:55:24.450	15.00TE	<-	0x00	RESP (8-bit)	---	data = 0x00
2017-11-10 13:55:24.480	47.00TE	->	0xC101	CMD (16-bit)	b*	ENABLE DEVICE TYPE (1/0x01)
2017-11-10 13:55:24.520	32.00TE	->	0x43FD	REQ (16-bit)	s33 (NLB13)	QUERY EMERGENCY STATUS (type=1)
2017-11-10 13:55:24.530	16.00TE	<-	0x0e	RESP (8-bit)	---	data = 0x0e
2017-11-10 13:55:24.560	47.00TE	->	0xC101	CMD (16-bit)	b*	ENABLE DEVICE TYPE (1/0x01)
2017-11-10 13:55:24.590	32.00TE	->	0x43FA	REQ (16-bit)	s33 (NLB13)	QUERY EMERGENCY MODE (type=1)
2017-11-10 13:55:24.600	15.00TE	<-	0x82	RESP (8-bit)	---	data = 0x82
2017-11-10 13:55:24.630	47.00TE	->	0xC101	CMD (16-bit)	b*	ENABLE DEVICE TYPE (1/0x01)
2017-11-10 13:55:24.660	32.00TE	->	0x43F4	REQ (16-bit)	s33 (NLB13)	QUERY LAMP EMERGENCY TIME (type=1)
2017-11-10 13:55:24.670	15.00TE	<-	0x01	RESP (8-bit)	---	data = 0x01
2017-11-10 13:55:24.710	47.00TE	->	0xC101	CMD (16-bit)	b*	ENABLE DEVICE TYPE (1/0x01)
2017-11-10 13:55:24.740	32.00TE	->	0x43F5	REQ (16-bit)	s33 (NLB13)	QUERY LAMP TOTAL OPERATION TIME (type=1)

Figure 253: DALI protocol analyzer

A drop down box allows selecting the DALI channel to log. With the **Set filter flags** button the number of logged frames can be reduced by configuring a filter to logging only certain frame types. By pressing the button **Start** or **Stop** the protocol analyzer can be started and stopped respectively. When stopped click on **Save** to store the protocol log as a CSV file. **Clear Log** clears the log data. Check **Automatic Scrolling** to always show the newest frames by automatically scrolling to stay at the end of the page.

Each line contains the following information:

- **Timestamp** (Example: "11:08:05.284"): Local time on the device when the frame was received (end of frame).

- **Settling time** (Example: “45.00TE”): Settling time between this and the previous frame in Te (1 Te = 416.67 µs). The maximum value shown is “99TE”.

- **Direction** (Example: “->”): Frames sent by the LOYTEC DALI controller are marked by “->”, while frames received are marked by “<-“.

- **Frame type** (Example: “REQ”): Type of DALI frame. Some possible frame types are shown in Table 15.

Frame type	Description
REQ (16-bit)	DALI request (IEC 62386-102, control gear)
CMD (16-bit)	DALI command (IEC 62386-102, control gear)
REQ (24-bit)	DALI request (IEC 62386-103, control device)
CMD (24-bit)	DALI command (IEC 62386-103, control device)
RESP (8-bit)	DALI response
EVNT	DALI event (IEC 62386-103, control device)
REQ (OSRAM)	DALI request (OSRAM proprietary)
CMD (OSRAM)	DALI command (OSRAM proprietary)
EVNT (Philips)	DALI event (Philips)
???	Unknown type

Table 15: DALI frame types.

- **Destination address** (Example: “s03”): Destination address of the frame. Possible address types are:

  - **sXX:** DALI short address, where XX is the short address (00-63).

  - **gXX:** DALI group address, where XX is the group number (00-15).

  - **b*:** DALI broadcast address.

  In brackets the channel, group or – if the device is assigned - device name is shown, respectively.

- **Message type & data** (Example: “QUERY STATUS”): Shows the DALI message type and the corresponding data (argument).

16.4.6 Emergency Logs

The Emergency Logs page allows displaying log files containing detailed information on tests executed on DALI emergency light equipment. There is a log file for each group containing emergency lights and one for each channel, which contains entries from emergency lights not assigned to a group. Again, if the device supports multiple DALI channels it is possible to switch between the channels using the tabs on the top (see Figure 254). Click on the log to display its contents.

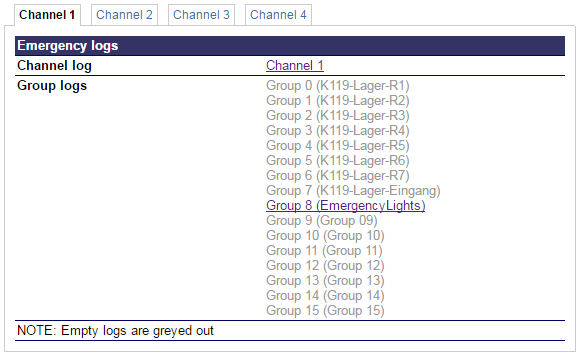


Figure 254: Choosing an Emergency Log.

As an example, Figure 255 shows the contents of an emergency log.

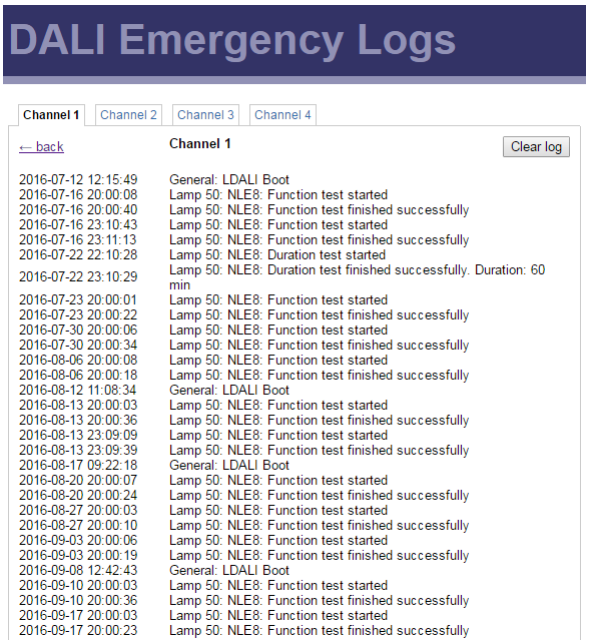


Figure 255: DALI Emergency Log.

16.5 LCD UI

The **DALI »»** menu allows executing maintenance tasks on the DALI network. The corresponding sub-menu is shown in Figure 256.



Figure 256: DALI Menu on LCD UI.

The menu item **Channel: x** (x = 1-n) shows the currently active channel. After pressing the jog dial the active channel can be changed. All other menu functions only affect the currently active channel.

The menu item **Manual Override** allows to manually override the DALI lights to either **On** or **Off**. Ensure this is set to **Auto** for control of the DALI lights via the data point interface and the controllers lighting application.

The menu item **DALI Power** allows disabling the internal DALI bus power supply.

The menu item **Assigned devices** lists all DALI devices configured on the DALI channel and allows to execute related maintenance functions (e.g. start/stop burn-in mode of selected lamps).

The menu item **Replace device** allows commissioning a new device, after it has been installed as a replacement for a broken DALI device. When using this function the complete DALI configuration of the replaced device (parameters, groups, etc.) is restored on the new device.

16.6 Troubleshooting

If you are experiencing problems with your DALI systems please follow this check list for troubleshooting:

- **Check firmware version**: Ensure you are using the latest device firmware version available via the LOYTEC website (http://www.loytec.com).

- **Test ballast wiring**: On devices without LCD UI press the ON/OFF/AUTO button once and verify all DALI luminaires connected to the channels connected to the LOYTEC DALI controller switch on, press it again and verify that they switch off. Finally press the button again to return to normal operation. On device with LCD UI perform the same test by using the Manual Override menu item in the LCD UI sub-menu DALI (see Section 16.5).



Figure 257: DALI Menu on LCD UI.

  If not all ballasts switch on and off, check the DALI and mains wiring of the affected ballasts. To check the DALI wiring, measure the voltage between the DALI terminals of the luminaire's ballast. It should be between 16 V DC and 22.5 V DC and must not fall below 14 V DC. If wiring is OK, check whether lamp or ballast are broken.

- **Check device limits**: Verify the number of ballasts does not exceed the limits given in Section 16.3.2.

- **Check cable length**: Verify DALI lines are no longer than a total of 300 m per DALI channel.

- **Check bus power supply temperature:** Verify, that the ambient temperature of the power supply is within the specified range. LOYTEC bus power supplies come with a built-in thermal overheat protection. Whether the bus power switched off due to overheating can be easily spotted by checking the statistic counter "**Bus supply failures**" (external bus power supply) or "**Bus supply overloads**" (internal bus power supply) on the DALI statistics web-UI page (see Section 16.4.4).

- **Check supported device types**: If your DALI network contains other devices than just DALI ballasts (e.g. sensors, buttons, etc.) check the L-DALI Compatibility list (see [9]) whether those devices are supported by the LOYTEC DALI controller.

- **Check Tridonic MSensor setup**: If your system contains sensors of type Tridonic MSensor please check the dial on the back of the sensor is set up correctly (position “F”).

16.7 DALI Error Codes

Table 16 lists typical error codes which can be observed during a DALI scan or device assignment.

Code (Web-UI)	Description	Possible Reason
8	Device not supported	• An unknown or proprietary (non-standard) device is connected • Old firmware version on controller
9	Cannot communicate on DALI bus.	• Problem with bus power: defective or non-standard. • Problem with DALI transceiver (RMA). Use a different port to verify.
10	Device does not respond to QUERY.	• Communication problem. Maybe due to 116mA bus power supply being too weak. • Device not fully standard compatible. • Bad wiring.
11	DALI-line busy	• DALI-line is shorted • A device is spamming the DALI-line • High DALI traffic
12	Protocol Error	• Device answers with unexpected answer to a query (maybe new or proprietary, using of old controller firmware version)
29	Cannot communicate with device. This error typically is non-critical (device is added ok).	• Communication problem. Maybe due to 116mA bus power supply being too weak. • Device not fully standard compatible. • Bad wiring.
31	Device not unique	• A firmware update of a device with multiple logical unit has been tried to be executed via several short addresses
32	Quiescent mode active	• An external application controller has forced the controller to go to quiescent mode

Table 16: DALI error codes.

17 Operating Interfaces

17.1 Common Interface

17.1.1 Schedule and Calendar XML Files

The daily schedule and calendar pattern configuration can be changed at run-time over the Web UI or the network. An alternative way to change that configuration is to download a schedule and calendar XML file via FTP onto the device. After the file has been downloaded, the new configuration becomes effective immediately. The device does not need to be rebooted. The files are located in

`/tmp/uid/sched/`*UID*`.xml`
`/tmp/uid/cal/`*UID*`.xml`

The *UID* is the unique ID of the data point. The UID can be obtained from the ID column in the data point list as shown in the Configurator software. A schedule data point with UID 107C would result in the schedule XML file '`/tmp/uid/sched/107C.xml`'. The UID remains constant for the life time of the data point even when the name or description is changed.

The content of the XML file must be compliant to the scheduleCfg schema. This schema can be found at the LOYTEC Web site. The XML documents can refer to the target namespace http://www.loytec.com/xsd/scheduleCfg/1.0/

17.1.2 Trend Log CSV File

The CSV file format for a trend log and the location of those files are defined in this section. The trend log CSV files are accessible either via their UID only, or in combination with contents of the trend log object name. The files are located in

`/tmp/uid/trend/`*UID*`.csv`
`/data/trend/`*Datapointname_UID*`.csv`

The *UID* is the unique ID of the data point. The UID can be obtained from the ID column in the data point list as shown in the Configurator software. For a more user-friendly listing of the files, the *Datapointname* contains the trend log's object name. It is truncated after 23 ASCII characters to fit the requirements of the file system. A trend CSV file for the trend object 'trend0' and the UID '107C' would result in the CSV file '`/data/trend/trend0_107C.csv`'. The UID remains constant for the life time of the object even when the name is changed.

The CSV file format for a trend log is defined in this section. The CSV file starts with a header, containing at least the first line, which specifies the CSV format (log_csv_ver). The current version is 2. The next line contains the field log_device. It has trailing fields that specify the vendor, product code, firmware version and device ID string. The Device ID String can be one of the following: (IP) 192.168.24.100, (BACnet Device) 224100, (CEA-709 NID) NID.

The log_info line specifies the fields UID and name of the trend log object. The line log_create has two fields specifying the date and time when this CSV log was generated. The

line log_capacity has two fields: the current number of log entries in the file and the log capacity.

Following are one or more lines of log_item. Each line specifies a trended data point. The first field is the index, the second the ID of the logged data point, the third the data point name. The data point name can be augmented by engineering units in square brackets. Log entries in the CSV refer to the item index to identify the data point, for which the entry was logged.

```
#log_csv_ver,2
#log_device;LOYTEC;Product Code;Firmware Version;Device ID String;Serial No
#log_info;Log-ID;Log Name
#log_create;YYY-MM-DD;HH:MM:SS
#log_capacity;filled;capacity
#log_item;index;UID;data point name [units]
```

After those lines any number of comment lines starting with a hash character '#' are allowed. One line contains the column headings. Lines that are not comments specify one log record per line, using the column information as described below. The columns are separated by commas ',' or semi-colons ';'. If commas are used as a separator, the decimal point must be a point '.'. If semi-colons are used, the decimal point must be a comma ','.

Column	Field	Example	Description
A	Sequence Number	50	The log record sequence number. This is the monotonously increasing sequence number, which is unique for each log record.
B	Source	0	Data point source identifier. Indexes into logger_entry header. For value lines in a multi-column CSV, this field indexes the first column, which has a value. For the ERROR record type, the field indexes the data source that caused the error. For LOGSTATE, TIMECHANGE records this field is not applicable and set to 255.
C	Record Type	2	The record type: LOGSTATE (0), BOOL (1), REAL (2), ENUM (3), UNSIGNED (4), SIGNED (5), NULL (7), ERROR (8), TIMECHANGE (9)
D	Error/Time Change/Log Status	1	This field is valid for records of type ERROR, TIMECHANGE, and LOGSTATUS.
E	Date/Time	2007-11-02 15:34:22	The date/time of the log record. This is in the format YYYY-MM-DD HH:MM:SS.
F	Value 0	24,5	Logged value from source 0 or empty
G	Value 1	200	Logged value from source 1 or empty
…	…		
…	Value $n-1$	5000	Logged value from source $n-1$ or empty

Table 17: Columns of the Trend Log CSV File.

There are as many value columns as value sources specified in the header. If at a given date/time more values are logged, all of them appear in the same line. If at that given time some sources did not log values, those columns are left empty. The "Source" column in a multi-value CSV refers to the first data source that supplied a value in a given line.

17.1.3 Alarm Log CSV File

The historical alarm logs are also accessible as CSV-formatted files. The alarm log CSV files are accessible either via their UID only, or in combination with contents of the alarm log object name. The files are located in

```
/tmp/uid/allog/UID.csv
/data/allog/Alarmlogname_UID.csv
```

The *UID* is the unique ID of the alarm log object. The UID can be obtained from the ID column in the data point list of the alarm log folder, similar to obtaining the UID of trend log objects. For a more user-friendly listing of the files, the *Alarmlogname* contains the alarm log's object name. It is truncated after 23 ASCII characters to fit the requirements of the file system. A trend CSV file for the alarm log object 'alarmlog0' and the UID '100C' would result in the CSV file '`/data/allog/alarmlog0_100C.csv`'. The UID remains constant for the life time of the object even when the name is changed.

The CSV format of the alarm log CSV file is identical to the trend log CSV format as described in Section 17.1.2.

17.1.4 DALI Emergency Light Test Log CSV File

When an emergency light test is performed the results are logged. These logs are available as CSV-formatted files. There is a log file for each group and one for each channel, which contains entries from emergency lights not assigned to a group. The files are located in

```
/tmp/app/grp<chnl><grp>_emerg_tst.csv
/tmp/app/chl<chnl>_emerg_txt.csv
```

Example: */tmp/app/grp104_emerg_tst.csv* contains the log information generated by all emergency lights assigned to group 4 on channel 1, */tmp/app/chl1_emerg_tst.csv* contains the log information generated by all emergency lights on channel 1 assigned to no group.

The logs contain information on all tests, no matter whether they were triggered using the data point interface (e.g. *nviEmergTest*), the Web Interface (see Section 16.4.2.4), or it was automatically started by the ballast itself due the configured auto-test calendar (see Section 16.4.2.7).

Logs can be downloaded using FTP or attached to e-mail templates (see Section "E-Mail" in the LINX Configurator User Manual [1]).

17.1.5 DALI Status CSV

The current status of all ballasts on a DALI channel is also accessible as CSV-formatted file. There is a status file for each channel. The files are located in

```
/tmp/dali<chnl>_status.csv
```

Example: */tmp/dali1_status.csv* contains the status information for all ballasts on channel 1.

The corresponding CSV file format is defined in this section. The CSV file starts with a header, containing at least the first line, which specifies the CSV format (**report_ver**). The current version is 1. The next line contains the field **report_device**. It has trailing fields that specify the vendor, product code, firmware version, the devices host name and the serial number. The **report_info** line specifies the containing the DALI channel number and name. The line **report_create** has a fields specifying the date and time when this CSV report was generated.

Following are a header line, a summary line and one line for each assigned DALI ballast. Table 18 conatins a description for each column in the CSV file. The summary line contains an aggregated status of all ballasts on the channel.

```
#report_ver;1
#report_device;LOYTEC;"LDALI-3E104";"6.0.0";"bg37u1-ldali-1";"013306-
800000143D8A"
#report_info;DALI Channel 1;"Channel 1"
#report_create;2016-03-02 12:53:31
#;Name;Type;Type Description;Status;Status Description;Last Status
Change;OK;Offline;Lamp Failure;Ballast Failure;Battery Failure;Function Test
Failed;Duration Test Failed;Battery Status (%);Last Function Test;Last
Duration Test;Last Battery Duration (min);Rated Battery Duration (min);Lamp
Emergency Time (h)
#;Summary;;Aggregated Status;0;OK;2016-02-29
16:26:31;51;0;0;0;0;0;0;100;;;0;;1
0;LA1;0;fluorescent lamp;0;OK;;yes;no;no;no;no;no;no;;;;0;0;
1;LA2;0;fluorescent lamp;0;OK;;yes;no;no;no;no;no;no;;;;0;0;
2;LA3;0;fluorescent lamp;0;OK;;yes;no;no;no;no;no;no;;;;0;0;
3;LA4;0;fluorescent lamp;0;OK;;yes;no;no;no;no;no;no;;;;0;0;
4;LA5;0;fluorescent lamp;0;OK;;yes;no;no;no;no;no;no;;;;0;0;
5;LA6;0;fluorescent lamp;0;OK;;yes;no;no;no;no;no;no;;;;0;0;
6;NLE8;1;TRIDONIC emergency lighting;0;OK;2016-02-29
16:26:31;yes;no;no;no;no;no;no;100;;;0;60;1
```

Column	Field	Example	Description
A	Index	1	Index of ballast (0-63)
B	Name	Lamp 1	Name of ballast
C	Type	0	Numeric representation of ballast type: 0 – fluorescent lamp 1 – emergency lighting 2 – HID lamp 3 – low voltage halogen lamp 4 – incandescent lamp 5 – 0-10V converter 6 – LED device 7 – switching function 8 – colour control 124 – LED with colour control 125 – HID with switching function 126 – LED with switching function 127 – LED emergency lighting 128 – PHILIPS OccuSwitch 129 – Generic ballast
D	Type Description	fluorescent lamp	Ballast type in human readable form
E	Status	0	Numeric representation of ballast status: 0 – OK 1 – Offline 2 – Lamp Failure 3 – Ballast Failure 4 – Battery Failure 5 – Function Test Failed 6 – Duration Test Failed Only the highest priority failure status is considered.
F	Status Description	OK	Ballast status in human readable form
G	Last Status Change	2016-02-29 16:26:31	Date & time of the ballast's last status change. Empty if no status change was obseverved since the DALI controller was booted.
H	OK	yes	"yes" if no error is pending, "no" if some error is pending. The summary line contains the number of ballasts without errors pending.
I	Offline	no	"yes" if the ballast is offline, "no" if it is online. The summary line contains the number of offline ballasts.
J	Lamp Failure	no	"yes" if a lamp failure is reported by the ballast, "no" if not. The summary line contains the number of ballasts reporting lamp failures.
K	Ballast Failure	no	"yes" if a ballast failure is reported by the ballast, "no" if not. The summary line contains the number of ballasts reporting ballast failures.
L	Battery Failure	no	Emergency lights only: "yes" if a battery failure is reported by the ballast, "no" if not. The summary line contains the number of ballasts reporting battery failures.

Column	Field	Example	Description
M	Function Test Failed	no	Emergency lights only: “yes” if a function test failure is reported by the ballast, “no” if not. The summary line contains the number of ballasts reporting function test failures.
N	Duration Test Failed	no	Emergency lights only: “yes” if a duration test failure is reported by the ballast, “no” if not. The summary line contains the number of ballasts reporting duration test failures.
O	Battery Status (%)	100	Emergency lights only: Battery charge level (if supported by the ballast).
P	Last Function Test	2016-02-29 16:26:31	Emergency lights only: Date & time the last function test was performed. Empty if function test was performed since the DALI controller was booted.
Q	Last Duration Test	2016-02-29 16:26:31	Emergency lights only: Date & time the last duration test was performed. Empty if duration test was performed since the DALI controller was booted.
R	Last Battery Duration (min)	80	Emergency lights only: Battery duration determined during last duration test (if supported by the ballast). Empty if duration test was performed since the DALI controller was booted.
S	Rated Battery Duration (min)	60	Emergency lights only: Rated battery duration (if supported by the ballast).
T	Lamp Emergency Time (h)	1	Emergency lights only: Number of hours the emergency light was in emergency/battery mode.

Table 18: Columns of the DALI Status CSV File.

17.2 CEA-709 Interface

17.2.1 Node Object

The L-INX and the L-GATE provide a node object conforming to the LONMARK guidelines.

- The Node Object accepts the following commands via *nviRequest*: RQ_NORMAL, RQ_UPDATE_STATUS, RQ_REPORT_MASK, RQ_ENABLE, RQ_DISABLE, RQ_UPDATE_ALARM, RQ_CLEAR_ALARM, RQ_RESET, RQ_CLEAR_RESET
- LONMARK alarming is supported via *nvoAlarm* (SNVT_alarm) and *nvoAlarm_2* (SNVT_alarm_2). This allows devices supporting the LONMARK alarm notifier profile to receive alarms generated by the device and react with a defined action (e.g., send an email). By supporting both alarm SNVTs, SNVT_alarm and SNVT_alarm_2, legacy and state-of-the-art alarm handling is supported.
- nviDateEvent (*SNVT_date_event*), nvoDateResync (*SNVT_switch*): These NVs are part of the standard LONMARK node object, if schedulers are used. If not bound, the local calendar is used. If a global calendar shall be used, both of these NVs must be bound to the respective NVs of the global calendar object.
- nviTimeSet (*SNVT_time_stamp*): When writing to this NV, the system is set, if the configure time-source is “LonMark” or “Auto” (see Section 3.5.1). The time value is interpreted as local time
- nvoSystemTemp (*SNVT_temp*): This NV can be used to poll the system temperature of the device. It does not send updates and must be polled.
- nvoSupplyVolt (*SNVT_volt*): This NV can be used to poll the supply voltage of the device. It does not send updates and must be polled.
- nvoIpAddress (*SNVT_str_asc*): This NV can be used to poll the IP address of the device. It does not send updates.

- nciEarthPos (*SNVT_earth_pos*): This configuration property can be used to set the earth position of the device. It has been implemented as an NV to make other devices send that configuration to the device over the network (e.g., from a GPS receiver).
- nviClearStat (*SNVT_switch*): When writing {100.0 1} to this NV, the channel monitor objects' statistics data are cleared.
- nvoUpTime (*SNVT_elapsed_tm*): This NV contains the elapsed time since the last reboot.

17.2.2 Real-Time Keeper Object

When the scheduler objects are enabled in the project settings, the device includes the standard LONMARK real-time keeper object. The Real-Time Keeper Object is used to synchronize the system time of multiple LONMARK compliant devices.

The object has the following network variables:

- nvoTimeDate (*SNVT_time_stamp*): Propagates the devices current system time and date (local time). It is typically bound to the nviTimeSet input network variable of the node objects of the LONMARK compliant devices, which are synchronized with the system time of the device. The update rate of the nvoTimeDate can be configured using the configuration property SCPTupdateRate (default every 60 seconds).

17.2.3 Channel Monitor Object

The Channel Monitor Object functional block is responsible for network monitoring. There is one object for each channel, the device is attached to: The channel monitor object with index 0 corresponds to the FT port of the device, while the object with index 1 corresponds to the IP-852 port of the device. If a port is not available in the current system configuration, the nvoElapsedTime is set to the invalid value and nvoPort is set to 255. The LINX-11x models do not possess a channel monitor object.

Each object has the following network variables:

- nvoPort (*SNVT_count*): Index of port associated with this Channel Monitor Object instance. Port 1 corresponds to the FT port of the device, while port 2 corresponds to the IP-852 port of the device. If the monitored port is not available in a system configuration, the value is 255. This NV is polled only.
- nvoElapsedTime (*SNVT_elapsed_tm*): Time since device powered up or since the statistics for this port where reset. The statistics can be reset with the network variable *nviClearStat* in the node object (see Section 17.2.1) or if the node is reset with a network management command (e.g., while the device is commissioned). If the monitored port is not available in a system configuration, the value is set to the invalid value. The NV is polled only.
- nvoAvgPkts (SNVT_count_32): The average number of packets per second received or transmitted via the associated channel since power-up or since the statistics for this port where reset.
- nvoIvalBandUtl (*SNVT_lev_cont*): Bandwidth utilization of associated channel during the last interval. For a smooth operation of the CEA-709 segment, the average bandwidth utilization must remain below 50 %.
- nvoIvalCrcErr (*SNVT_lev_cont*): Percentage of packets with CRC error received on the associated channel during the last interval.
- nvoIvalMissed (*SNVT_lev_cont*): Percentage of packets from the associated channel which could not be processed during the last interval.
- nvoIvalPkts (*SNVT_count_32*): Number of packets received or transmitted via the associated channel during the last interval.

- nvoTotalCrcErr (*SNVT_count_32*): Total number of packets with CRC error received via the associated channel since power-up or since the statistics for this port where reset.
- nvoTotalMissed (*SNVT_count_32*): Total number of packets from the associated channel which could not be processed since power-up or since the statistics for this port where reset.
- nvoTotalPkts (*SNVT_count_32*): Total number of packets received or transmitted via the associated channel since power-up or since the statistics for this port where reset.
- nvoMaxBandUtl (*SNVT_lev_cont*): Maximum value of *nvoIvalBandUtl* since power-up or since the statistics for this port where reset. For a smooth operation of the CEA-709 segment the average bandwidth utilization must remain below 50 %.
- nvoMaxCrcErr (*SNVT_lev_cont*): Maximum value of *nvoIvalCrcErr* since power-up or since the statistics for this port where reset.
- nvoMaxMissed (*SNVT_lev_cont*): Maximum value of *nvoIvalMissed* since power-up or since the statistics for this port where reset.
- nvoMaxPkts (*SNVT_count_32*): Maximum value of *nvoIvalPkts* since power-up or since the statistics for this port where reset.
- nvoIvalMisPre (*SNVT_count_32*): Number of missed preambles per second on the associated channel measured during the last interval. A missed preamble is detected whenever the link layer receives a preamble which is shorter then the defined preamble length. A large number in this counter is usually due to noise on the channel.
- nvoTotalMisPre (*SNVT_count_32*): Total number of missed preambles per second on the associated channel measured since power-up or since the statistics for this port where reset.
- nvoMaxMisPre (*SNVT_count_32*): Maximum value of *nvoIvalMisPre* since power-up or since the statistics for this port where reset.
- nvoChnlAlarm (*SNVT_switch*): Signals an overload alarm condition of the channel during the last statistic interval. A channel can be overloaded due to one of the following conditions:
  - The bandwidth utilization during the last statistic interval (*nvoIvalBandUtl*) exceeded the limit defined by the *SCPThighLimit1* (default 70 %) OR
  - The CRC Error Rate during the last statistic interval (*nvoIvalCrcErr*) exceeded the limit defined by the *SCPThighLimit1* (default 5 %) OR
  - The Missed Packets Rate during the last statistic interval (*nvoIvalMissed*) was not zero OR
  - The Missed Preamble Rate during the last statistic interval (*nvoIvalMisPre*) exceeded the limit defined by the *SCPThighLimit1* (default switched off).

  If an overload is detected, the network variable is set to {100, ON}. If no error occurred, it is set to {0, OFF}.
- nvoChnlAlarmRat (*SNVT_lev_cont*): Ratio between statistic intervals during which the channel was in overload alarm condition and intervals during which the channel was not in overload alarm condition since power-up or since the statistics for this port where reset.

In addition, each channel monitor object has the following SCPTs:

- SCPTifaceDesc: This configuration property contains a human-readable name of the monitored port. Possible values on the device are “CEA-709”, “IP”, or “inactive”.
- SCPTmaxSndT: Defines how often output NVs are transmitted. Exceptions are nvoPort, and nvoElapsedTime, which are polled-only.

17.2.4 Calendar Object

When the scheduler objects are enabled in the project settings, the device includes the standard LONMARK calendar object.

17.2.5 Scheduler Object

When the scheduler objects are enabled in the project settings, the device includes the configured number of standard LONMARK scheduler objects.

17.2.6 Clients Object

When the remote AST object feature is enabled in the project settings, the device includes a proprietary object, which is a container for network variables required to implement the remote object features.

For remote schedulers and calendars, *nviSchedLink* and *nviCalLink* NVs are created. For alarm clients, nviAlarm_2 NVs are created.

17.2.7 Gateway/PLC Objects

The device contains eight proprietary Gateway/PLC objects. If the device contains the IEC61131 function, the blocks are called 'PLC', otherwise they are called 'Gateway'. These are containers for all NVs which are configured on the device's CEA-709 port. They are intended for grouping NVs. When static NVs are created, they can be assigned to any of the eight gateway/PLC blocks. When creating dynamic NVs in the LNS-based tool, the NVs should be added to the gateway/PLC blocks.

17.3 BACnet Interface

17.3.1 Device Object

The BACnet interface provides one device object as shown in Table 19. The following Sections describe the device object's properties in detail, subsuming related properties in a single Section in order to provide a coherent overview.

Property Identifier	Property Datatype	Conformance Code
Object_Identifier	BACnetObjectIdentifier	R
Object_Name	CharacterString	R
Object_Type	BACnetObjectType	R
Vendor_Name	CharacterString	R
Vendor_Identifier	Unsigned16	R
Model_Name	CharacterString	R
Firmware_Revision	CharacterString	R
Application_Software_Version	CharacterString	R
Location	CharacterString	W
Description	CharacterString	W
Protocol_Version	Unsigned	R
Protocol_Revision	Unsigned	R
Protocol_Services_Supported	BACnetServicesSupported	R
Protocol_Object_Types_Supported	BACnetObjectTypesSupported	R
Object_List	BACnetARRAY[N] of BACnetObjectIdentifier	R
Database_Revision	Unsigned	R
Max_APDU_Length_Accepted	Unsigned	R
Segmentation_Supported	BACnetSegmentation	R
Max_Segments_Accepted	Unsigned	R
APDU_Segment_Timeout	Unsigned	W
APDU_Timeout	Unsigned	W
Number_Of_APDU_Retries	Unsigned	W
Max_Master	Unsigned(1..127)	R
Max_Info_Frames	Unsigned	R
System_Status	BACnetDeviceStatus	R
Device_Address_Binding	List of BACnetAddressBinding	R
Active_COV_Subscriptions	List of BACnetCOVSubscription	R
UTC_Offset	Integer	W
Daylight_Savings_Status	Boolean	R
Local_Date	Date	R
Local_Time	Time	R
Time_Synchronization_Recipients	List of BACnetRecipient	W
UTC_Time_Synchronization_Recipiens	List of BACnetRecipient	W
Time_Synchronization_Interval	Unsigned	W
Align_Interval	Boolean	W
Interval_Offset	Unsigned	W
Configuration_Files	BACnetARRAY[N] of BACnetObjectIdentifier	R
Last_Restore_Time	BACnetTimeStamp	R
Slave_Proxy_Enable[1]	BACnetARRAY[N] of Boolean	W
Auto_Slave_Discovery[1]	BACnetARRAY[N] of Boolean	W
Manual_Slave_Address_Binding[1]	List of BACnetAddressBinding	W
Slave_Address_Binding[1]	List of BACnetAddressBinding	R

Table 19: Properties of the Device Object.
[1] Only available if the device is a BACnet/IP-BACnet MS/TP router.

17.3.2 Device Name and ID

The following properties of the Device object, which are part of every BACnet object, identify the device uniquely.

Object_Identifier (Read-Only). This property, of type *BACnetObjectIdentifier*, is a numeric code that is used to identify the object. For the Device object, the object identifier must be unique internetwork-wide.

The *Object_Type* part of the *Object_Identifier* of the Device object is 8 (= DEVICE). The instance part of the *Object_Identifier* of the Device object is configurable via the configuration UI (see Section 3.5.17). The default value is 17800.

Object_Name (Read-Only). The name of the object. The value of *Object_Name* of the Device object is configurable via the configuration UI (see Section 3.5.17). For the Device object, this name shall be unique within the BACnet internetwork.

Object_Type (Read-Only). The object's type. For the Device object, the value of this property is 8 (= DEVICE).

17.3.3 Device Information

A whole set of properties provides general purpose information about the device.

Vendor_Name (Read-Only). The value of this property is "LOYTEC electronics GmbH".

Vendor_Identifier (Read-Only). A numerical value identifying the BACnet vendor. The value of this property is 178.

Model_Name (Read-Only). The value of this property is equal to the product code of the device. Examples are "LINX-200" or "LINX-221".

Firmware_Revision (Read-Only). The value of this property gives the current BACnet module version used on the device.

Application_Software_Version (Read-Only). The value of this property gives the build date and the version of the current application on the device.

Location (Read-Writable). A string intended to be used to describe the physical location of the device, e.g., "1st floor". This property can be set via the configuration UI (see Section 3.5.17). The default value is "unknown".

Description (Read-Only). A string intended to be used to describe the device's purpose. This property can be changed via the configuration UI (see Section and 3.5.17).

Protocol_Version (Read-Only). The BACnet protocol version supported by the device. The value of this property is 1.

Protocol_Revision (Read-Only). The BACnet protocol revision of the BACnet version supported by the device. The value of this property is 6.

Protocol_Services_Supported (Read-Only). A string of bits marking which BACnet services can be executed by the device. For a detailed list of the BACnet services supported, please refer to the product's PICS document.

Protocol_Object_Types_Supported (Read-Only). A string of bits identifying which BACnet object types are supported by the device. For a detailed list of supported object types, please refer to the product's PICS document.

17.3.4 Object Database

The following properties provide information about the BACnet objects contained in the device.

Object_List (Read-Only). This property holds a *BACnetARRAY* of object IDs (object type, object instance pairs), one object ID for each object within the device that is accessible through BACnet services.

Database_Revision (Read-Only). This property, of type *Unsigned*, is a logical revision number for the device's object database. It is incremented when an object is created, an object is deleted, an object's name is changed, an object's Object_Identifier property is changed, or a restore is performed.

17.3.5 Protocol Parameters

BACnet protocol parameters are accessible via the properties listed below.

Max_APDU_Length_Accepted (Read-Only). The maximal size of an APDU (Application Protocol Data Unit) accepted by the device. The value of this property is 487 if BACnet MS/TP is used and 1476 if BACnet/IP is used. When the device can act as a router between BACnet/IP and BACnet MS/TP, the value of this property is 1476.

Segmentation_Supported (Read-Only). The value of this property indicates whether and which kind of segmentation is supported by a device. The value of this property is SEGMENTED_BOTH.

Max_Segments_Accepted (Read-Only). The maximum numbers of segments accepted by a device. The value of this property is 16.

APDU_Segment_Timeout (Read-Writable). Timeout in milliseconds allowed between segments. The value of this property is 2000 milliseconds by default. On MS/TP networks, this value should be increased to 40000 (40 sec).

APDU_Timeout (Read-Writable). Time in milliseconds the device waits for an answer before retrying or giving up on a request; also see *Number_Of_APDU_Retries*. The value of this property is 3000 milliseconds. On MS/TP networks, this value should be increased to 60000 (1 min).

Number_Of_APDU_Retries (Read-Writable). The number of times the device will try to re-send a packet before giving up on a request; also see *APDU_Timeout*. The value of this property is 3 by default.

Max_Master (Read-Writable). This property is only present if BACnet MS/TP is enabled. It defines maximal MS/TP MAC number at which the device expects an MS/TP master. The value of this property is configurable via the configuration UI (see Section 3.5.17) and must be in the range 1-127.. The default value of this property is 127.

Max_Info_Frames (Read-Writable). This property is only present if BACnet MS/TP is enabled. It defines the maximal number of MS/TP packets the device can send when it holds the MS/TP token. Increasing this value will increase latency on the MS/TP network. The value of this property is configurable via the configuration UI (see Section 3.5.17). The default value of this property is 1.

17.3.6 Diagnostics

Several properties provide run-time information about the device.

System_Status (Read-Only). The value of this property is always OPERATIONAL.

Device_Address_Binding (Read-Only). This property contains a list of bindings between BACnet device instance numbers (the instance number part of the Device object ID) and BACnet addresses. This property tells a user which BACnet address the device will actually use when trying to communicate with another device known only by its device instance number. This information can be helpful when diagnosing network configuration problems.

Important! ***A BACnet address consists of the BACnet network number, which is 0 for the local network, and the BACnet MAC address of the device.***

In particular problems exist, if two or more devices in the network have been wrongly assigned the same device instance number. In this case two BACnetAddressBinding entries with the same instance number but different BACnet addresses will be listed—provided the ambiguous instance number is in some way required by the device (e.g., by a client mapping).

Important! ***Bindings between device instance numbers and BACnet addresses are only listed in Device_Address_Binding if they are actually required by a given configuration, and are currently known or ambiguous.***

Slave_Address_Binding (Read-Only). This property is only present if the device is a BACnet/IP-BACnet MS/TP router. It lists bindings between BACnet MS/TP slave instance numbers (the instance number part of the slave's Device object ID) and BACnet addresses of slaves on the MS/TP network for which the device serves as a slave proxy, see Section 17.3.10 for details.

Active_COV_Subscriptions (Read-Only). This property lists currently active COV subscriptions.. Each entry of type *BACnetCOVSubscription* provides information about the recipient address, the monitored property ID, whether notification are confirmed or unconfirmed, the remaining time of the subscription, and optionally the COV increment.

Whenever the device receives a COV subscription via one of the services SubscribeCOV or SubscribeCOVProperty, a new entry is added to the list or an existing entry is updated (re-subscription). An entry is removed from the list when a subscription terminates, either because it times out or because it was actively unsubscribed by the subscriber.

17.3.7 Date & Time

The device's time and date are exposed to the network via the following set of properties.

UTC_Offset (Read-Writable). This *Integer* value specifies the time difference between local time and UTC in minutes. The value of this property is configurable via the configuration UI (see Section 3.5.1).

Important! ***Note that UTC_Offset is relative to local time and not relative to UTC, i.e., a time zone offset of GMT+1 (Berlin, Paris, Vienna) corresponds to UTC_Offset being set to -60 (minutes).***

Daylight_Savings_Status (Read-Only). This *Boolean* value indicates whether (TRUE) or not (FALSE) daylight saving correction of the local time is currently active. The daylight saving scheme is configurable via the configuration UI (see Section 3.5.1).

Local_Date (Read-Only). The current date according to the device's clock. The value of this property can be changed via the configuration UI (see Section 3.5.1).

Local_Time (Read-Only). The current time according to the device's clock. The value of this property can be changed via the configuration UI (see Section 3.5.1).

17.3.8 Time Master

The device can serve as a BACnet time master, i.e., it can issue TimeSynchronization and UTCTimeSynchronization request on time synchronization events. A time synchronization

event occurs after rebooting, when the device's clock changes, or, if so configured, the event is generated periodically. The following properties are used to configure the time master. Use a BACnet operator workstation to write these properties over the BACnet network.

Time_Synchronization_Recipients (Read-Writable). This list of recipients will receive TimeSynchronization requests on time synchronization events. A recipient is either specified by its device ID (the object ID of its Device object), or its BACnet address. By default, this list is empty.

UTC_Time_Synchronization_Recipients (Read-Writable). This list of recipients will receive UTCTimeSynchronization requests on time synchronization events. A recipient is either specified by its device ID (the object ID of its Device object), or its BACnet address. By default, this list is empty.

Time_Synchronization_Interval (Read-Writable). The *Unsigned* value of this property specifies the time interval in minutes in which periodic time synchronization events are created. If set to zero, no periodic time synchronization events are generated.

The actual clock time at which periodic time synchronization events are generated is determined by the properties *Time_Synchronization_Interval*, *Align_Interval*, and *Interval_Offset*; Table 20 outlines how these properties interact.

Time_Synchronization_Interval	Align_Intervals	Periodc Time Synchronization Event At…
Multiple of 1440 (minutes), i.e., multiple of one day	TRUE	*Interval_Offset* minutes after midnight, every (*Time_Synchronization_Interval*/1440) days
Multiple of 60 (minutes) but *not* multiple of 1440 (minutes), i.e., multiple of one hour	TRUE	*Interval_Offset* minutes from the current* hour, every (*Time_Synchronization_Interval*/60) hours
Multiple of 1440 (minutes), i.e., multiple of one day	FALSE	*Interval_Offset* minutes from the current* minute, every (*Time_Synchronization_Interval*/1440) days
Multiple of 60 (minutes), but *not* multiple of 1440 (minutes), i.e., multiple of one hour	FALSE	*Interval_Offset* minutes from the current* minute, every (*Time_Synchronization_Interval*/60) hours
Neither multiple of 60 or 1440, but greater than zero	TRUE or FALSE	*Interval_Offset* minutes from the current* minute, every *Time_Synchronization_Interval* minutes
Zero	TRUE or FALSE	Never

Table 20: Periodic time synchronization events are parameterized by the properties *Time_Synchronization_Interval*, *Align_Interval*, and *Interval_Offset*.
* Current hour or minute refers to the hour or minute at which one of the properties *Time_Synchronization_Interval*, *Align_Interval*, and *Interval_Offset* is written, e.g., the hour or minute the device completes the boot process or one of these properties is modified via BACnet services.

By default, the value of *Time_Synchronization_Interval* is 1440 (minutes), i.e., one day.

Align_Intervals (Read-Writable). The *Boolean* value of this property determines whether or not periodic time synchronization events shall be anchored at the start of a day or hour (TRUE) or not (FALSE), provided *Time_Synchronization_Interval* is a multiple of a day (1440 minutes) or hour (60 minutes). Table 20 details on how this property influences generating periodic time synchronization events. The default value of this property is TRUE.

Interval_Offset (Read-Writable). While *Time_Synchronization_Interval* specifies the period in which time synchronization events are generated, the *Unsigned* value of this property determines the point of time in minutes within this interval at which the time synchronization event is actually triggered. If the value of *Interval_Offset* is larger than the

value of *Time_Synchronization_Interval*, the remainder of *Interval_Offset* divided by *Time_Synchronization_Interval* is used. The default value of this property is 0.

17.3.9 Backup & Restore

The following properties are related to backup & restore procedures.

Configuration_Files (Read-Only). The contents of this property is an array of object IDs of File objects that can backed-up or restored during a BACnet backup or restore procedure. Outside a BACnet backup or restore procedure, this property is empty. After a BACnet backup or restore procedure has been initiated, it contains the object ID *(File, 0)*, i.e., the File object whose instance number is 0.

Last_Restore_Time (Read-Only). The *BACnetTimeStamp* of the last restore procedure.

17.3.10 Slave Proxy

A device configured as BACnet/IP-BACnet MS/TP router, can serve as a slave proxy i.e., the device can answer Who-Is broadcast requests with I-Am responses for BACnet MS/TP slaves which, by definition, cannot initiate any communication and, thus, cannot answer broadcasts. The following properties allow configuring and monitoring the slave proxy.

Slave_Proxy_Enable (Read-Writable). For each BACnet MS/TP port, this property contains a *Boolean* that allows a user to enable (TRUE) or disable (FALSE) the slave proxy for the given port. By default, the slave proxy is enabled on all MS/TP ports.

Auto_Slave_Discovery (Read-Writable). For each BACnet MS/TP port, the slave proxy is capable of auto-detecting slaves on the MS/TP network attached to the port. This auto-detection mechanism can be disabled (FALSE) or enabled (TRUE) by changing the *Boolean* values stored in this property. Aside from auto-detecting slaves, the presence of slaves can also be manually configured in the property *Manual_Slave_Address_Binding*. By default, slave auto-detection is enabled on all MS/TP ports.

Note: *Due to bandwidth and latency limitations on MS/TP networks, the auto-discovery process may initially take up to 10min. However, once, slaves have been discovered, slaves will be quickly re-discovered after reboots or power-outs since the slave proxy caches information about slaves found on the MS/TP networks. To speed up auto-detection of slaves newly added to an existing MS/TP network for which auto-detection is enabled, simply disable and then re-enable auto-detection on given MS/TP port, i.e., set Auto_Slave_Discovery for the port to FALSE and then back to TRUE.*

Manual_Slave_Address_Binding (Read-Writable). Aside from auto-detecting slaves, see *Auto_Slave_Discovery*, slave bindings can also be manually configured via this property. Each entry of this list is a BACnetAddressBinding, i.e., a pair consisting of a slave device's instance number and its BACnet address. Note, that bindings in this list may not necessarily appear in the property *Slave_Address_Binding*, e.g., if for a given binding no physical slave is present at the given MS/TP MAC address. By default, this list is empty.

Important! ***Only use Manual_Slave_Address_Binding if the slave is not auto-detected. Note, that bindings in Manual_Slave_Address_Binding must contain the correct network number of the MS/TP network to which the slave is attached.***

Slave_Address_Binding (Read-Only). This property lists bindings of instance numbers and BACnet addresses of all slaves for which the slave proxy answers Who-Is requests. Thus, this property can be used to check if slaves have been auto-discovered or manually bound successfully. The property is also helpful in discovering network configuration issues involving slaves: If two or more slaves on the attached MS/TP networks have been erroneously assigned the same device instance number (the instance number of the slave's Device object), the given instance number will be listed accordingly often in this property.

17.3.11 Client Mapping CSV File

Client functionality for the BACnet server objects can be defined by so-called *client mappings*. These mappings basically specify whether present value properties shall be written to or polled from the BACnet network, and what the destination address and objects are. These definitions can be downloaded as a CSV file onto the device using FTP.

The CSV file must be named 'bacclnt.csv' and stored in the directory '/var/lib/bacnet' on the device. The file is read when the device boots. If any errors occur they are reported in '/tmp/bacclnt.err'.

The column format is shown in Table 21. Lines beginning with a hash ('#') sign are comment lines. The example values in Table 21 setup a client mapping named "Lamp Room 302", which writes (mapping type 2) the present value of the local object AI,4 to the remote object AO,1 on the device with the instance number 17801.

Column	Field	Example	Description
A	Description	Lamp Room 302	User-defined description of this client mapping. Can be left empty. Don't use commas or semi-colons in the text!
B	Local Object-Type	AI	The BACnet object type of the local server object (AI, AO, AV, BI, BO, BV, MI, MO, MV, ACCM, LOOP)
C	Local Object Instance Number	4	The object instance number of the above object.
D	Remote Device Instance	17801	The device object instance number of the remote BACnet device
E	Remote Object-Type	AO	The BACnet object type of the remote server object (AI, AO, AV, BI, BO, BV, MI, MO, MV, ACCM, LOOP)
F	Remote Object Instance Number	1	The object instance number of the above object.
G	Map Type	2	Defines the type of the mapping: 0=Poll, 1=COV, 2=Write, 3=Value
H	Interval	60	Defines the poll interval in seconds for poll/value mappings and the COV lifetime in seconds for COV mappings. Note: In previous versions this column was also used to specify the write priority for write mappings. This usage of column H is deprecated and column I should be used to specify priority.
I	Priority	8	For write and value mappings this defines the write priority (1..16). Omit this field or set it to '-1' to write w/o priority.
J	Local Property ID	45	Specifies the property ID of the local object, which is mapped to the remote object. If omitted, the Present_Value of the local object is mapped.
K	Remote Property ID	45	Specifies the property, which is written/read on the remote object. If omitted, the remote property ID is the Present_Value.

Table 21: CSV Columns of the BACnet Client Mappings File.

17.3.12 EDE Export of BACnet Objects

The BACnet server object configuration of the device is accessible as a set of CSV files following the EDE format convention. They can be downloaded via FTP from the directory '/data/ede' on the device. The files are

- lgate.csv: This is the main EDE sheet with the list of BACnet objects.

- lgate-states.csv: This is the state text sheet. For each state text reference in the main sheet, a line contains the state texts for this multi-state object.
- lgate-types.csv: This is the object types text sheet. The file contains a line for each object type number. Note, that lines for standard object types can be omitted.
- lgate-units.csv: This is the unit text sheet. The file contains a line for each engineering unit enumerator value. Note that lines for standard units can be omitted.

17.4 SNMP Interface

The Simple Network Management Protocol (SNMP) is a common protocol for monitoring and managing devices. SNMP is an "Internet-standard protocol" and is defined by the Internet Engineering Task Force (IETF). It is typically used in IT environments for server, network and supply management and monitoring.

SNMP allows querying status and statistics data from devices and also allows devices to alarm network management applications using SNMP traps. A managed device contains an SNMP agent which communicates with a management system using UDP. The SNMP agent holds collects and provides its data items in a tree. The data provided by an SNMP agent is defined by Management Information Bases (MIBs). These define the names and data types of the management data. Every data item is assigned an object ID (OID). A device can support an arbitrary number of MIBs, such as CPU statistics or network traffic statistics.

17.4.1 SNMP Features

LOYTEC devices supporting SNMP share these common features:

- Read-only access for SNMP version 2C and 3
- Standard MIBS: SNMPv2-MIB, SNMPv2-SMI, RFC1213-MIB, IF-MIB, IP-MIB, DISMAN-EVENT-MIB, HOST-RESOURCES-MIB, SNMP-FRAMEWORK-MIB, SNMP-MPD-MIB, SNMP-USER-BASED-SM-MIB, SNMP-VIEW-BASED-ACM-MIB,
- Option to expose OPC data points to SNMP.
- Option to create a device-specific MIB file.
- Option to send traps to a management system.

17.4.2 Configuration

The SNMP agent can be configured in the Web UI and in the configuration software. Figure 258 shows the Web interface. The settings in the configuration software are similar.

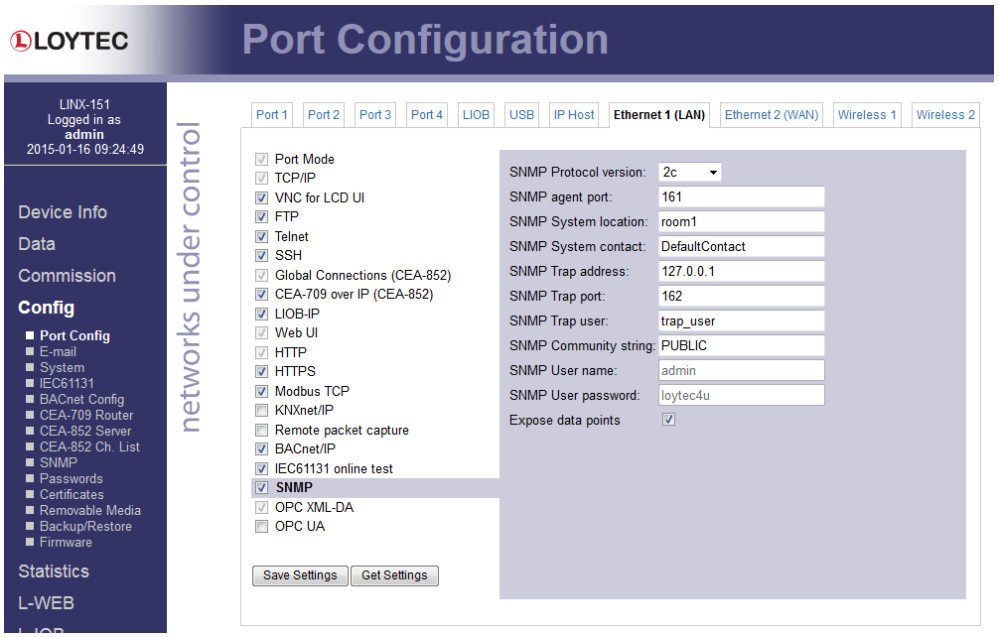


Figure 258: SNMP configuration page

The following settings are used to configure the SNMP agent:

- **SNMP Protocol version**: This setting selects between version 2C, 3 and 2C+3. Protocol version 2C is more common, but lacks encrypted authentication.
- **SNMP agent port** This select the UDP port on which the SNMP agent listens. It is recommended to keep this port at its default setting, port 161.
- **SNMP System location:** This defines the value of the `SNMPv2-MIB::sysLocation` OID. It is used to locate a device via SNMP.
- **SNMP System contact:** This defines the value of the `SNMPv2-MIB::sysContact` OID. It is used to identify the responsible contact persion for the deivce
- **SNMP Trap address:** This setting defines the destination IP address to which traps (alarms) are sent.
- **SNMP Trap port:** his setting defines the destination UDP port to which traps (alarms) are sent.
- **SNMP Trap user:** This setting defines the user name when sending traps (SNMP v3)
- **SNMP Community string:** This defines the (read) community string used for SNMP v2c.
- **SNMP User name:** This defines the user name required to access the SNMP agent (SNMP v3)
- **SNMP User password:** This defines the user password required to access the SNMP agent (SNMP v3).
- **Expose data points:** This switch allows to access data points exposed to OPC also to be accessed via SNMP.

17.4.3 Exposing Data Points to SNMP

The SNMP agent allows exposing data points to SNMP. It considers every data point which is exposed via OPC also to be exposed via SNMP.

As SNMP has several restrictions on what can be represented, the following mappings are made:

- **Binary data points**. Binary data points are mapped to the INTEGER type. FALSE is mapped to 0, TRUE is mapped to 1 and an invalid value is mapped to -1.
- **Analog data points**: SNMP has no standard way to represent floating point values, so their values are mapped to the STRING type. A value of "--" identifies an invalid value
- **Multistate data points**: Multistate data points are mapped to the STRING data type. Their values are represented by the multi-state text labels.

SNMP variable names have to be unique within their MIB, so data points with the same name in different folders are made unique by the following name scheme: `dpNNNNXUUUUUUUU`, e.g. `dpFreeMemoryX00000003`. NNNN is the data point name with all forbidden characters removed (only a-z, A-Z and 0-9 is allowed). UUUUUUUU is replaced with the unique ID of the data point.

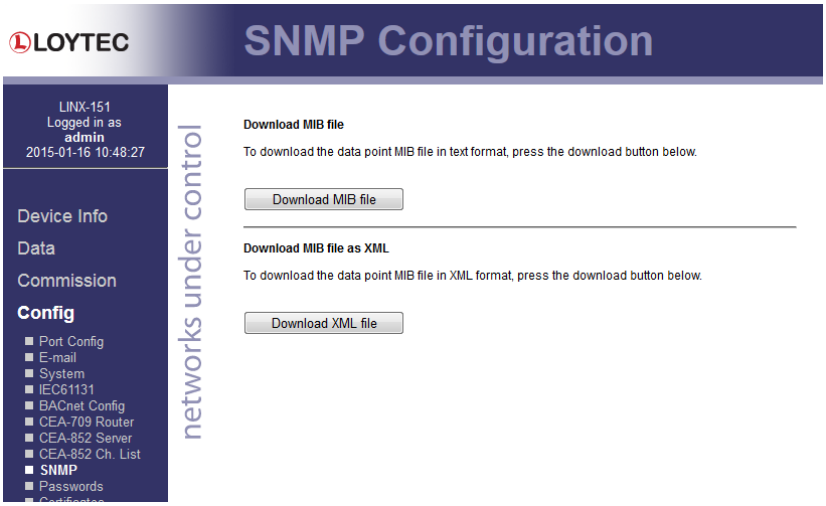


Figure 259: Downloading device-specific MIB files

Figure 259 shows the Web UI page which allows downloading the device specific MIB file. The "Download MIB file" buttons generates a MIB file which can be used by a network management tool. The "Download XML file" button generates an XML-encoded representation of the MIB contents.

Note that the MIB files are dependent on the data point configuration, so that changes in the data point configuration will change the MIB contents.

17.4.4 Alarming

The SNMP agent can send a trap if an alarm occurs in a generic alarm server. To connect the generic alarm server to the SNMP agent, it has to report to the special SNMP technology alarm server. The configuration steps in the **Create Alarm Server** dialog are shown in Figure 260.

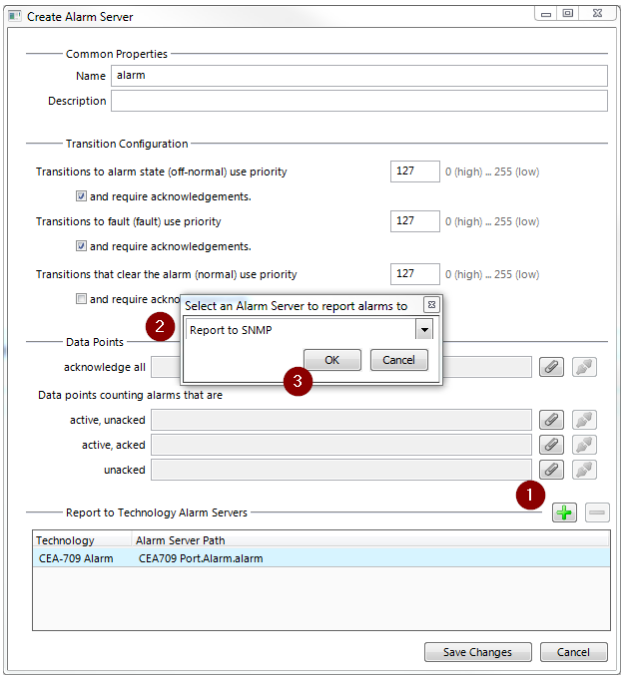


Figure 260: Report to SNMP

17.4.5 SNMP Security

As SNMP provides access to internal device information which could be exploited for an attack, SNMP should be used only in internal, non-critical environments.

SNMP Version 2C uses unencrypted authentication and payload. The community string is transmitted in clear text and can be easily extracted from captured network traffic.

SNMP Version 3 supports encrypted authentication and payload encryption. LOYTEC devices support only authentication. The password is not transmitted in clear text then.

LOYTEC devices do not support write accesses via SNMP.

18 Network Media

18.1 FT

The device's FT port is fully compatible to the parameters specified by LONMARK for this channel. FT ports can also be used on Link Power (LP-10) channels. However, the device does not provide the power supply for Link Power channels.

When using the Free Topology Segment feature of the FT, only one termination (Figure 261) is required and can be placed anywhere on the free topology segment. Instead of building the termination, one can order the L-Term module (LT-33) from LOYTEC, which can be used to properly terminate the bus.

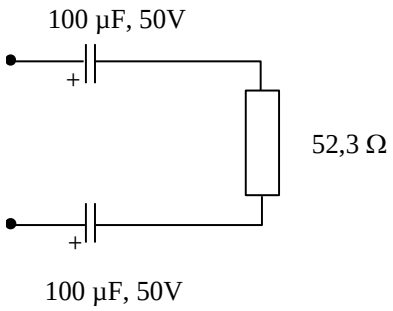


Figure 261: FT Free Topology Termination.

In a proper bus topology, two terminations are required (Figure 262). These terminations need to be placed at each end of the bus. Here, also L-Term modules can be used at either end.

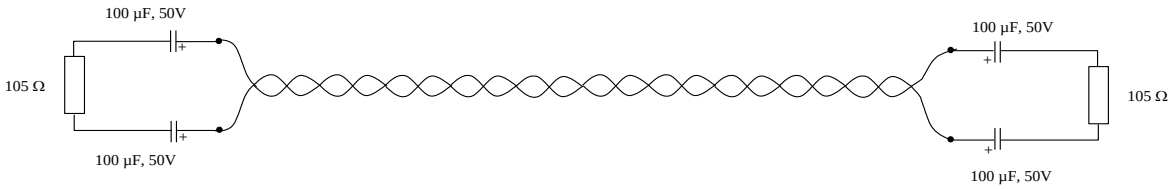


Figure 262: Termination in an FT Bus Topology.

18.2 M-Bus

The device uses the RS-232 console interface for the connection to an external M-Bus transceiver (repeater). The M-Bus specifies no special topology requirement, though it is not advised to use a ring topology. A maximum of 250 M-Bus slave devices can be connected to the bus, in fact, the external bus transceiver can have a lower limit of connected devices. Please refer to the datasheet of the transceiver used for more detailed information. The usual cabling is a standard telephone wire (JYStY N*2*0.8 mm). The maximum distance between

a slave and the repeater is 350 meters at Baud rates from 300-9600 Baud; by limiting the lower Baud rates and using fewer slaves, this limit can be increased. Additionally, it must be ensured that the bus voltage does not fall below 12 V. The maximum cable length of the system must not exceed 1000 m (maximum cable capacitance of 180 nF).

18.3 Modbus RS-485

The Modbus RS-485 port of the device is an electrical interface in accordance to EIA-485. The topology of the Modbus RS-485 consists of a trunk cable, along which the devices are connected either directly or via short derivation cables. Without repeater a maximum of 32 slave devices with full RS-485 unit load can be connected to the bus. If RS-485 transceivers of slave devices are assured to pose only 1/2, 1/4 or even 1/8 unit load, a maximum of 64, 128, 256 slaves can be operated without a repeater, respectively. Alternatively, a repeater may be used. In any case, a maximum of 247 slaves can be addressed.

Each Modbus RS-485 network segment must be properly terminated with an LT-04 network terminator connected at each of the two ends of the segment media. Some Modbus slave devices might require a biasing terminator to guarantee a defined level on the wire when being idle. Use an LT-B4 instead of the LT-04 on one end in this case. Figure 263 shows an example Modbus RS-485 network configuration including biasing network termination.

The maximum length of the cabling depends on the Baud rate used. Without repeater a maximum length of 1000 meters is possible at 9600 Baud. According to the Modbus standard the derivation cabling must never exceed 20 m.

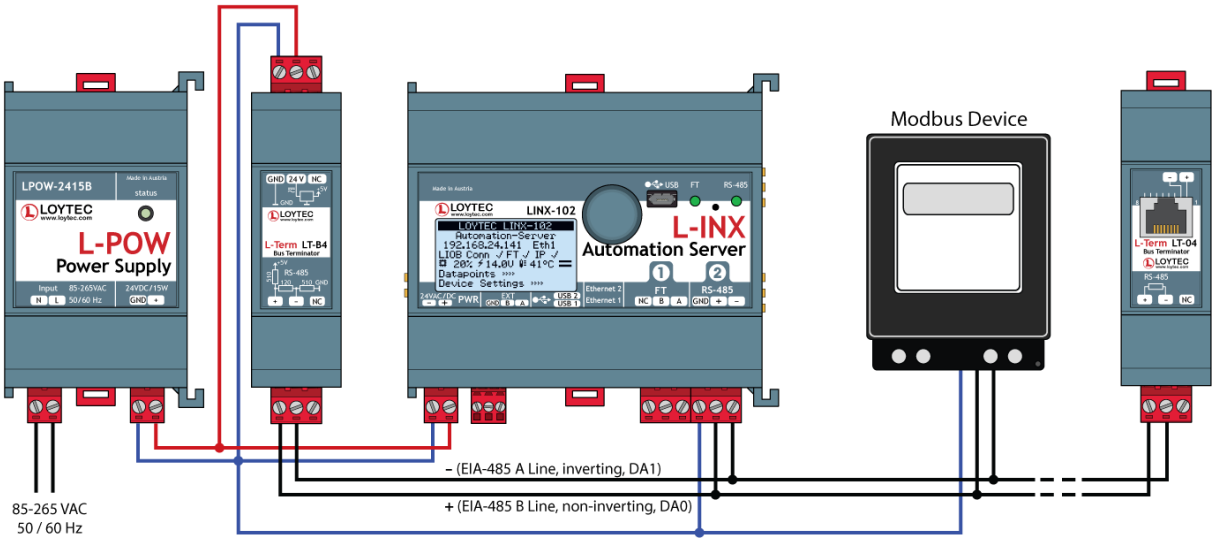


Figure 263: Modbus RS-485 network

18.4 MS/TP

MS/TP is an RS-485 protocol and usually needs three wires (negative, positive, and reference). Polarity must be connected correctly. When using 2-wire MS/TP, earth ground must be connected to the negative terminal of the power supply. Never connect the positive terminal of the power supply to earth ground! Each MS/TP network segment must be properly terminated. Use an LT-04 network terminator connected at each of the two ends of the segment media.

The RS-485 transceiver of the device represents a full-load on the RS-485 bus. Consequently, a minimum of 31 devices are supported on the MS/TP channel. More devices may be

possible, if they represent half-load or quarter-load. Please consult the third-party documentation. If more MS/TP devices need to be connected, use an RS-485 repeater to separate them electrically.

Logically, the MS/TP bus supports up to 255 devices. Each MS/TP device must be assigned a unique MAC address. Up to 127 MS/TP masters can be connected. Make sure, that the Max_Master setting includes the highest MS/TP master MAC address.

For operation of some slower devices on the MS/TP network it is recommended to set the following properties of the device object to fine-tune communication on the network:

- APDU_Timeout = 60000 (1 min).
- APDU_Segement_Timeout = 40000 (40 sec).
- Optionally, disable MS/TP slave proxy if not needed in order to optimize bandwidth usage: Slave_Proxy_Enable = { False }.

18.5 Physical Connection of Inputs

18.5.1 Connection of Switches

On- or off-switches can either be connected to the DIs (Digital Inputs) or to the UIs (Universal Inputs) in digital interpretation.

18.5.1.1 Switch connected to a DI

A switch can be directly connected to a digital input as shown in Figure 264.

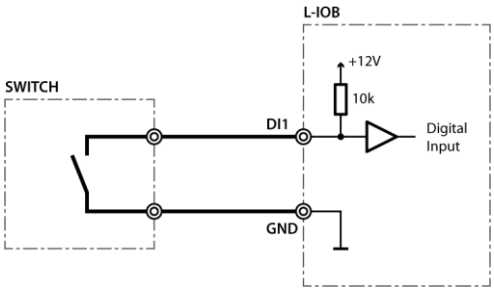


Figure 264: Switch connected to DI

The digital inputs (DI) recognize the following digital signals according to the connected resistance (switch):

Resistance of Switch	Status
< 6.8 kΩ	Closed Switch
> 10 kΩ	Open Switch

18.5.1.2 Switch connected to a UI

A switch can be directly connected to a universal input with signal type resistance as shown in Figure 265.

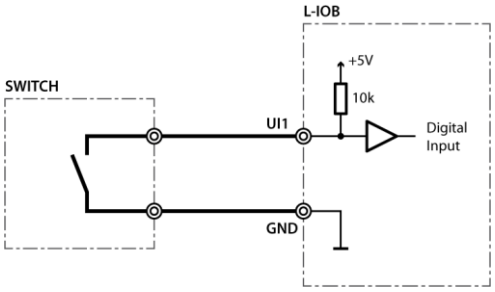


Figure 265: Switch connected to UI

UIs recognize the following digital signals according to the input resistance (switch):

Resistance Switch	Status
< 1.9 kΩ	Closed Switch
> 6.7 kΩ	Open Switch

18.5.2 Connection of S0 Pulse Devices (Meters)

S0 pulse meters must be connected to digital inputs (DI) as shown in Figure 266.

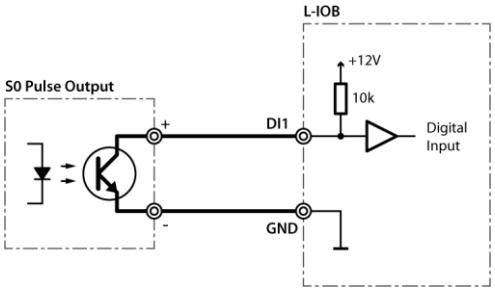


Figure 266: S0 pulse meter connected to DI

18.5.3 Connection of Voltage Sources to Universal Inputs

The Universal Input (UI) provides voltage measurement both if used as an analog or digital input. The signal type must be configured to 'Voltage 0-10V' or 'Voltage 2-10V' in both cases.

18.5.3.1 Voltage Source connected to UI with Analog Interpretation

Figure 267 shows the connection of a voltage source to a universal input in analog mode.

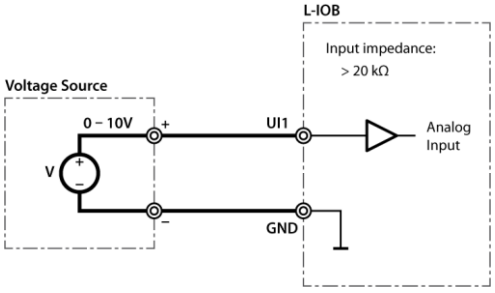


Figure 267: Voltage source on UI in analog mode

18.5.3.2 Voltage Source connected to UI with Digital Interpretation

Figure 268 shows the connection of a voltage source to a universal input in digital mode. In this case, the voltage source acts as a switch with the depicted low and high levels.

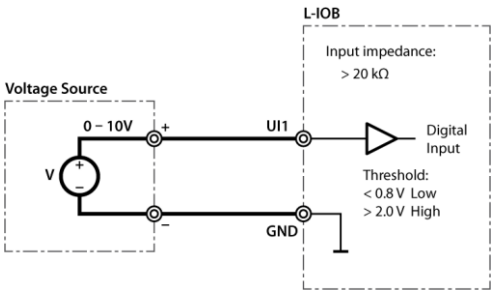


Figure 268: Voltage source on UI in digital mode

18.5.4 Connection of 4-20mA Transmitters to Universal Inputs

18.5.4.1 4-20mA Transmitter connected to UI with Internal Shunt

Some universal inputs have an internal shunt which can be activated (in pairs with another UI) in the Configurator software (signal type 'Current 4-20mA int. Shunt'). Which UIs are equipped with shunts is documented in the Section "Specifications" of the respective product's User Manual. Figure 269 shows the connection of a 4-20mA transmitter to a universal input with internal shunt.

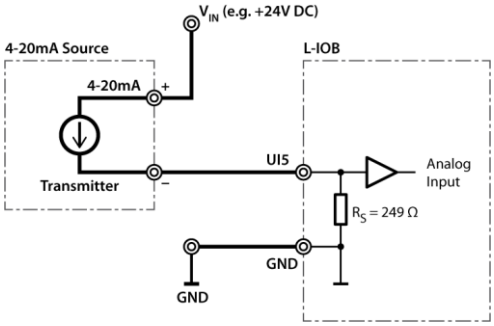


Figure 269: 4-20mA transmitter with internal shunt on UI

18.5.4.2 4-20mA Transmitter connected to UI with External Shunt

On universal inputs, which do not have an internal shunt, an external shunt must be used as shown in Figure 270. The signal type must be set to 'Current 4-20mA' in the Configurator software.

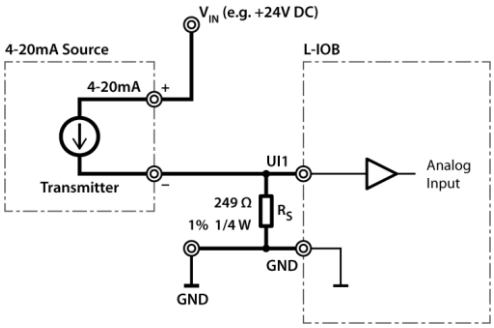


Figure 270: 4-20mA transmitter with external shunt on UI

18.5.5 Connection of Resistive Sensors

Figure 271 shows the connection of resistive sensors to the universal inputs with a temperature sensor as an example. Sensors in the resistance range of 1 kΩ to 100 kΩ can be measured. The signal type must be set to 'Resistance' in the Configurator software.

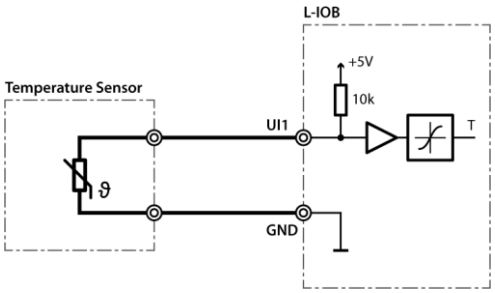


Figure 271: Temperature measurement on UI

18.5.6 Connection of STId Card Readers

Figure 272 shows the connection of an STId card reader to three L-IOB inputs (UIs or DIs). Observe that the clock signal must be connected to an interrupt-capable input of the L-IOB device. More information on STId card readers can be found in the LINX Configurator User Manual [1].

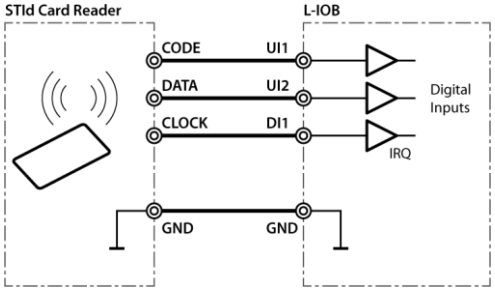


Figure 272: STId card reader

18.6 Physical Connection of Outputs

18.6.1 6A Relays with one External Fuse

The total current of all used 6A relays must be restricted to 6A, if more than two relays share a common (COM) terminal. The wiring shown in Figure 273 can be used for all L-IOB models with common terminals.

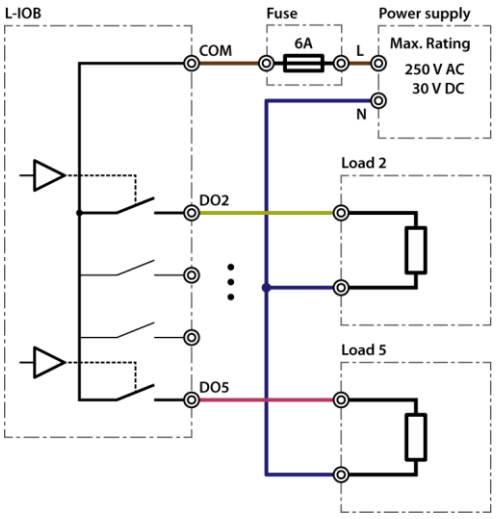


Figure 273: 6A relays with one external fuse

18.6.2 6A Relays on LIOB-xx2 using Separate Fuses

Figure 274 shows the wiring of the 6A relays for the LIOB-182/482/582 models using separate fuses. In this case, two relays share one common terminal (COM).

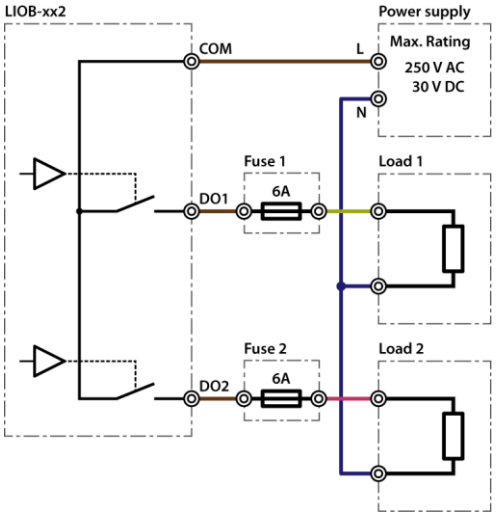


Figure 274: LIOB-182/482/582 6A relays

18.6.3 16A and 6A Relays on LIOB-xx3

The 16A and 6A relays on the LIOB-183/483/583 models all have two separate terminals per relay. There are no common (COM) terminals. This means that a 16A (or 6A) fuse must be wired to one of the two terminals of each relay, as shown in Figure 275.

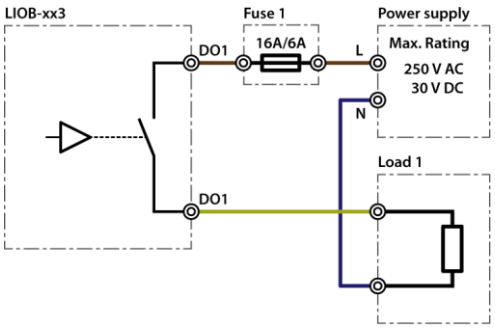


Figure 275: LIOB-183/483/583 16A/6A relays

18.6.4 External Relays and Inductive Loads

When controlling an external relay or inductive load using a L-IOB relay, either an integrated suppressor circuit must be used for the inductor, or a free-wheeling diode, a varistor, RC circuit, etc. must be installed to suppress voltage peaks and sparking due to switching off inductive circuits. It is recommended to use diodes that are part of the 1N400x family and to place them close to the relay, as shown in Figure 276. Figure 277 shows the connection of a 230V relay with a varistor.

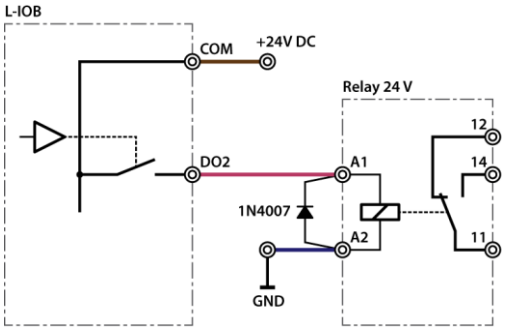


Figure 276: Suppressor circuit with free-wheeling diode

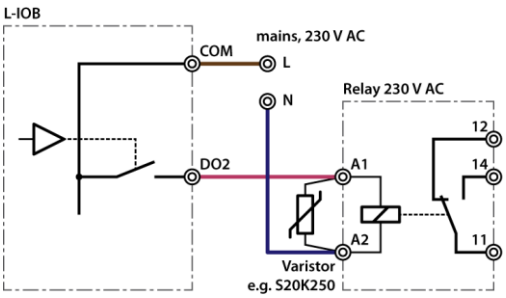


Figure 277: Suppressor circuit with varistor

18.6.5 Triacs

Figure 278 shows the wiring of the 0.5A Triac Outputs.

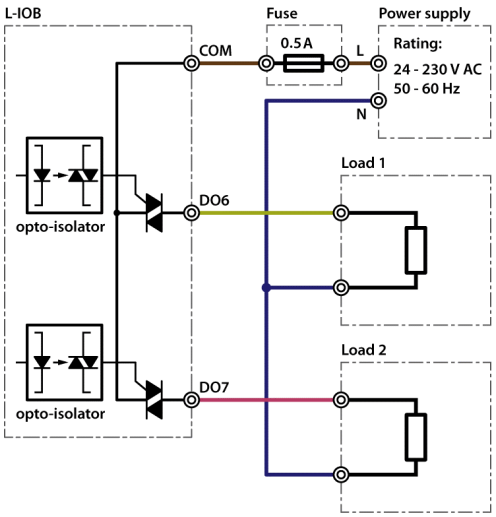


Figure 278: 0.5A Triacs

18.6.6 Analog Outputs

Figure 279 shows the wiring of the analog outputs (AO). Observe that the analog outputs are labeled '0-10V OUT' but are in fact capable of delivering over 11V.

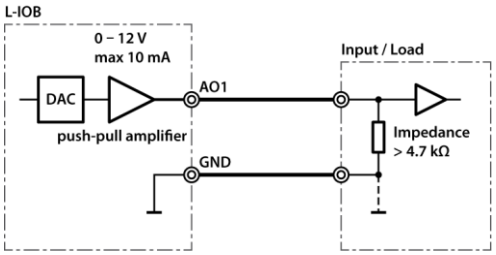


Figure 279: Analog outputs

The input impedance of the connected load must be greater than or equal to 4.7 kΩ for linear output.

18.7 Redundant Ethernet

18.7.1 Ethernet Cabling Options

Some device models are equipped with two Ethernet ports, which are connected to an internal Ethernet switch. This allows for advanced cabling options to reduce cabling costs or to increase network resilience. For this discussion, the term *upstream* is used to designate the direction towards the network, which the devices are connected to. Likewise, the term *downstream* is used to designate devices more distant to the network which the devices are connected to.

Redundant cabling options are enabled by the Rapid Spanning Tree Protocol (RSTP) which is implemented in most managed switches. Please note, that this is a feature of the switch, not of the L-INX or the L-GATE, so that LOYTEC cannot give a guarantee that this will work with a particular switch model. In no case redundant cabling options will work with unmanaged switches. The older Spanning Tree Protocol (STP) should not be used for this type of application, as it converges too slowly.

Star topology: In the most basic setup, a device is connected to an Ethernet switch with one cable. This is called a star cabling because all devices are connected to a common upstream device. In this setup, the cable and the switch are single point of failures.

Chain topology: Because the L-INX/L-GATE itself acts as an Ethernet switch, this device can be connected to a chain. This is a special form of the star topology. Its advantage is the reduced cabling costs. The disadvantage is the connection loss to downstream devices when an upstream device is powered-off, reset or removed. Also, the Ethernet bandwidth (100 MBit/s) is shared among all members of the chain. The last device has one unused Ethernet port, as it is not allowed to create Ethernet loops without STP. The recommended maximum number of daisy-chained devices is 20.

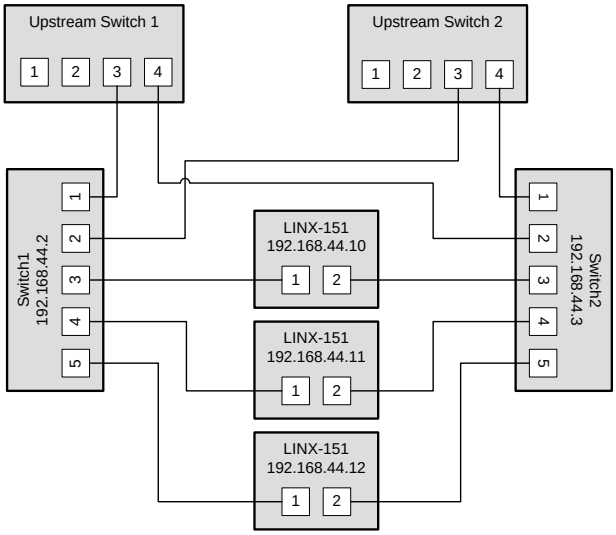


Figure 280: Fully redundant Ethernet topology

Fully redundant topology: Both Ethernet ports are connected to a different upstream switch. Thus, a single cable or upstream switch problem can be tolerated. This topology requires RSTP. In Figure 280, the LINX-151 with IP addresses 192.168.44.10 to 192.168.44.12 are connected in this way. This connection scheme increases switch and cabling costs, but increases network resilience. Note that the upstream network is connected via the lowest-numbered ports. If this is not possible, the ports need to be configured to the lowest STP port priority value (which is the highest priority).

Ring topology: In this setup, the devices are connected in a chain and each end of the chain is connected to a different upstream switch. This topology requires RSTP. If a single device is powered off, the RSTP will automatically recalculate the spanning tree so that all other devices in the chain are reachable. Only if two devices are power-off at the same time, the devices between them will not have an Ethernet connection. In Figure 281, the L-INX devices with IP addresses from 192.168.44.10 to 192.168.44.12 are connected in this way. The recommended maximum number of daisy-chained devices is 20.

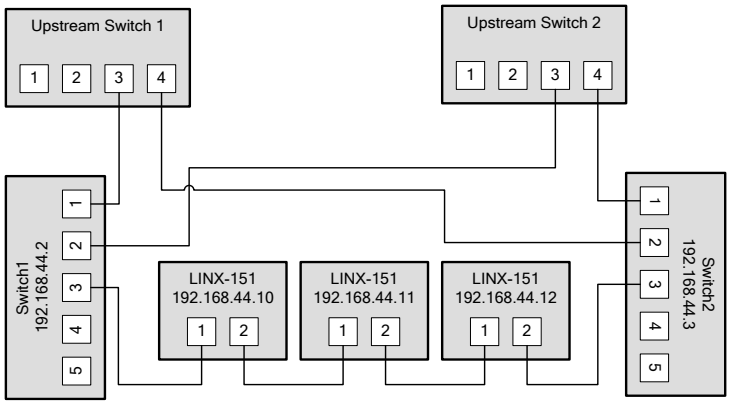


Figure 281: Ring Ethernet topology

18.7.2 Upstream Options

In case of redundant switches, there are two possible upstream topologies:

Single upstream connection: Switch1 (or Switch2, but not both) is connected to the upstream network while Switch2 only provides a redundant path to the Loytec devices. The redundant path is created by a direct Ethernet cable between Switch1 and Switch2 which needs to be plugged into a lower-numbered port than the L-INX devices are connected to. If this is not possible, the STP port priority for the cross-connection cable needs to be set to a low value. The RSTP domain should be restricted to Switch1 and Switch2. This can be done by enabling a BPDU filter on the port on Upstream Switch 1. This will block all RSTP packets to enter the upstream network. A sample setup for this topology is shown in Figure 282.

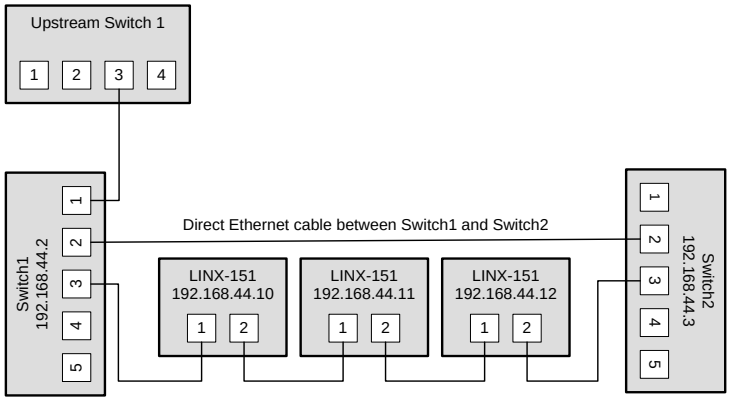


Figure 282: Single upstream connection.

Redundant upstream connection: Switch1 and Switch2 are both connected to the upstream network, either to two ports on the same switch or to two redundant upstream switches. In this case, RSTP is needed to ensure a loop-free topology between the upstream switches, Switch1 and Switch2, so the RSTP domain includes the upstream network and the chained L-INX/L-GATE devices. The configuration of Switch1 and Switch2 need to ensure that they are not selected as the root bridge. If possible device communication should be bound to a separate VLAN and MSTP (Multiple Spanning Tree Protocol) should be employed to isolate the spanning tree operations. This topology is shown in Figure 280.

18.7.3 Preconditions

For the fully redundant and ring topology, the following preconditions have to be met:

- The upstream switches have to support the Rapid Spanning Tree Protocol (RSTP), as defined in IEEE 802.1w.
- The upstream switches have to provide a broadcast storm filter.
- Two distinct switches are required for each end of the device chain.
- Both upstream switches are connected to the same Ethernet network.

18.7.4 Switch Settings

The switches which connect the devices to the network need the following settings. Note that these are only recommendations or starting points. Each network with redundant connections needs testing and verification to prevent network loops.

- The STP bridge must be enabled.
- The STP bridge priority should be set to the minimum (61440), so that these switches are not elected as root bridges.
- The bridge mode should match the upstream bridge modes, preferable 802.1s or 802.1w.

If the upstream network uses RSTP, the timing parameters of the upstream networks must be used. Else the timing parameters should be set to minimum values for fast convergence:

- Bridge max age time: 6 seconds
- Hello time: 1 seconds
- Forward delay: 4 seconds
- All ports connected to Ethernet rings have to be configured as NON-EDGE ports, so that the RSTP can detect loops
- The switches should be configured to block broadcast storms. A recommended rate is 5% or 3000 packets/seconds.

The upstream switches need the following configuration:

- If a single upstream connection is used, the connected port on the upstream switch should have BPDU filtering enabled.
- If redundant upstream connections are used, the connected ports on the upstream switches should have a BPDU root guard enabled.

18.7.5 Testing

When the switches are configured and the devices are connected, the following tests are recommended. These tests are important to confirm that the STP changes due to topology changes to not interfere with the rest of the network.

- Check that no broadcast storms are sent into the upstream network by capturing traffic between Switch1, Switch2 and the Upstream switch. This test should be done continuously, especially during switch and device power cycles.
- Check that all devices can be reached (ICMP ping).

Execute these tests for these conditions:

- Power up all switches and devices. Wait until all devices are up, then test.
- Power-off Switch1. Wait approx. 10 seconds, then test.
- Power-on Switch2, power-off Switch1. Wait until Switch2 has booted, then test.
- Power-on Switch1. Wait until Switch1 has booted, then test.
- Reboot all L-INX and L-GATE devices. Wait until the devices have booted, then test.
- Remove a single Ethernet cable. Wait approx. 10 seconds, then test. This test should be repeated for different cables. Make sure that at least the following connections are tested:
  - The connection between Switch1 and the L-INX directly connected to Switch1.
  - The connection between Switch2 and the L-INX directly connected to Switch2.
  - A connection in the L-INX chain which is not connected directly to either Switch1 or Switch2.

18.7.6 Example switch configuration

The following example shows the configuration commands for Switch1, Switch2 and the upstream switch (HP Procurve syntax) in the setup shown in Figure 280.

Upstream switches:

```
config
spanning-tree
spanning-tree priority 8
spanning-tree 3,4 root-guard
spanning-tree hello-time 1
spanning-tree forward-delay 4
spanning-tree maximum-age 6
exit
```

Switch1 and Switch2:

```
config
spanning-tree
spanning-tree priority 15
spanning-tree 1,2 port-priority 0
spanning-tree 3-5 port-priority 8
spanning-tree hello-time 1
spanning-tree forward-delay 4
spanning-tree maximum-age 6
exit
```

18.8 WLAN

18.8.1 Introduction

Devices supporting the LWLAN-800 wireless adapter can be connected to IEEE 802.11 wireless networks. The following operation modes are supported:

- **Client mode (separate network)**: The WLAN client connected to an existing access point. The firewall of the WLAN interface can be configured to provide only a subset of

the services of the device. For example, the WLAN interface could expose the Web UI, but not BACnet communication.

- **Access point mode (separate network)**: In the isolated access point mode, a client can connect to the wireless network created by the device. The device will assign an IP address to the client and will redirect all traffic to itself. This mode is used to configure a device with a mobile device.

- **Access point mode (bridged)**: In the bridged access point mode, a client can connect to the access point and also can use the network devices on the bridged Ethernet device. In this mode, the DHCP server is deactivated to avoid interference with an existing DHCP server in the Ethernet network.

- **Mesh point (separate network)**: This mode is used to create an IEEE 802.11s mesh network. Mesh points communicate with other mesh points in their radio vicinity and automatically choose the best route. Mesh networks can be used to extend the range of a wireless network or to create redundant radio links.

- **Mesh point (bridged)**: This mode is like the mesh point mode and also bridges the mesh point to an Ethernet network. Thus devices in the Ethernet network can communicate with devices in the mesh network. Only one mesh point should be in the bridged mode to avoid network loops.

The LWLAN-800 interface can use two WLAN functions at the same time. This can be used for advanced setups, like:

- Wireless 1 is used as an access point for configuring the device, while the Wireless 2 interface is used to participate in a mesh network.

- Wireless 1 is used as a bridged access point for configuring the device and the devices on the Ethernet network while Wireless 2 connects to another wireless network to reach a remote device.

However, there are restrictions when using both interfaces at the same time:

- Both functions need to use the same radio band.

- Both functions need to use the same channel.

18.8.2 802.11s Mesh Networking

WLAN client and access point modes are similar to other devices using 802.11 wireless networks. This section explains the features and benefits of the 802.11s network.

A mesh network removes the roles of clients and access points. Every node in a mesh network can send and receive data, as in a normal wireless network. However, every mesh node also routes packets to other mesh nodes. It observes the signal strength to all reachable nodes and distributes this information to other mesh nodes. Thus, the mesh network can transmit data between nodes with are not in their radio vicinity. In this case, a path between sender and receiver is selected and the intermediate nodes transmit the packet over several hops.

As the signal strenght and thus the range of a node can change over time, as well as nodes can be added and removed, the best path can change. The 802.11s routing protocol takes this into account and changes paths dynamically.

802.11s also provides strong encryption using the AuthSAE (Simultaneous Authentication of Equals) protocol, so that each pair of mesh nodes use an encrypted link. It is resistant to passive, active and dictionary attacks, given a strong pre-shared key.

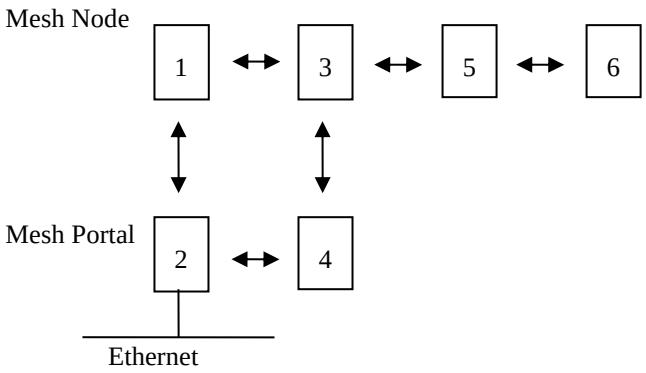


Figure 283: Mesh Networking

Figure 283 shows the roles of mesh nodes and possible links. Mesh point 1 can communicate with point 2 and point 3. It learns that the mesh point 2 is the mesh portal, so all traffic leaving the mesh network is automatically routed towards mesh point 2.

Mesh point 4 has mesh point 2 and 3 in its radio vicinity, but cannot communicate directly with mesh point 1. So mesh points 1 to 4 have two ways to reach each other and can tolerate the failure of a single node. This makes a mesh network resilient to node failure or fading radio links.

Mesh point 6 is an example on how mesh networks can be used to extend radio range. If point 2 communicates with point 6, there are two possible paths: 2-4-5-6 and 1-3-5-6. It selects the better path and mesh point 5 will extend the network range.

This example shows that every additional mesh point can make the network more resilient to failures or can extend the range far beyond the range of a single radio.

18.8.3 Hardware Installation

Connect the LWLAN-800 interface to the device with a USB cable, and then power the device. Do not remove the interface during operation.

The LWLAN-800 supports two antennas which should be mounted outside any metallized housing.

19 Firmware Update

LOYTEC devices support remote upgrade over the network. To guarantee that the device is not destroyed due to a failed firmware update, the firmware consists of two images:

1. The fallback image,

2. the primary image.

The fallback image cannot be changed. Thus, if the update of the primary image fails or the image is destroyed by some other means, the fallback image is booted and allows reinstalling a valid primary image. When the device boots up with the fallback image, all port LEDs are flashing red.

Newer devices do not have a dedicated fallback image anymore. Instead, they keep the last working firmware image as a backup. If a firmware upgrade fails or renders the device unsuable in any other way, the last working firmware image is re-tinstalled.

Depending on the device model, different firmware images (.dl files) are applicable. To make things simple, LOYTEC provides a firmware archive as a ZIP file. LOYTEC firmware upgrade interfaces (Web UI and Configurator) will choose the correct image from the archive and use it for the upgrade.

19.1 Firmware Update via the Configurator

The primary image can be updated using the Configurator. For this purpose, it is recommended to have the device connected to the Ethernet and to have a valid IP configuration (see Section 3.11.1). The Configurator must be installed as described in the LINX Configurator User Manual.

To Update the Firmware using the Configurator

1. Start the Configurator from the Windows Start menu: **Start → Programs → LOYTEC LINX Configurator → LOYTEC LINX Configurator**.

2. Select the menu: **Connection → Connect to device**. This opens the device connection dialog as shown in Figure 284.

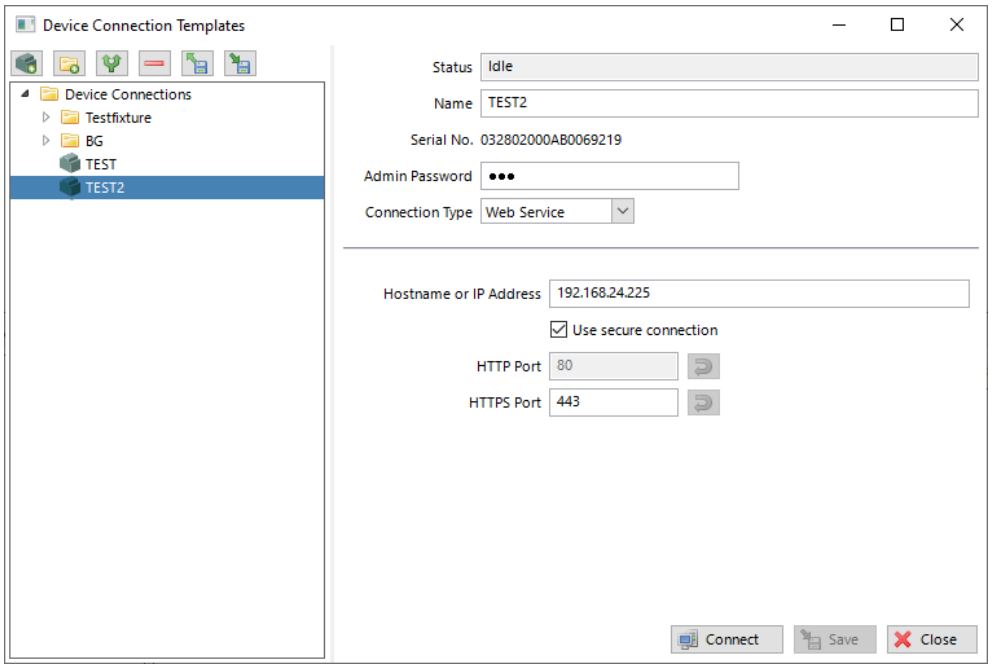


Figure 284: Device connection dialog.

3. In the connection dialog, enter the IP address of the device as well as the admin user's password. The password can be changed via the Web interface (see Section 3.1).

4. If the device uses other port settings than the standard settings or the device is operated behind a NAT router, adapt the HTTP(S) port accordingly.

5. Click on **Connect**.

Note: *Alternatively, one can also connect via LNS. A firmware upgrade over an FT-10 channel, however, needs a lot more time to complete than over IP.*

6. Optionally, check for updates by selecting the menu **Help → Check for updates …**. This function checks for new firmware and Configurator versions.

7. Select the menu: **Firmware → Update …**

8. This opens the **Firmware Update** dialog as shown in Figure 285. Click on the button and select the firmware image.

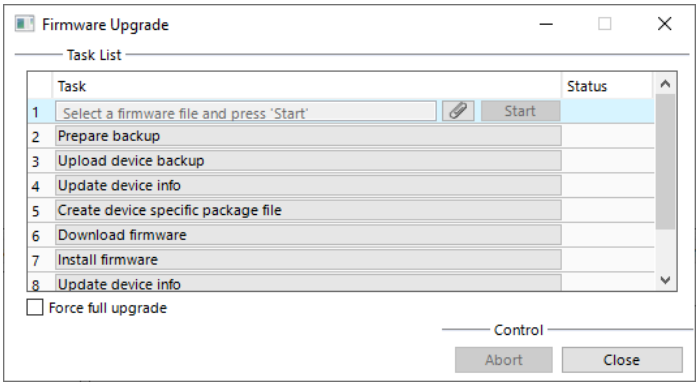


Figure 285: Firmware Update dialog of the Configurator.

9. Click on **Start** and observe the download progress.

10. When the download is complete, a dialog appears. Click **OK**.

11. In the Firmware Update dialog, click **Close**.

12. The device's firmware has now been successfully upgraded.

19.2 Firmware Update via the Web Interface

The device's firmware can also be upgraded using the Web interface. This option can be found in the **Config** menu under the **Firmware** item. For more details see Section 3.11.2.

19.3 Firmware Update via USB Memory Stick

The device's firmware can also be upgraded using a USB memory stick. When connecting the memory stick a pop-up menu opens on the LCD display. For more details see Section 2.6.

19.4 Firmware Update of L-IOB I/O Modules

The firmware of a L-IOB I/O module can be upgraded through the L-IOB host, if the host is a L-INX or L-ROC device. For doing so, the Configurator needs to be connected to the L-IOB host to perform the upgrade of all connected L-IOB I/O modules.

To Upgrade the L-IOB Firmware over the L-INX

1. Start the Configurator and connect to the L-INX device, which hosts the L-IOB I/O modules.

2. Select menu **Firmware / Update attached LIOB devices**.

3. This opens the Firmware Upgrade dialog as shown in Figure 286 and starts the detection of all connected L-IOB devices. Using the **Upgrade** checkbox in the **L-IOB Overview** list, it is possible to choose which devices shall be upgraded.

4. Click on to select the L-IOB firmware images for LIOB-Connect/FT (LIOB-10x/15x) and LIOB-IP (LIOB-45x/55x) devices. Observe that there are different firmware images for these two groups. Click on repeatedly to add more firmware images. The added firmware images are assigned to the matching L-IOB devices, which is indicated in the **Remarks** column. If any of those I/O modules shall not be upgraded, de-select them in the **Upgrade** column.

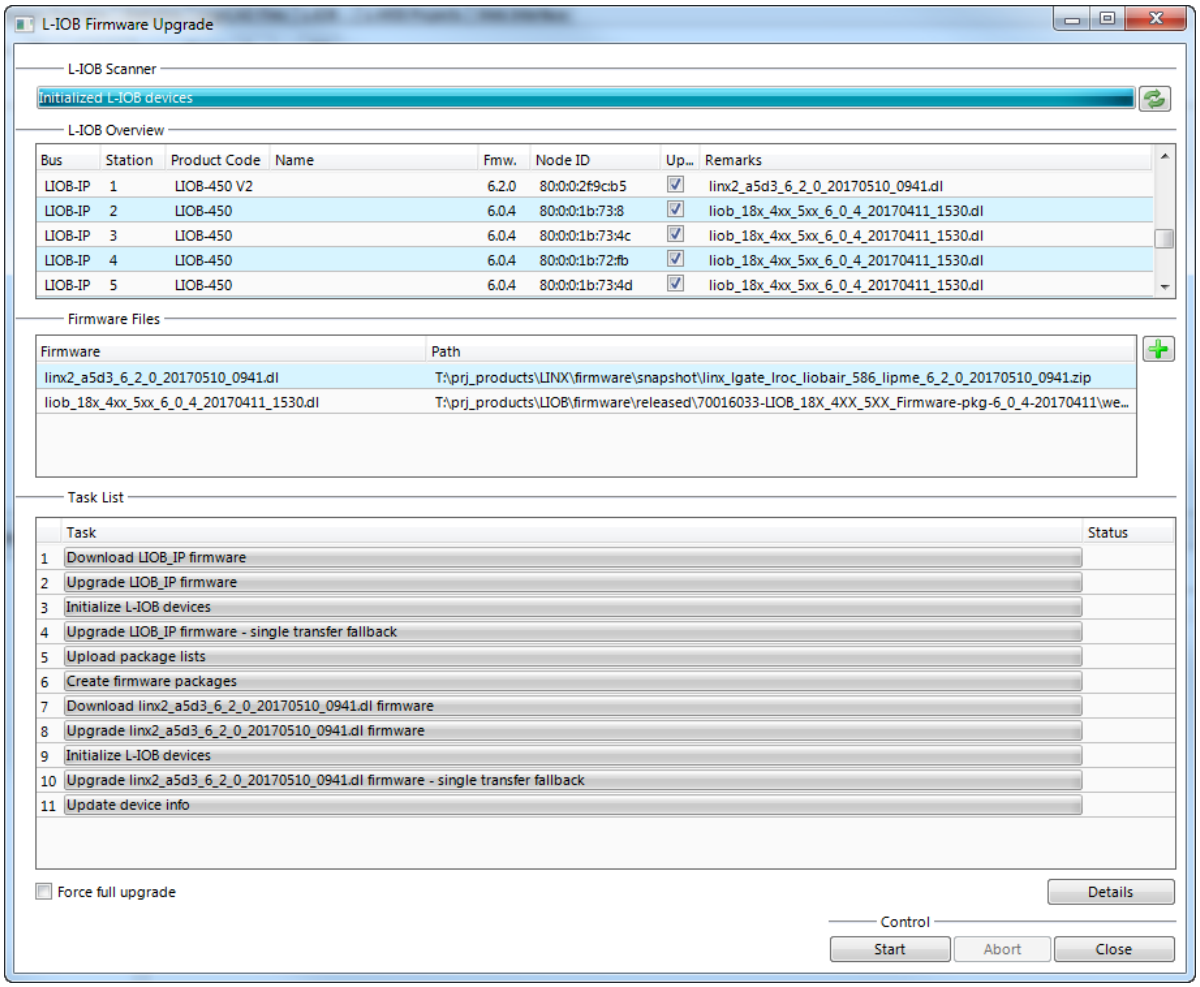


Figure 286: L-IOB Firmware Update dialog of the Configurator

5. In order to minimize download time, the Configurator effectively upgrades only those devices that have an older firmware. If that optimization shall be turned off, check **Force full upgrade**.

6. Click on **Start**.

7. Observe the download progress. When the download is complete, click **Close**.

The L-IOB firmware of LIOB-45x/55x devices in LIOB-IP device mode can also be directly updated over IP. This method is faster and also the only possible upgrade method if the L-IOB host is a LIOB-48x/58x device.

To Upgrade the LIOB-45x/55x Firmware directly

1. Start the Configurator and connect directly to the L-IOB device using a Web service Connection.

2. Select menu **Firmware / Update**.

3. This opens a Firmware Update dialog as shown in Section 19.1. Click on the  button and select the L-IOB firmware image. Observe that LIOB-45x/55x devices need a different firmware than the other models.

4. Click on **Start**.

5. Observe the download progress. When the download is complete, click **Close**.

20 Troubleshooting

20.1 Technical Support

LOYTEC offers free telephone and e-mail support for the L-INX product series. If none of the above descriptions solves your specific problem please contact us at the following address:

LOYTEC electronics GmbH
Blumengasse 35
A-1170 Vienna
Austria / Europe

e-mail : ***support@loytec.com***
Web : ***http://www.loytec.com***
tel : ***+43/1/4020805-100***
fax : ***+43/1/4020805-99***

or

LOYTEC Americas Inc.
N27 W23957 Paul Road
Suite 103
Pewaukee, WI 53072
USA

e-mail: ***support@loytec-americas.com***
Web: ***http://www.loytec-americas.com***
tel: ***+1 (512) 402 5319***
fax: ***+1 (262) 408 5238***

20.2 Packet Capture

20.2.1 Configure Remote Packet Capture

Remote packet capture is able to capture packets on the Ethernet port and on the MS/TP port. The MS/TP remote packet capture option is only available, if the MS/TP port is enabled on the device (see Section 3.5.21). To enable the remote packet capture feature, go to the **Ethernet** port configuration and enable **Remote packet capture** as shown in Figure 287.

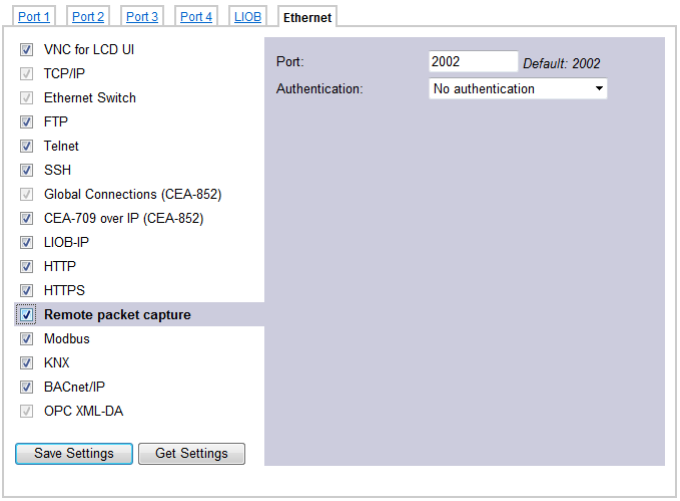


Figure 287: Remote packet capture port configuration.

The default **Port** setting may be changed to the desired port. Normally, this can be left at its default. If **No authentication** is selected, the device will allow incoming capture connections without requiring any credentials. If **Username and Password** is selected as authentication method, the client Wireshark will be required to provide valid credentials before the capture session can be started. Note, that only the users **admin** and **operator** are allowed to connect if this authentication method is selected.

Click the **Save Settings** button to save the configuration. The changes take effect and do not require to reboot the device. The remote capture can also be disabled again without a reboot.

20.2.2 Enable Local Capture

The device provides a local capture feature. With local capture enabled the device logs packets to an internal ring buffer. The log can be downloaded from the Web interface. To verify that the device is set up correctly, go to **Statistics → Packet capture** as shown in Figure 288**.**

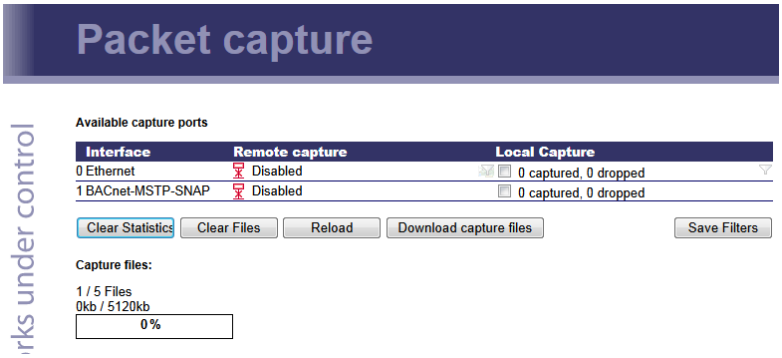


Figure 288: Packet capture statistics.

Verify that the Ethernet and optionally the MS/TP capture ports are listed in the **Available capture ports** table and that the **Remote capture** status for these ports reads **Disconnected**. If the MS/TP port is not listed on a device that has an MS/TP port, make sure that the MS/TP port is enabled in the port configuration.

To log offline without a Wireshark attached to the device, click the check box **Local Capture**. The device will then start capturing packets and stores them in a ring buffer. The log file can be downloaded by clicking on the button **Download capture files**. This stores a ZIP archive of the packet capture to your local hard drive. Capture files can be cleared by clicking **Clear Files**. After a reboot all local capture files are lost.

For local Ethernet capture additional capture filters can be added to narrow down the amount of logged packets to those of interest. Select the line Ethernet port line and enter a basic filter expression at the bottom of the page. Then click on **Add** and add more filters, which all must apply (AND condition). Finally click on **Save Filters** to store and activate the local capture filters. Figure 289 shows an example filter for packets to and from IP address 192.168.24.100 using the 'Host' filter. Add the 'Port' filter to further narrow down on the TCP/UDP port.

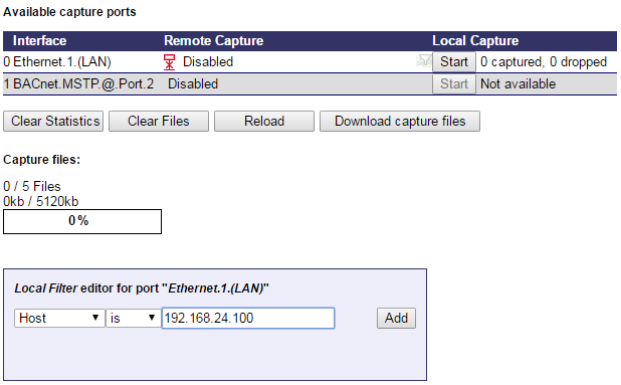


Figure 289: Adding local Ethernet capture filters.

20.2.3 Run Wireshark Remote Capture

The remote packet capture requires the use of Wireshark 1.6.11 with WinPCAP 4.1.2. Please update your Wireshark installation to this version or use a newer Wireshark version.

To add a remote capture port

1. Open Wireshark and choose the menu **Capture → Options…** . This opens the **Capture Options** dialog as shown in Figure 290.

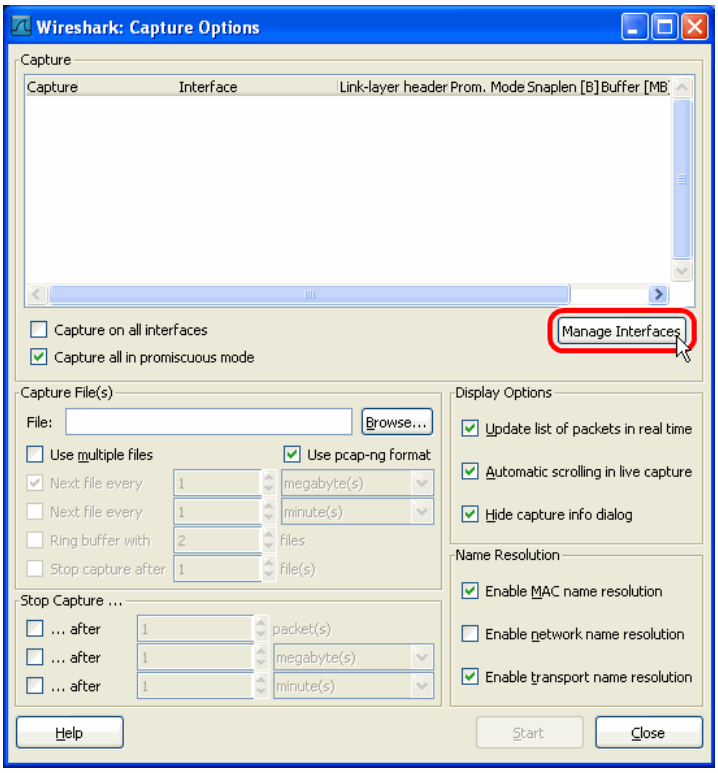


Figure 290: Wireshark Capture Options Dialog.

2. Click the **Manage Interfaces** button to open the **Add new interfaces** dialog.

3. Select the **Remote Interfaces** tab and click **Add** as shown in Figure 291.

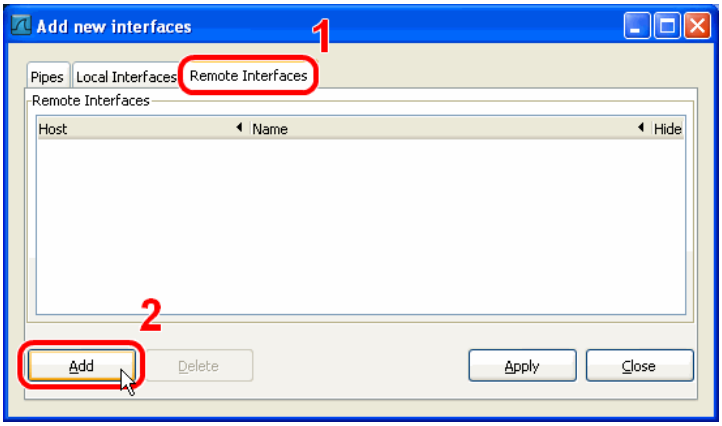


Figure 291: Wireshark Add New Interfaces Dialog.

4. Enter the correct settings for **Host** and **Port** (default 2002) and, if authentication is enabled, enter **Username** and **Password** in the corresponding fields as shown in Figure 292.

5. Note that only the users **admin** and **operator** are allowed to connect.

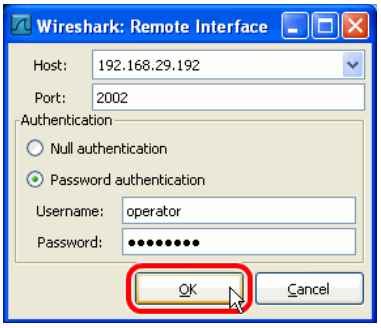


Figure 292: Wireshark Remote Interface Dialog.

6. Click **OK** to retrieve the interface list from the device.

7. If the connection to the device was established successfully, the **Remote Interfaces** list will be updated with information about all capture ports available on the device as shown in Figure 293.

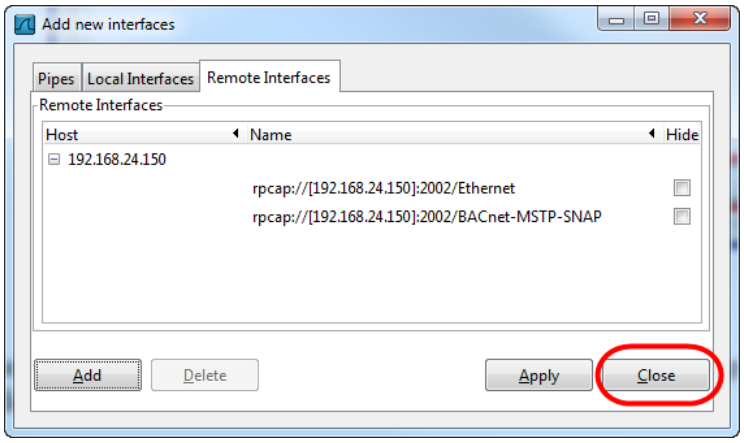


Figure 293: Added new interface to Wireshark.

8. Close the **Add new interfaces** and **Capture Options** dialogs to return to the main window.

To Start a Remote Capture

1. Select the created remote interface from the interface list in the main window. It is named 'Raw Ethernet traffic' for remote Ethernet dapture and 'SNAP encapsulated BACnet MS/TP traffic' for remote MS/TP capture.

2. Click the **Start** button as shown in Figure 294.

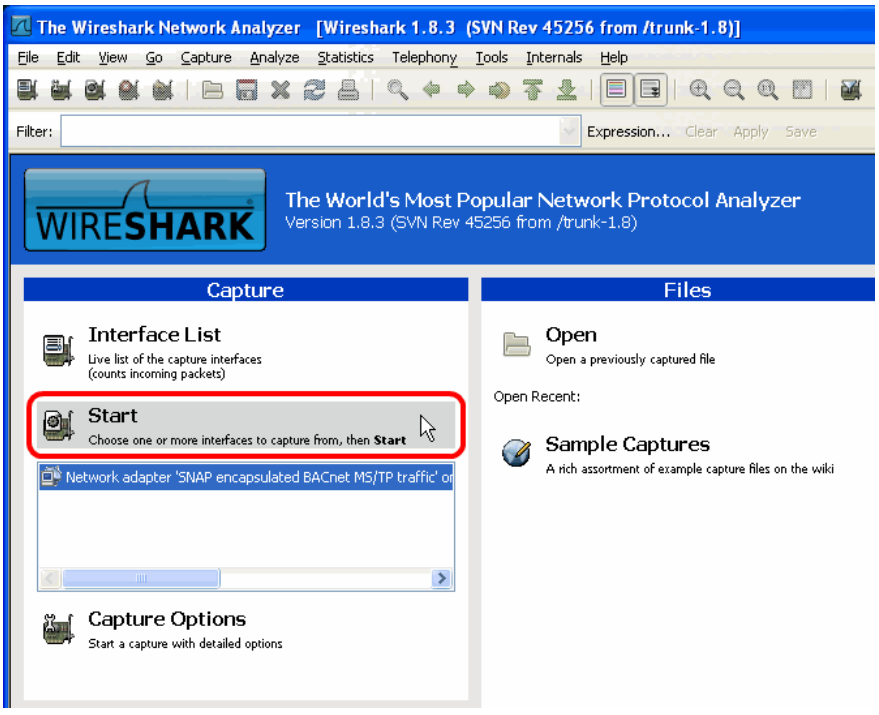


Figure 294: Start Remote Capture in Wireshark.

3. Wireshark will attempt to establish a connection to the device and, if successful, start displaying packets. An example capture is shown in Figure 295.

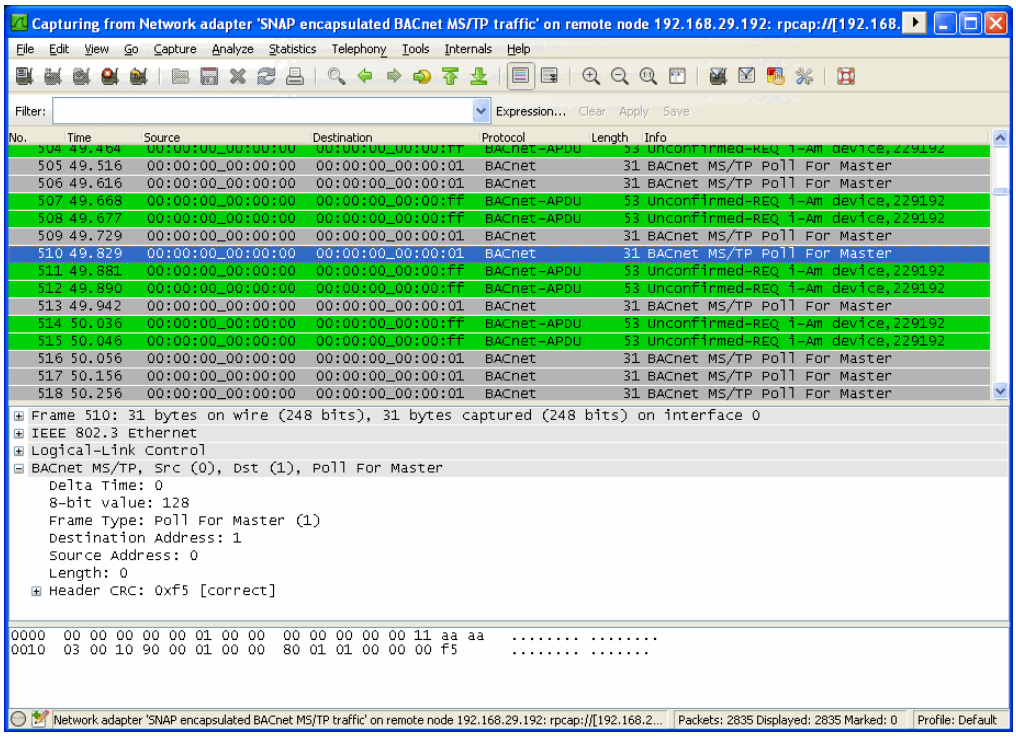


Figure 295: Example MS/TP remote capture in progress.

21 References

[1] LINX Configurator User Manual 8.2, LOYTEC electronics GmbH, Document № 88086711, December 2023.

[2] L-IP User Manual 8.2, LOYTEC electronics GmbH, Document № 88065917, January 2024.

[3] LIP-ME20X User Manual 8.2, LOYTEC electronics GmbH, Document № 88073513, December 2023.

[4] NIC User Manual 4.2, LOYTEC electronics GmbH, Document № 88067217, April 2013.

[5] LWEB-900 User Manual 4.0.1, LOYTEC electronics GmbH, Document № 88081510, September 2022.

[6] L-VIS User Manual 8.0, LOYTEC electronics GmbH, Document № 88068527, June 2023.

[7] L-IOB I/O Module User Manual 8.2, LOYTEC electronics GmbH, Document № 88078517, December 2023.

[8] L-DALI User Manual 8.0 LOYTEC electronics GmbH, Document № 88077119, March 2023.

[9] AN011E L-DALI Compatibility List, LOYTEC electronics GmbH, Document № 86002010, April 2020.

[10] LWEB-802/803 User Manual 4.6, LOYTEC electronics GmbH, Document № 88074225, April 2023.

[11] LOYTEC LDALI Devices User Manual 3.30, LOYTEC electronics GmbH, Document № 88094302, October 2023.

22 Revision History

Date	Version	Author	Description
2016-03-23	6.0	STS	Initial revision.
2016-10-19	6.1	STS	Updated for firmware version 6.1. Section 2.1 Device setup LCD UI rotation, new icons. Updated Section 3.2.8 Mesh configuration. Section 8.3.6 L-STAT firmware upgrade, backup/restore on Modbus Web UI. Section 11.3.4 EnOcean teach-in using transmission ID. Section 3.2.2 Backup/restore options added. Added Chapter 12 MP-Bus. Section 3.3.7 Moved Alarm log to Data menu. Updated Section 10.3.4 SMI calibration. Added Section 15.1.4.3 LOYTEC LDALI RM1 relay module. Added Section 15.2.6 Emergency Logs.
2017-04-24	6.2	STS	Updated for firmware version 6.2. Section 2.6 LCD UI firmware upgrade. Updated Section 3.2.26 L-LOGICAD configuration. Added Section 3.2.27 L-STUDIO configuration. Added Section 12.2.2 LMPBUS-804. Section 12.3.4 added port selection, updates in MP-Bus scan, PPX addressing. Added Section 18.4: Firmware Update of L-IOB I/O Modules. Section 19.3.2 Wireshark: Clarify language that filters are AND.
2018-05-15	6.4	STS, JB	Updated for firmware version 6.4. Section 3.1 Language selector. Section 3.2.3: Lock settings on Web UI that are configured by L-STUDIO deploy. Augmented Section 3.2.29 on when self-signed certificates are required. Updated Section 3.2.30 Web UI firmware upgrade: backup before upgrade. Added Section 3.2.33 Scripting Web interface. Added Section 3.9.1 Web UI safe reboots. Updated Section 6.2.2 OPC UA and Security. Added Section 6.2.5 Connect with an OPC UA client. Updated Section 7.4 for multiple M-Bus ports. Section 15.1.4: Added LDALI-MS2, LDALI-BM2, L-RC1. Section 15.2.3: Added new DALI colour picker.
2019-05-15	7.0	STS	Updated for firmware version 7.0. Added Section 3.2.24 VPN configuration. Updated Section 3.3.1 on value source information. Section 12.2.2 documented 2 x LMPBUS-804 feature. Added Section 14.1.1 Supported ekey models.
2020-04-30	7.2	STS	Updated for firmware version 7.2. Section 3.1.1: Updated device setup and password enforcement. Section 3.2.4: added IPv6 static config, NTP setting. Section 3.2.7 Dynamic DNS. Section 3.2.8 updated LWLAN-800 AP client limit. Section 3.2.19 BACnet/IPv6 configuration. Section 3.2.25: Added description of the VPN tab. Added Section 3.2.36: Node-RED editor. Section 3.2.38: Added LTE configuration. Section 3.2.39: Added SMS gateway. Updated 3.5.2: Updated IP statistics. Section 3.5.14: Mobile network statistics page. Section 3.8.6: Updated LIOB I/O test description. Section 15.1.4: Added description of LDALI RM3, RM4 and RM8, added feedback feature for button modules. Section 15.2.2: Added description of new functions in the DALI-Installation-Tab of the WebUI. Removed Section 19.2 Statistics on the console.

Date	Version	Author	Description
2021-01-29	7.4	STS, UR	Updated for firmware version 7.4. Chapter 3: Reorganized to match new menu structure. Section 3.5.5: Added 802.1X port authentication. Section 3.5.25: Updated slave proxy function. Section 3.5.29: Added LWEB-900 VPN registration. Section 3.6.4: LOYTEC device discovery in Node-RED. Added Section 3.7.3 User Management. Section 8.3.1: Added LRS232-802 description. Section 15.1.4: Added description for DALI Device Types LDALI-MS2-BT / LDALI-MS4-BT / LDALI-RM5 / LDALI-RM6 / LDALI –PWM4 / LDALI-PD1, Section 15.2: Update of scan function description and WebUI-figures
2022-01-30	7.6	STS, UR	Updated for firmware version 7.6. Section 2.1: Describe VPN setup menu. Section 3.3.2: Manual Override option to clear all override values. Section 3.5.1: New timezone configuration. Section 3.5.6: Added 3rd NTP server and descibe Internet connection sharing. Section 3.5.30: VPN Configuration on the VPN port config tab. Section 3.5.33: Moved license menu. Section 3.6.4: Node-RED safe mode option. Section 3.11.4: New clear project page. Section 3.11.5: Skip safe reboot option. Section 15.1.3.1: Various Refinements in LOYTEC multisensor description. Section 15.1.3.2: Added measurement range for generic instance. 15.1.4.4: switching operating mode of LDALI RM5/RM6. 15.1.4.6: added certification, load definition and hint for common lamps for LDALI-PD1. 15.1.4.7: detailed description of LDALI-PWM4-x types. 15.1.7: Added mode using local datapoints for mains off handling. 15.2.2: added description for new options on DALI installation site and introduction for light sensor calibration. 15.2.4: added new screenshot for DALI statistics and description for statistical parameters. 15.5: Added description for some DALI error codes.
2022-11-08	7.6.2	UR	Section 2.4.2.: Added unconfigured mode for Relays on LIOB. Section 15: Bluetooth - Added Section for new technology.
2023-03-30	8.0	STS, UR	Updated for firmware version 8.0. Section 2.1 Added VPN setup using a USB thumb drive. Added Section 2.7 PIN code protection and UnprotectedBrowse folder. Added Section 3.2.11 BACnet/SC statistics. Section 3.3.1 Data point pagination. Section 3.3.4: Added color selection for presets. Section 3.3.6: Added iCalendar scheduler. Section 3.5.8 + 3.5.9: WLAN tab updates (Client, AP, Mesh). Added Section 3.5.20 BACnet/SC configuration. Section 3.5.29 Added EC keys to SSH server. Section 3.5.33 Send test SMS. Section 3.7.2 Added EC key option to certificate management. Section 8.3.3 Modbus commission: Enter IP + port number for Modbus TCP. Section 15: Bluetooth – chapter reworked. Section 16: LDALI – Moved LDALI-devices description to separate manual. Updates on actuators and sensor datapoint representations.
2023-12-30	8.2	STS	Updated for firmware version 8.2. Added Section 3.3.2 Edit Priority array. Section 3.7.3: Specified limits of usernames.