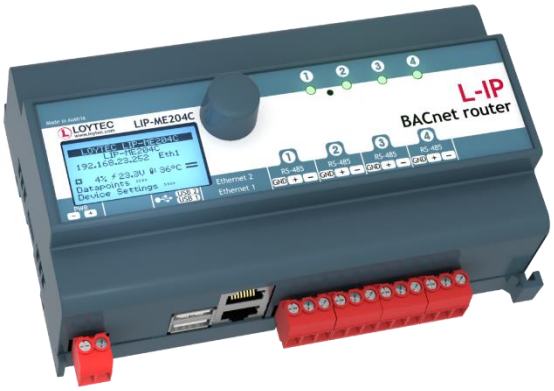
LIP-ME20X™

L-IP™ BACnet Router

User Manual

Delta IBT (Europe) GmbH



Contact

Delta Intelligent Building Technologies (Europe) GmbH
Blumengasse 35
1170 Vienna
AUSTRIA/EUROPE
support@loytec.com
http://www.loytec.com

Version 8.6

Document № 88073515

DELTA IBT (EUROPE) MAKES AND YOU RECEIVE NO WARRANTIES OR CONDITIONS,
EXPRESS, IMPLIED, STATUTORY OR IN ANY COMMUNICATION WITH YOU, AND
DELTA IBT (EUROPE) 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.

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 Delta IBT (Europe).

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 Delta Intelligent Building Technologies (Europe) 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 7

1.1 Overview 7

1.2 LIP-ME20X Models 8

1.3 Scope 8

2 Disclaimer Cyber Security 9

3 Safety Instructions 10

4 What's New in LIP-ME20X 16

4.1 New in LIP-ME20X 8.6.0 16

4.2 New in LIP-ME20X 8.4.0 17

4.3 New in LIP-ME20X 8.2.0 18

4.4 New in LIP-ME20X 8.0.0 18

4.5 New in LIP-ME20X 7.6.0 19

4.6 New in LIP-ME20X 7.4.0 20

4.7 New in LIP-ME20X 7.2.0 21

4.8 New in LIP-ME20X 6.4.0 23

4.9 New in LIP-ME20X 6.0.0 24

4.10 New in LIP-ME20X 5.3.0 25

4.11 New in LIP-ME20X 5.1.0 25

5 Quick-Start Guide 27

5.1 Hardware Installation and IP Connection 27

5.2 Configuration of the LIP-ME20X 27

5.2.1 Configuration on the Web Interface 27

5.2.2 Configuration on the LCD Display 27

5.3 Remote Protocol Analyzer 29

5.4 Reset to Factory Defaults 29

6 Hardware Installation 30

6.1 Enclosure 30

6.2 Product Label 30

6.3 Mounting 30

6.4 LED Signals 31

6.4.1 MSTP Activity LED 31

6.5 LCD Display and Jog Dial 31

6.6 Wiring 33

7 Firmware Update 34

7.1 Firmware Update Via the Web Interface 34

7.2 Firmware Update Via the USB Port 34

8 Troubleshooting 35
8.1 Technical Support 35
8.2 Packet Capture 35
9 Security Hardening Guide 36
9.1 Installation Instructions 36
9.2 Firmware 36
9.3 Ports 36
9.4 Services 37
9.5 Upgrade Key Strength 38
9.6 Logging and Auditing 38
9.7 Network Access 38
9.8 Password Protection 38
9.9 Encryption-At-Rest 39
9.10 Secure Disposal and Decommissioning 39
9.11 Information Policy 39
10 Specifications 41
10.1 Physical Specifications 41
10.1.1 LIP-ME201C, LIP-ME202C 41
10.1.2 LIP-ME204C 41
10.2 Resource Limits 42
11 References 43
12 Revision History 44

Abbreviations

100BaseT .....100 Mbps Ethernet network with RJ-45 plug
ACL .....Access Control List
BACnet .....Building Automation and Control Network
BBMD.....BACnet Broadcast Management Device
BDT .....Broadcast Distribution Table
B/IP .....BACnet over IP (this is a BACnet data link layer)
DHCP.....Dynamic Host Configuration Protocol
DNS .....Domain Name System
DST.....Daylight Saving Time
FD .....Foreign Device
FTP.....File Transfer Protocol
GMT.....Greenwich Mean Time
IP.....Internet Protocol
LAN .....Local Area Network
MAC .....Media Access Control
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
NTP.....Network Time Protocol
OPC.....Open Process Control
OPC UA.....OPC Unified Architecture
RSTP.....Rapid Spanning Tree Protocol (Standard IEEE 802.1D-2004)
SNMP .....Simple Network Management Protocol
SSH .....Secure Shell
UI .....User Interface
UTC .....Universal Time Coordinated
VPN .....Virtual Private Network
WLAN .....Wireless LAN

1 Introduction

1.1 Overview

The LIP-ME20X is a BTL-certified BACnet router between MS/TP and B/IP (BACnet over IP) as well as a BBMD (BACnet Broadcast Management Device) for transportation of BACnet broadcasts over an IP network with several subnets. A router to BACnet/SC is also available. Additionally, it can serve as a BACnet time master and a BACnet MS/TP slave proxy. The LIP-ME20X also provides additional features such as optional write protection of the BDT, a BACnet/IP access control list and a simple BBMD communications test to troubleshoot the network. The L-IP models also provide an embedded BACnet/SC hub function. The MS/TP port supports remote Wireshark packet capture for troubleshooting the MS/TP channel.

The LIP-ME202C and LIP-ME204C model are true multi-port MS/TP routers that come with two Ethernet ports and two or four MS/TP ports respectively. The device setup can be done easily on the LCD display. Each of the MS/TP ports is routed to BACnet/IP and/or BACnet/SC and can serve a full-blown MS/TP channel. Communication settings as well as sophisticated MS/TP token passing statistics are available on the Web interface per MS/TP port. The remote Wireshark packet capture feature is also available on each of the MS/TP ports. This makes the LIP-ME202C and LIP-ME204C a perfect alternative to installing four separate routers, reducing space and cost.

In addition the LIP-ME20XC models are also equipped with enhanced security features such as a built-in firewall and a secure Web interface for installation using HTTPS with self-signed or installable CA certificates. By configuring separate IP networks on the two Ethernet ports, the BACnet network can be entirely isolated from the configuration interface. It is also possible to separate BACnet/IP and BACnet/SC into separate networks.

For perfect integration into building management software such as the LWEB-900 by LOYTEC, the LIP-ME20XC offers an embedded OPC UA server with certificate authentication, which exposes important operational parameters as OPC tags. For enhanced maintainability by IT departments these models provide the same data also through an SNMP server. Together with the LWLAN-800 adapter the LIP-ME20XC can operate BACnet/IP on the WLAN. By setting up an access point on the BACnet/IP network, the device can be used to distribute MS/TP channels on a wireless network.

The LTE-800 mobile interface is available for LIP-ME20XC and offers access over a mobile network. Together with the integrated OpenVPN client a secure BACnet channel can be established and the LIP-ME20XC device is also reachable over multi-NAT access networks, such as LTE.

1.2 LIP-ME20X Models

This Section provides an overview of the different LIP-ME20X models in Table 1. This table identifies the different features of those models. Models that possess a certain feature have a check mark (✓) in the respective column. If a feature is not available in the particular model, the column is left blank.

Model / Features	LIP-ME201C	LIP-ME202C	LIP-ME204C
BACnet Router	✓	✓	✓
MS/TP Ports	1	2	4
BBMD	✓	✓	✓
BACnet/SC Router	✓	✓	✓
BACnet/SC Hub (A64)	✓	✓	✓
OPC XML-DA	✓	✓	✓
OPC UA	✓	✓	✓
SNMP	✓	✓	✓
LCD Display	✓	✓	✓
USB	✓	✓	✓
Ethernet Switch/Hub	✓	✓	✓
WLAN, LTE	✓[1]	✓[1]	✓[1]
SSH, HTTPS, Firewall	✓	✓	✓

[1] To operate these protocols an expansion module is needed and must be ordered separately.

Table 1: Available features in different LIP-ME20X models.

1.3 Scope

This document covers LIP-ME20X devices.

2 Disclaimer Cyber Security

LOYTEC offers a portfolio of products, solutions and systems with cyber security functions that enable the secure operation of devices, systems and networks in the field of building automation and control technology. To ensure that devices, systems, and networks are always protected against online threats, a holistic security concept is required that is implemented using the latest technology and is being kept up-to-date. The LOYTEC portfolio is only one component of such an overall concept.

The customer is responsible for preventing unauthorized access to the devices, systems and networks. These should only be connected to a network or the Internet if adequate security measures are in place (e.g. firewalls, separate networks) and a connection is required for operation. In addition, LOYTEC's recommendations for securing devices in the Security Hardening Guide (Chapter 9) must be followed. For additional information, please contact your support person at LOYTEC or visit our website.

LOYTEC is constantly working on improving the existing products in order to follow the latest cyber security standards. Therefore, LOYTEC strongly recommends installing updates as soon as they become available and always using the latest software versions. LOYTEC explicitly points out that using older versions or refraining from updates increases the risk of online security threats, exposing the device to known and documented security threats, which may result in unauthorized access to the device, modification or disclosure of configuration and confidential user data, or disruption of building automation operation. LOYTEC disclaims liability for security incidents, accidents, or failures that are attributable to the use of a product on which available security updates have not been installed.

3 Safety Instructions



ATTENTION

General Safety Instructions

Please regard the following general instructions for project planning and execution:

- Regard all measures or prohibitions of the respective country to avoid danger of electricity and high voltage.
- Other relevant regulations of the respective country.
- House installation regulations of the respective country.
- Regulations of the utility company.
- Any specifications, diagrams, dispositions, cable lists and regulations of the customer or system integrator.
- Any third-party regulations (e.g., general contractor or client).



ATTENTION

Country-specific Safety Regulations

Failure to observe country-specific safety regulations can lead to property damage and personal injury. Therefore, comply with the country-specific regulations and the corresponding safety guidelines.



CAUTION

Electrical Safety

Essentially, electrical safety in building automation systems from LOYTEC is based on the use of extra-low voltage and safe isolation from mains voltage.



CAUTION

IEC (SELV, PELV) (world-wide)

Depending on the extra-low voltage earthing (24VAC), this results in an application according to SELV or PELV in accordance with IEC 60364-4-41:

- Ungrounded = SELV (Safety Extra Low Voltage),
- Earth ground = PELV (Protected Extra Low Voltage).



CAUTION

NEC (North America)

Class 2 transformers with energy limitation to 100 VA or Class 2 circuits with max. 100 VA (using a non-energy-limiting transformer of max. 400VA) combined with overcurrent limits (T-4A fuses) can be used for each individual 24VAC device. Several fuses for several isolated secondary circuits per transformer are possible. The same applies to power supplies with 24VDC.



CAUTION

Device Safety

Device safety is guaranteed by supply with low voltage 24VAC or 24VDC and a double insulation between mains voltage 230VAC, 24VAC circuits and the housing or by supply via Power over Ethernet (PoE Class 1). In addition, the specific regulations for electrical wiring according to this manual must be observed.



ATTENTION

Installation Personnel

Only qualified staff may carry out electrical installations.



CAUTION

Installation according to Safety Class II

LOYTEC devices, which are designed in compliance with safety class II, must be mounted accordingly.

The following requirements apply:

- Protection against electric shock has to be ensured by an appropriate enclosure.
- Ensure proper working cable relief for installation in safety class II equipment.



ATTENTION

Environment Conditions

LOYTEC devices have to be installed in a dry and clean environment. In addition the permissible environment conditions specified in the product data sheet must be observed.



CAUTION

Earth Ground of ⊥ (System Zero AC/DC 24V)

The following items must be observed when earth-grounding system zero ⊥ 24VAC:

- In principle, both earth-grounding and non-grounding of system zero of the operating voltage 24VAC is permitted. Important are the local regulations and customs. Due to functional requirements, earth ground may be necessary or inadmissible.
- It is recommended to ground 24VAC systems unless this contradicts the manufacturer's instructions.
- To avoid earth loops, systems with PELV may only be connected to earth ground at one point in the system. Unless otherwise stated, usually at the transformer.
- The same applies to 24VDC power supplies.



CAUTION

Functional Earth ⏚

Functional earth must be connected to the building's protective earthing (PE) system on the installation side.



CAUTION

Operating Voltage 24V AC/DC

The power supply must meet the requirements for SELV or PELV. Permitted deviation of the nominal voltage:

- At the transformer or power supply: 24V AC/DC -10 … + 10%
- At the device: 24V AC or DC ±10 %



CAUTION

Specification for 24VAC Transformers

IEC: safety transformers according to IEC 61558 with double insulation, designed for 100% duty cycle to supply SELV or PELV circuits.

U.S.: Class 2 circuits according to UL 5085-3.

For efficiency reasons, the power drawn from the transformer should be at least 50% of the nominal load.

The nominal power of the transformer must be at least 25 VA. Using a transformer of smaller size, the ratio of open circuit voltage to voltage at full load becomes unfavorable (> + 20%).



CAUTION

Specification for 24VDC Power Supplies

Power supplies must be designed for 100% duty cycle to supply SELV or PELV circuits.

U.S.: Class 2 circuits according to UL 5085-3.

For efficiency reasons, the power drawn from the power supply should be at least 50% of the nominal load.



CAUTION

Protection of the 24VAC Supply Voltage

Transformers must be protected on the secondary circuit, according to the transformer dimensions and the effective load of all connected devices:

Always protect the 24VAC conductor (system potential),

Additionally protect the conductor ⊥ (system zero) where required.



CAUTION

Protection of the 24VDC Supply Voltage

24VDC power supplies must be short-circuit proof or have an internal microfuse.

Local regulations must be observed.



CAUTION

Protection of Mains Voltage

Transformers/24VDC power supplies must be protected on the primary circuit using a control cabinet fuse.



CAUTION

Power over Ethernet (PoE)

LPAD-7 Touch Panels require a PoE Class 1 power supply (max. 12W), which must be compliant to IEEE 802.3at-2009.

For the power supply of the PoE switches observe the manufacturer's specifications.



CAUTION

Device Installation/Removal in De-Energized State Only

Ensure that the power supply is switched off before starting to install or uninstall LOYTEC devices. Do NOT connect or disconnect equipment with power switched on, unless instructed otherwise. Do NOT assemble or disassemble devices with power switched on, unless instructed otherwise.



CAUTION

Power Supply Protection

When installing LOYTEC devices, ensure that the power source is adequately protected by means of a suitably-rated fuse or thermal circuit breaker.



CAUTION

Power Supply Voltage

Do not connect a voltage supply greater than the specified maximum rating. Refer to product label and/or datasheet for the correct voltage.



CAUTION

DALI is FELV (Functional Extra Low Voltage)

A DALI-line is treated to be FELV. Since it is non-SELV the relevant installation regulations for low voltage apply.



ATTENTION

DALI Wiring

A DALI-line may be installed within the same cable or as single conductors within the same tube as mains supply. The DALI-line is either limited to a maximum length of 300 m using a minimum cross-section of 1.5 mm2 (AWG15) or it must be ensured that the voltage drop on the DALI-line does not exceed 2 V.



CAUTION

Attention to External Voltages

Any kind of introduction or spreading of dangerous voltages onto the low-voltage circuits of the system (e.g. due to incorrect wiring) must be avoided at any circumstance and represents an immediate life danger or can lead to the entire or partial destruction of the building automation system.

4 What's New in LIP-ME20X

4.1 New in LIP-ME20X 8.6.0

This section describes the major changes and new features. For a full list of changes refer to the Readme file.

BACnet Rev 1.26 BTL certified

The BACnet certification of all BACnet models has been updated to comply with protocol revision 26. All new device models are now BTL certified. New BACnet features in that release include

- Network port objects
- BACnet/SC with certificate renewal over BACnet

BACnet/SC Embedded Hub

Some LOYTEC devices now come with an embedded BACnet/SC hub. This hub can be used as a local failover hub. This can keep a local BACnet/SC segment alive if a centralized, remote hub is going offline. The embedded hub can also be used as a primary hub for creating small local BACnet/SC networks.

BACnet IP-IP and SC-SC Router

LOYTEC devices that support BACnet routing now also support multiple instances of BACnet/IP or BACnet/SC on different IP interfaces (e.g. one BACnet/IP on the LAN and one BACnet/IP on the WAN). The built-in router then routes between all those BACnet network ports. Specifically, this feature makes BACnet/IP-to-BACnet/IP routters possible, as well as BACnet/SC-to-BACnet/SC routers. Morover, the SC-SC routers are beneficial for semgmenting BACnet/SC into one or more local SC segments that use the router to a global BACnet/SC network (e.g. a BACnet OWS in the cloud).

LDAP User Authentication

The device firmware supports LDAP integration for authenticating users. LDAP users are in addition to built-in and locally defined users. The LDAP configuration defines the LDAP server, bind user/password and user and group queries. Local user roles are mapped to specific LDAP groups. Secure LDAP is also supported.

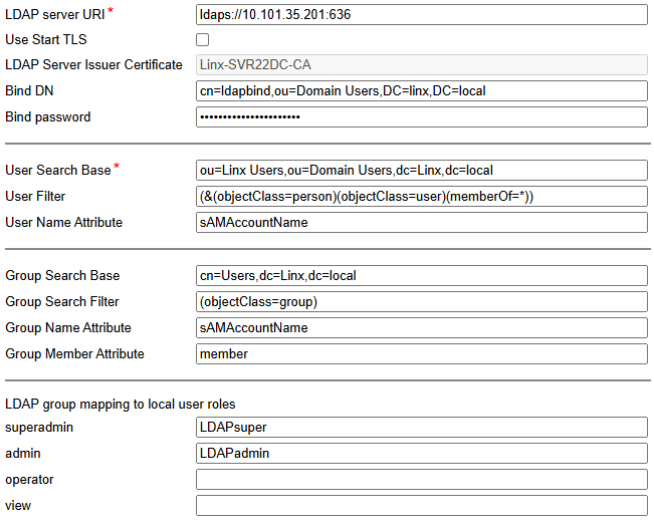


Figure 1: LDAP configuration Web UI.

Zero-Config IP

The default setting on the Ethernet interface is to acquire IP addresses via DHCP. In case there is no DHCP server or the DHCP server is temporarily unavailable, the new zero-config IP feature will assign an IP address in the automatic private IP addressing (APIPA) range 169.254.0.1 to 169.254.255.254. Once assigned this auto-IP address persists over power-on resets. Devices with auto-IP can be found using their mDNS name (i.e. hostname.local).

VNC connection on Web UI

The LCD display on LOYTEC devices can be operated over the network using a VNC connection. The VNC protocol is now available through a websocket URI on the device for so-called ‘noVNC’ clients. This is a secure alternative to the legacy VNC port. The device Web UI offers a simple VNC connect button to open the LCD display content in the web UI using that secure websocket channel.

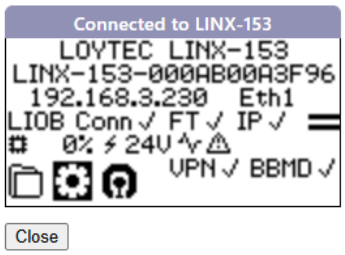


Figure 2: Secure noVNC popup window on the Web UI.

4.2 New in LIP-ME20X 8.4.0

This section describes the major changes and new features. For a full list of changes refer to the Readme file.

Enhanced Account Security and View Role

The built-in user accounts (admin, operator, guest) can be disabled to prevent attacks on those well-known accounts. The admin account can only be disabled, if a custom user account with

the superadmin role is created instead. For all accounts, the default settings enforce the use of strong passwords.

The new “view” role has been added that allows a user to view configuration settings only. A view user cannot change any configuration settings.

BACnet/SC Node Improvements

The LOYTEC BACnet/SC node has been extended to improve troubleshooting and compatibility with third-party hubs. The node now supports uploading a CA certificate chain. While not required by the standard, this feature gives extra flexibility with certain PKI implementations.

The BACnet/SC node also supports a Wireshark interface, that can be enabled for troubleshooting the encrypted traffic. On the network, IPv6 is supported for hub connections.

Discovery of Devices via loytec.local

Unconfigured LOYTEC devices starting with firmware 8.4.0 can now be easily found without knowing the IP address by simply calling the Web page ‘loytec.local’. The search is implemented as an mDNS discovery on the local network. A device finder page is displayed that provides links to all devices found.

Configuration of an Internet Failover Interface

LOYTEC devices can support multiple paths to reach the Internet. For example, Ethernet and an attached LTE-800 interface. For such scenarios, a failover interface can be selected. This failover interface is used as the default route to the Internet, if the primary interface lost Internet connection. This can be configured on the IP Host tab.

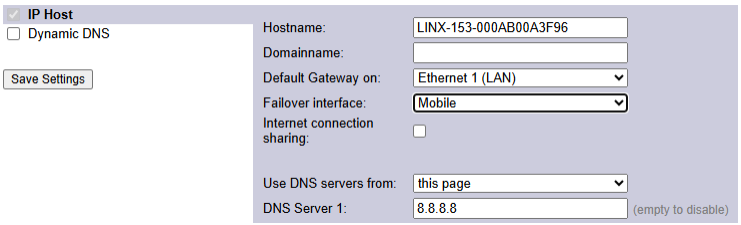


Figure 3: Configuration of an Internet failover interface.

4.3 New in LIP-ME20X 8.2.0

This section describes the major changes and new features. For a full list of changes refer to the Readme file.

Support new A64 models

The new L-IP models based on A64 hardware are now supported. The new firmware also contains a major security upgrade to OpenSSL 3.1.

4.4 New in LIP-ME20X 8.0.0

This section describes the major changes and new features. For a full list of changes refer to the Readme file.

New WLAN Configuration Tabs and System Registers

The WLAN configuration of the port configuration has been re-modelled to better match the client and access point (AP) use cases. The tabs are now labelled **WLAN Client** and **WLAN Access Point**. These tabs are restricted to settings that apply to their respective use.

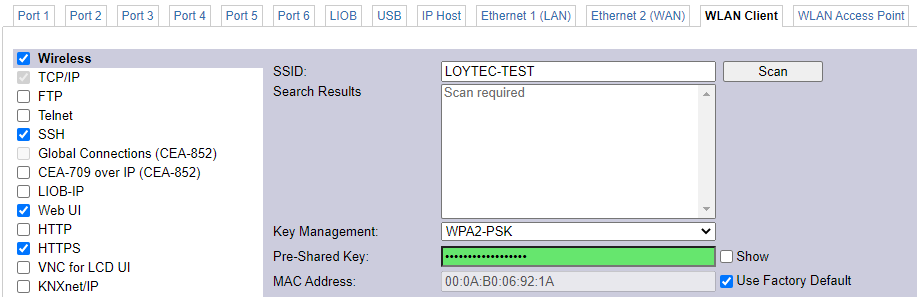


Figure 4: New WLAN configuration tabs

The system registers have also been moved to sub-folders named WLAN Client and WLAN Access Point. Setting SSID, Key and writing the new Enable system register under either port allows enabling the client or AP, respectively.

BACnet/SC

LOYTEC devices support the BACnet/SC node function. This allows LOYTEC devices to register with BACnet/SC hubs and be integrated in BACnet/SC networks, thus benefitting from increased security including TLS encryption and authentication. On devices with a BACnet router, BACnet/SC can be enabled in addition to or as a replacement of BACnet/IP. Devices without the BACnet routing function can enable either BACnet/SC or BACnet/IP.

The internal device certificate can be used out-of-the-box, and CA-signed operational certificates can be installed as needed. When BACnet/SC and BACnet/IP and/or MS/TP are enabled, the device acts as a router between those interfaces. It is also possible to run BACnet/SC on a separate network than BACnet/IP.

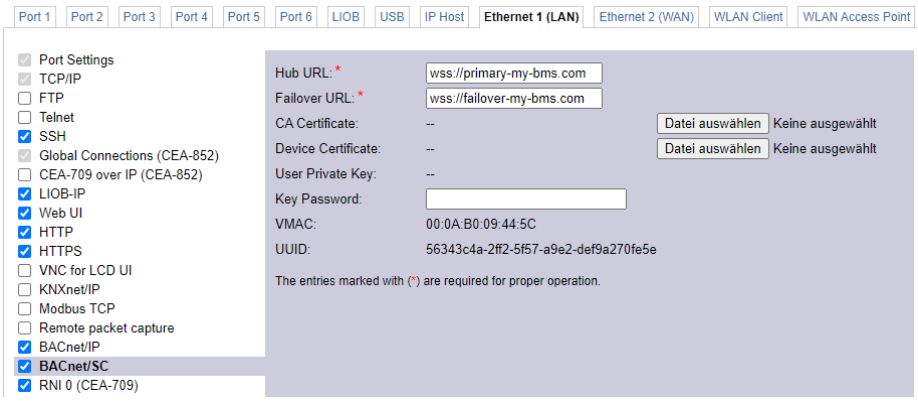


Figure 5: BACnet/SC configuration on Ethernet

4.5 New in LIP-ME20X 7.6.0

This section describes the major changes and new features. For a full list of changes refer to the Readme file.

BTL Testplan 16 Certified

The BACnet certification of all BACnet models has been updated to comply with protocol revision 16. All new device models are now BTL certified. New BACnet features in that release include

- Support extended “jumbo” MS/TP frames.

WiFi Enterprise

To further increase security in a WiFi network, IT departments support the 802.1X authentication method on WiFi also known as WiFi Enterprise. LOYTEC devices can enable WiFi Enterprise in the WiFi settings by selecting WPA2-ENTERPRISE key management. The authentication methods Protected EAP (PEAP), Tunneled TLS (TTLS) and EAP-TLS (using certificates) are supported.

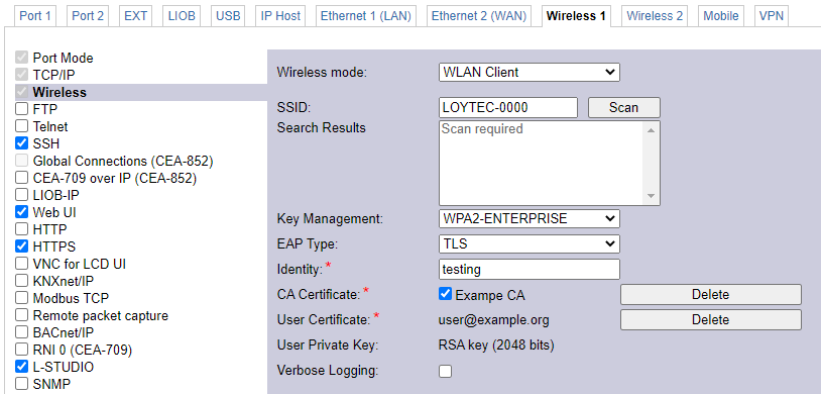


Figure 6: Configure WiFi Enterprise

4.6 New in LIP-ME20X 7.4.0

This section describes the major changes and new features. For a full list of changes refer to the Readme file.

New Menu Structure on Web UI

The menu structure on the Web UI has been redesigned to be more intuitive and group frequent actions together. New top-level menus help keeping the menus organized into typical tasks, such as statistics, data viewing, commissioning, configuration, programming, security, and maintenance.

User Management on the Device

LOYTEC devices now provide a simple user management to create users and passwords on the go. Users can be assigned roles, such as ‘admin’, ‘operator’ or ‘lweb’ roles. Users having the ‘lweb’ role are limited to using LWEB-802/803 visualization projects only and have no other device operation capabilities.

The Web UI on the device allows creating, deleting and modifying users and assigning roles. As an example, an additional admin user can be created who is allowed to configure the device without knowing the master admin password. This user account can easily be disabled again.

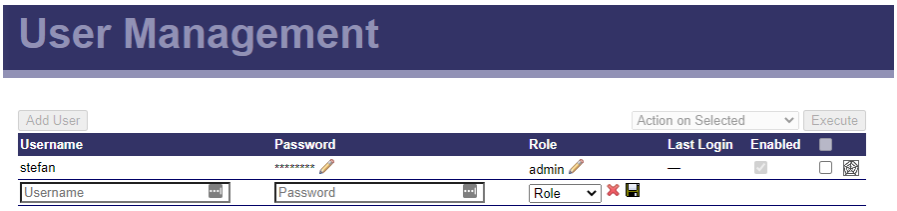


Figure 7: User management on the device.

Network 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. The authentication methods Protected EAP (PEAP), Tunneled TLS (TTLS) and EAP-TLS (using certificates) are supported.

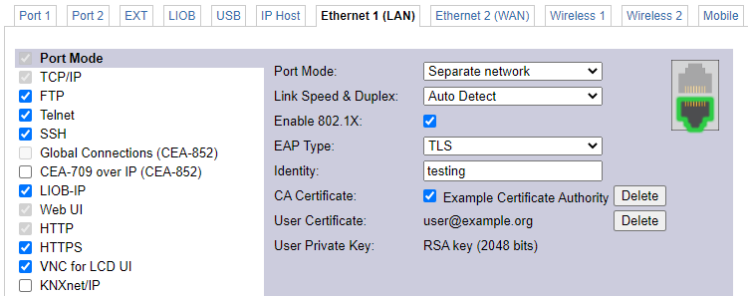


Figure 8: Configure 802.1X port authentication

4.7 New in LIP-ME20X 7.2.0

This section describes the major changes and new features. For a full list of changes refer to the Readme file.

New User Manual Structure

The LIP-ME20X User Manual has been split up into two parts: The LIP-ME20X User Manual, which now covers the specific functions of the LIP-ME20X device models. And the LOYTEC Device User Manual for the common Web interface, LCD display and operating interfaces topics common to all LOYTEC devices.

Support for LTE

LOYTEC devices now support the LTE-800 mobile interface. This interface is connected via the USB port and offers LTE/UMTS/GSM mobile network access. A SIM card from your provider needs to be inserted and the LOYTEC device is ready on the mobile network. A **Mobile** tab has been added to the port configuration interface for configuring the LTE-800. Simply enable Mobile Network, enter your APN data and select which protocols shall be run on LTE. The VPN client is also ready to be used on the LTE mobile network.

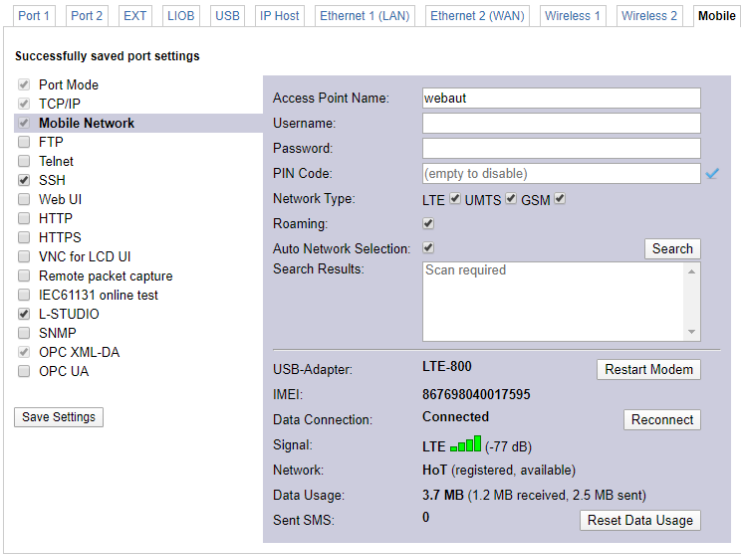


Figure 9: LTE-800 mobile configuration

Internet Connection Sharing

Combined with an LTE-800 mobile interface a LOYTEC device can act as a NAT router to share the mobile Internet connection with other devices on the LAN. For doing so, the **Internet connection sharing** feature can be enabled on the **IP Host** tab, where the default router interface is selected. Other devices on the LAN need to specify the IP address of the LOYTEC device offering connection sharing as their default gateway. This way, local devices can use NTP, VPN client or other Internet services.

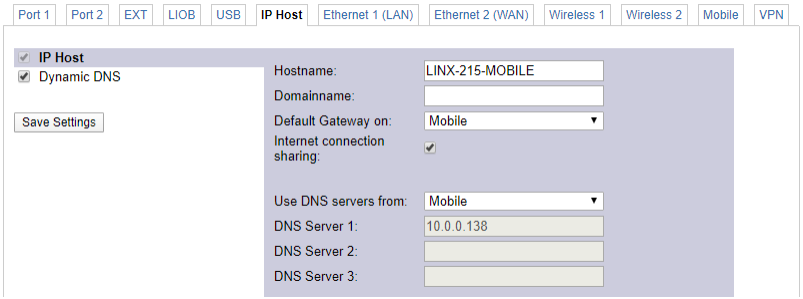


Figure 10: Internet connection sharing

Dynamic DNS

LOYTEC devices can now make use of a dynamic DNS service to register a public DNS name. This makes the device reachable over a publich IP address that can change over time, for instance an LTE-800 mobile interface using a public IP address assigned by the mobile carrier. A number of dynamic DNS providers are preconfigured and can be selected on the **IP Host** tab of the port configuration as shown in Figure 11.

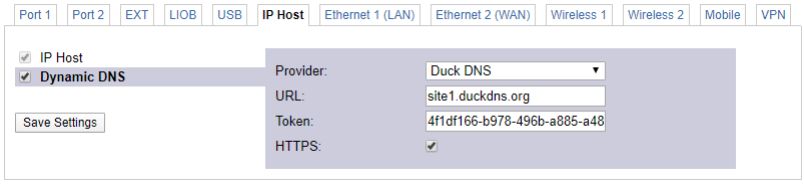


Figure 11: Dynamic DNS Settings

Secure Building Automation Protocols using VPN

This firmware version enhances flexibility and control over which building automation protocols are directly available on the VPN. A separate **VPN** tab has been added to the port configuration that allows configuring IP-based control protocols to be running directly on the VPN client. This effectively secures otherwise unsecured automation protocols such as BACnet/IP. When running on the VPN interface, the protocols are assigned the VPN's IP address and as a protocol node, the LOYTEC device is also reachable over multi-NAT access networks, such as LTE.

For example, simply set up BACnet/IP on the VPN interface and add all other BACnet/IP devices to the same VPN. Each node establishes a secure channel to the OpenVPN server hub, which routes the traffic between the communicating peer nodes. No unencrypted traffic will ever be transmitted.

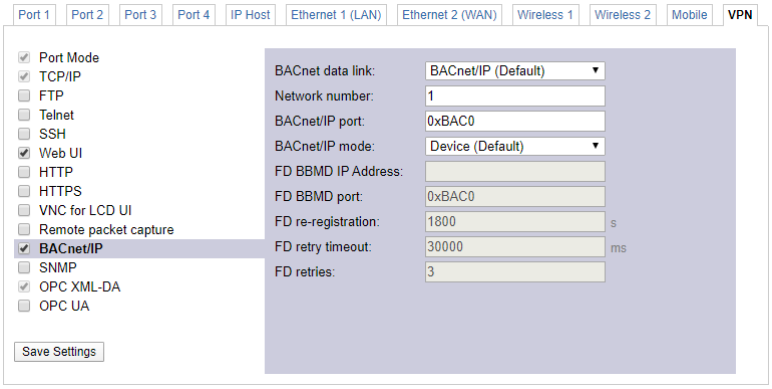


Figure 12: VPN tab on the port configuration interface.

IPv6

LOYTEC devices now support IPv6 using stateless address autoconfiguration (SLAAC) or having a configured, fixed IPv6 address. The IPv6 feature is available on all Ethernet and WLAN ports. With SLAAC no further configuration (except the required IPv6 router equipment) is required. The static IPv6 address can be configured on the TCP/IP settings on the port configuration.

Protocols that support IPv6 are the Web interface, SSH, HTTPS, NTP and BACnet/IPv6. Additional IPv6 statistics have been added to the IP statistics pages for troubleshooting.

4.8 New in LIP-ME20X 6.4.0

This section describes the major changes and new features. For a full list of changes refer to the Readme file.

Localized Web Interface

The entire Web interface of the device has been localized to German, French, and Chinese language. Simply change the language on the LCD display or directly on the Web interface via the new flag symbol on the upper right corner. Changing language is instant and does not require a reboot.

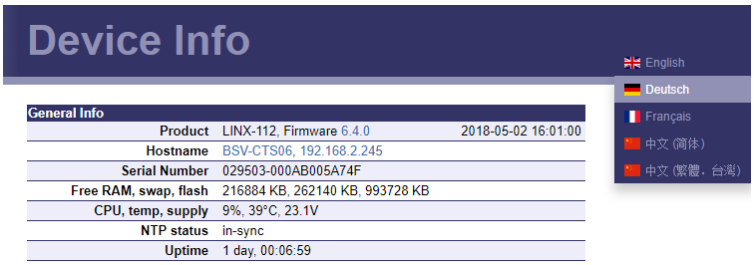


Figure 13: Language selection on the Web interface

Safe Reboot and Auto-Login

Changing IP settings and rebooting could end in a device unreachable, if something was different than expected. The new safe reboot feature helps out by reverting the changes made, if not logged in in on the Web interface within 5 minutes after the reboot. Locking oneself out by entering a mistaken IP address is no longer possible.



Figure 14: Safe reboot screen suggesting new IP address.

Another new feature that helps getting logged in again is the session auto-login. After a device has rebooted the Web interface restores the session and automatically logs in again. Even when changing a static IP address the device tries to connect to the new IP or suggests links for opening the device info page under the new IP address.

Backup before Upgrade

The firmware upgrade feature has been made safer by creating a backup before executing the upgrade. This feature has been added to firmware and Configurator upgrade paths. It is, however, optional and can be turned off by deselecting the check box.

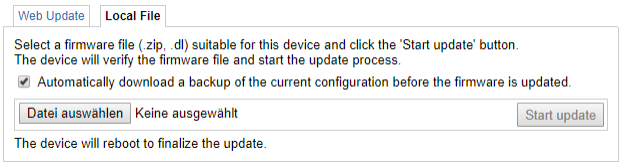


Figure 15: Backup before Upgrade on the Web interface.

4.9 New in LIP-ME20X 6.0.0

This section describes the major changes and new features. For a full list of changes refer to the Readme file.

BTL Testplan 12 Certified

The BACnet certification of all BACnet models has been updated to comply with protocol revision 12. All new device models are now BTL certified.

4.10 New in LIP-ME20X 5.3.0

This section describes the major changes and new features. For a full list of changes refer to the Readme file.

New Models LIP-ME201C, LIP-ME202C

This firmware release supports the new models LIP-ME201C and LIP-ME202C. The LIP-ME202C is a BACnet/IP router with two MS/TP ports. Both models have an LCD display, dual Ethernet and a built-in firewall.

Project Documentation

A new feature on the device is a Web UI for creating and viewing project documentation on the device. The documentation editor requires admin rights and allows storing files on the device or creating documentation links as URLs. Both items can be viewed by guest users. Examples include storing cabling plans as PDF or adding links to a Web site containing manuals, plans or other useful project documentation.

4.11 New in LIP-ME20X 5.1.0

This section describes the major changes and new features. For a full list of changes refer to the Readme file.

Dual-Ethernet with Separate Networks

LIP-ME20X models with two Ethernet interfaces can now be configured to work with separate and isolated IP networks. For example, one Ethernet interface can be accessed over HTTPS from a WAN connected to Ethernet 2 while the building network services are running locally on the LAN connected to Ethernet 1. For configuration the device provides separate Ethernet tabs in the port configuration, which allow selecting the offered services on each interface. The example in Figure 16 shows a WAN interface with HTTPS and OPC UA only, while BACnet/IP is still bound to Ethernet 1 (LAN).

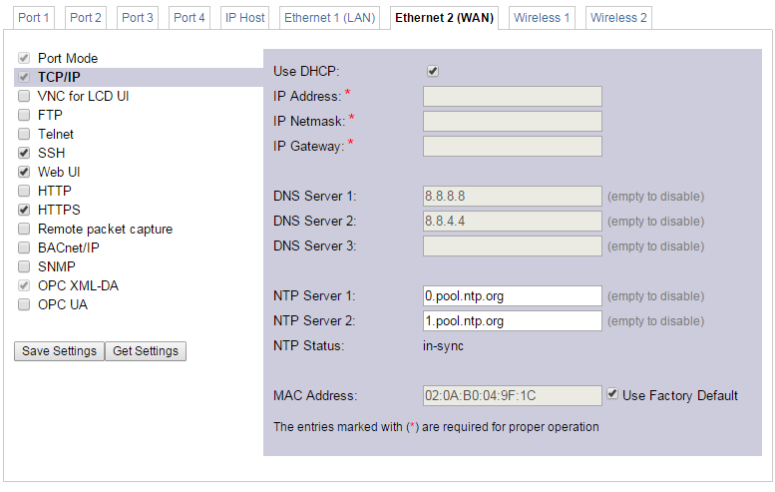


Figure 16: New Ethernet 2 (WAN) tab

WLAN Interface

In combination with the external LWLAN-800 interface, the device provides new interface tabs for wireless IP networks. Similar to the second Ethernet interface, one can choose which protocols are available on the wireless network. The wireless interface can be configured as a WLAN client, access point or mesh node. Using the latter, a wireless mesh network of LOYTEC devices can be built.

Web Interface

The Web interface of the device offers a number of new features:

- A new device info page provides a quick overview of all relevant operational parameters, such as CPU load, active protocols, time synchronization and many more.
- A new firmware upgrade menu on the Web interface allows online checking for firmware updates and upgrading by selecting a local firmware file.

OPC UA Server

The OPC server on the devices, which support security, has been extended by an OPC UA server. This supports the OPC UA binary protocol and exposes the same OPC tags as the well-known OPC XML-DA server. In addition OPC UA offers superior security features as well as slimmer data transfers. For more information on the OPC UA server please refer to respective Section in the L-INX/L-GATE User Manual [2].

SNMP

For accessing vital operational data in standard IT equipment, LIP-ME20X devices offer an SNMP management base (MIB). All system registers are available in that MIB. The MIB file can be downloaded from the device and imported in the SNMP management tool. Alarms on the device can be exposed as SNMP traps..

5 Quick-Start Guide

This chapter provides the minimum list of steps necessary to setup the LIP-ME20X.

5.1 Hardware Installation and IP Connection

- Connect power, Ethernet, and MS/TP (Section 6.6).
- The device is shipped with DHCP. The IP address is displayed on the LCD display.
- If a static IP configuration is required, configure the IP address using the jog dial on the LCD display (Section 5.2.2).
- Reboot the LIP-ME20X to commit the new IP settings.

5.2 Configuration of the LIP-ME20X

5.2.1 Configuration on the Web Interface

- Open your Web browser and type in the IP address shown on the LCD display or type in 'loytec.local'. As a first step you will be asked to enter passwords for the administrator and operator accounts before proceeding. Only strong passwords are accepted.
- Then click on **Config** menu. Click on **BACnet Config** and setup the BACnet Device Configuration (see Section 3.2.17 BACnet Configuration in the LOYTEC Device User Manual [1]).
- Click on **Port Config** and setup the BACnet/IP and BACnet MS/TP port configuration (see Section 3.2.18 BACnet/IP Configuration and Section 3.2.20 BACnet MS/TP Configuration in the LOYTEC Device User Manual [1]). Make sure to set distinct network numbers, which is required by the router to operate.
- If the LIP-ME20X should also act as a BBMD, click on **BACnet BDT** and setup the Broadcast Distribution Table (see Section 3.2.24 BACnet BDT Configuration in the LOYTEC Device User Manual [1]).
- Reboot the LIP-ME20X to commit the changes.

5.2.2 Configuration on the LCD Display

Device models with an LCD display can also be configured to their basic settings through jog dial navigation on the LCD UI. Turn the jog dial to navigate between menu items 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. Some input fields provide acceleration. This means turning faster changes the value in larger increments.

To Set the IP Address on the LCD Display

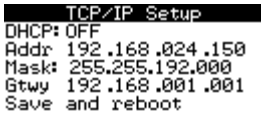
1. On the LCD main screen set the desired language. Navigate to the flag symbol, press the button and choose the desired language.



2. Navigate to the IP address on the main screen and press the button.



3. There navigate to the needed input fields, press and change the value. Press again to set the value. Continue to the next field.



4. Finally navigate to **Save and reboot** and press.

5. Acknowledge the reboot and the device reboots with the new IP address.

To Configure the BACnet Device ID Over the LCD Display

1. On the LCD main screen navigate to **Device Settings »»**.

2. Then navigate to the menu **BACnet »»**.

3. In that menu navigate to the **ID** input for entering the device ID. The field is split into two controls, one for the thousands and one for singles, to simplify entering big numbers.



4. After the device ID has been entered the device name is automatically assembled using that device ID, if no other name has been configured on the Web UI.

5. On a BACnet router navigate to the **BAC/IP Net** menu item and enter the BACnet network ID of the BACnet/IP network. Then choose the appropriate **MS/TP Net** number for each available MS/TP port. Note, that the network IDs must be unique in the entire BACnet network. To disable the router port, scroll down till **off** appears.

6. To let the changes take effect, the device needs to be rebooted. For doing this now you may select the menu item **Save and reboot**.

5.3 Remote Protocol Analyzer

The LIP-ME20X is equipped with a built-in Ethernet, BACnet/SC and MS/TP protocol capture facility. This facility can be used for local offline logging, which stores a log file on the device, or online remote logging with Wireshark. With remote capture a Wireshark protocol analyzer on the PC can capture a live log of the MS/TP channel or the Ethernet port. On models with multiple MS/TP ports a logging facility is available on each port. For doing so, the remote capture has to be enabled. See Section 8.2 for more details.

5.4 Reset to Factory Defaults

In case the password of the device has been forgotten you may need to reset the device back to factory defaults to gain access again. On the LIP-ME201 press the service button and power-cycle the device. Keep the button pressed until the port LEDs illuminate orange permanently. Release the button within five seconds from that time on to reset the device to factory defaults.

On the models with an LCD display go to the menu to **Device Settings »»**. Then choose **Device Management »»** and select **Factory Default**. Acknowledge with **YES** which reboots the device into factory default settings.

6 Hardware Installation

6.1 Enclosure

The enclosure of the product and its terminal layout are shown on the installation sheet found in the product's box.

6.2 Product Label

The product label on the side of the LIP-ME20X contains the following information (see Figure 17):

- LIP-ME20X order number and date code,
- serial number with bar-code (Ser#).

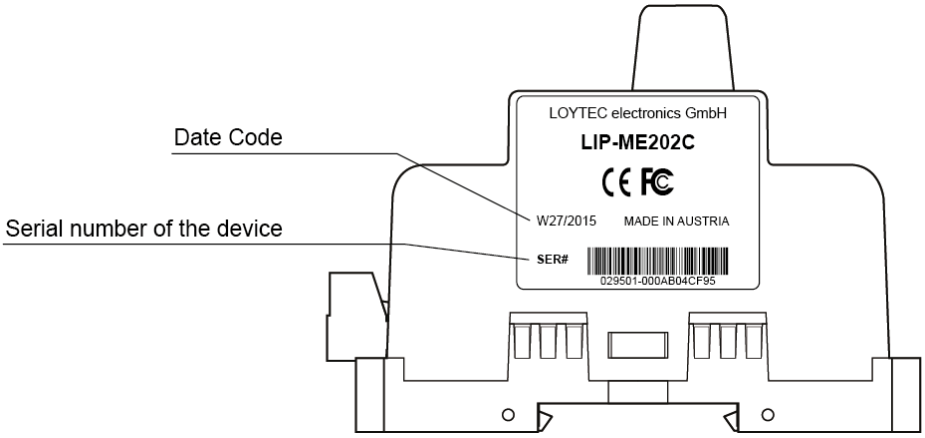


Figure 17: Example product label.

Unless stated otherwise, all bar codes are encoded using "Code 128". An additional label is also supplied with the device for documentation purposes. The specific contents of the product label are shown on the installation sheet found in the product's box.

6.3 Mounting

The device comes prepared for mounting on DIN rails following DIN 50 022. The device can be mounted in any position. However, an installation place with proper airflow must be selected to ensure that the LIP-ME20X's temperature does not exceed the specified range (see Chapter 10).

6.4 LED Signals

6.4.1 MSTP Activity LED

The MS/TP port has a three-color MSTP Activity LED. Table 2 shows the different LED patterns of the port and their meaning. A permanent color reflects a state. Flicker is for 25 ms when there is activity on the MS/TP data link layer.

Behavior	Description	Comment
GREEN permanently, flicker off	Multi-Master, token ok, flicker when traffic	Normal condition on a multi-master MS/TP network.
ORANGE flicker	Sole master, flicker when traffic	Normal condition on a single-master MS/TP network.
RED permanent, flicker GREEN	Token lost state, flicker when transmit attempt	Cable might be broken.
RED flash fast	Transmission or receive errors	This indicates bad cabling.

Table 2: MS/TP Activity LED Patterns

6.5 LCD Display and Jog Dial

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 18. It displays the device's IP address, hostname, CPU load, system temperature and supply voltage.

Below are menu items. Turn the jog dial to navigate between menu items 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 18: 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 19.



Figure 19: 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.

- **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-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.

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

The **Device Settings »»** menu also allows configuring basic BACnet settings. Navigate to the **BACnet »»** sub-menu, which is displayed in Figure 19.



Figure 20: 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.

6.6 Wiring

The wiring information of the product and its terminal layout are shown on the installation sheet found in the product's box.

7 Firmware Update

The LIP-ME20X firmware supports remote firmware upgrade over the network and the USB port.

To guarantee that the LIP-ME20X is not destroyed due to a failed firmware update, the firmware consists of two images:

- LIP-ME20X fallback image,
- LIP-ME20X primary image.

The LIP-ME20X 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 LIP-ME20X boots up with the fallback image, the port LEDs are flashing red.

The firmware image is distributed in a firmware ZIP archive that applies to all LIP-ME20X models

7.1 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 refer to the LOYTEC Device User Manual [1].

7.2 Firmware Update Via the USB Port

The device's firmware can be upgraded using a USB memory stick. The LCD display provides a menu to select and perform the upgrade. Select **Device Management »» USB Storage »» Firmware Update** and choose the firmware file. For more details refer to the LOYTEC Device User Manual [1].

8 Troubleshooting

8.1 Technical Support

LOYTEC offers free telephone and e-mail support for our LIP-ME20X product. If none of the above descriptions solves your specific problem please contact us at the following address:

Delta Intelligent Building Technologies (Europe) GmbH
Blumengasse 35
A-1170 Vienna
Austria / Europe

e-mail : ***support@loytec.com***
web : ***https://www.loytec.com***
tel : ***+43/1/4020805-100***

or

Delta Intelligent Building Technologies (Canada) Inc.
17850 56 Ave
Surrey, BC V3S 1C7
CANADA

e-mail: ***support@loytec-americas.com***
web: ***https://www.loytec.com***
tel: ***+1 800.335.8221***

8.2 Packet Capture

Please refer to the Troubleshooting Chapter in the LOYTEC Device User Manual [1] to learn more about packet capture on the LOYTEC device.

9 Security Hardening Guide

This guide contains security-relevant information for operating the product on IT networks. The information refers to the firmware version and the instructions found in the previous chapters of this User Manual.

9.1 Installation Instructions

Install the device over the Web interface:

- Set up the BACnet protocol settings as described in Section 5.2.1. When connecting over the Web UI use https:// in the URL.
- Set a secure password for the admin and operator accounts.
- Disable the HTTP, FTP, and Telnet servers in the IP port configuration as described in the LOYTEC Device User Manual [1]. Note, that FTP and Telnet are disabled in factory defaults as of firmware 7.0.0.
- Create a new HTTPS server certificate as described in the LOYTEC Device User Manual [1].
- Set a password for the "guest" user or disable the guest user to protect information of the device info page from unwanted disclosure.

9.2 Firmware

The device is equipped with one piece of software. This is the firmware image and its related firmware version. The firmware is distributed as a downloadable file. The device can be upgraded by placing the firmware image onto the device using the procedure described in Chapter 7. The device firmware is signed by LOYTEC and its signature integrity is verified before the upgrade is allowed. If the firmware's signature cannot be verified, the upgrade is not performed and the file is deleted.

Firmware Upgrade Cyber Security Disclaimer

LOYTEC regularly releases firmware updates that address security vulnerabilities. Failing to install a security update leaves the device exposed to known and documented security threats, which may result in unauthorized access to the device, modification or disclosure of configuration and confidential user data, or disruption of building automation operation. LOYTEC disclaims liability for security incidents, accidents, or failures that are attributable to the use of a product on which available security updates have not been installed. It is the explicit obligation of the user to install any security updates promptly as soon as published by LOYTEC.

9.3 Ports

This Section lists all ports, which may be used by the device. The ports are default settings for their respective services. If not stated otherwise, the ports can be changed.

Required Ports:

- 47808 udp: This is the data exchange port for BACnet/IP. It is required for the primary function of the device to exchange control network data between routers over the IP network. Each device needs this port open. The port can be changed.

Optional ports not necessary for the primary product function. They can be disabled as described in the installation instructions in Section 9.1:

- 21 tcp: This port is opened by the FTP server. The port can be changed and disabled.
- 22 tcp: This port is opened by the SSH server. The port can be changed and disabled.
- 23 tcp: This port is opened by the Telnet server. The port can be changed and disabled.
- 80 tcp: This port is opened by the Web server. It should be disabled and HTTPS (port 443) be used instead. The port can be changed.
- 161 tcp: This port is opened by the SNMP server. This port is disabled by default. The port can be changed.
- 443 tcp: This port is opened by the secure Web server for HTTPS. It can be disabled.
- 2002 tcp: This port is opened by the Wireshark protocol analyzer front-end. This port is disabled by default. The port can be changed.
- 4840 tcp: This port is opened by the OPC UA server. This port is disabled by default. The port can be changed.
- 5353 udp: This port is open for finding the device using mDNS names such as loytec.local. This port can be disabled.
- 1900 udp: This port is open for the SSDP discovery service. It cannot be disabled.
- 5900 tcp: This port is opened by the VNC server, if it is enabled. This port is disabled by default. The port can be changed.

9.4 Services

Required services:

- BACnet/IP or BACnet/SC: Primary function of the device. This service is in accordance with the standard ANSI/ASHRAE 135-2024.

Optional services not necessary for the primary product function. They can be disabled as described in the installation instructions in Section 9.1:

- mDNS: This service is used for finding the device via multicast DNS in order to establish initial communication. This allows using DNS names such as loytec.local in the Web browser. This service can be disabled.
- HTTP: Web server. It provides a Web-based configuration UI. The Web UI can be disabled after setting up the device.
- FTP: FTP server. It is used for firmware upgrade and access to the log file.
- Telnet: Telnet server. It provides access to the device console menu over the network.
- SSH: SSH server. It provides secure access to the device console menu over the network.
- HTTPS: Secure Web server. It provides a Web-based configuration UI using HTTPS.
- VNC: The VNC server can be used for remote access to the LCD display on devices that have it. The service is disabled by default.
- OPC UA: This secure service provides access to data points over the OPC UA standard. The service is disabled by default.

- SNMP: SNMP server. It provides network management information on the device used by standard IT tools. The service is disabled by default.
- Wireshark front-end: The Wireshark protocol analyzer may connect to this service and retrieve online protocol analyzer logs. The service is disabled by default.

9.5 Upgrade Key Strength

The secure services (HTTPS, SSH) rely on certificates to authenticate the device against the connecting client. This is key to prevent man-in-the-middle attacks. The device comes with pre-installed server certificates. It is recommended to upgrade the pre-installed certificate to an individual server-certificate and use stronger key length.

- Server certificate (for HTTPS, OPC UA): Follow the instructions in the LOYTEC Device User Manual [1] Section 3.2.29 Certificate Management on how to upgrade the pre-installed X.509 server certificate to a custom, self-signed or CA-signed certificate with stronger key length.
- SSH key upgrade: If SSH is enabled it is recommended to upgrade the SSH key length. Refer to the LOYTEC Device User Manual [1] Section 3.2.28 SSH Server Config on how to upgrade your RSA key to 2048 bits.

9.6 Logging and Auditing

The device contains a log file, which can be read out over SSH or the Web server. This log contains information when the device started and when crucial communication errors occur. Other information such user log-on are not logged as they are not part of the primary services of this device.

Logged events:

- Time of the last power-on reset of the LIP-ME20X device.
- Time and version of the last firmware upgrade.
- Time when the device configuration has been cleared or the device was reset to factory defaults.
- Static errors in the device configuration.
- System overload situations as one-time log messages since last power-on.
- Crucial communication errors.
- Logins and login failures.
- Failed firmware upgrade attempts.

9.7 Network Access

Network access can be protected by using 802.1X port authentication (as of firmware 7.4.0) using EAP-TLS, PEAP, or TTLS. Unused Ethernet ports can be disabled.

9.8 Password Protection

Devices provide separate administrative (admin) and operative (operator) user accounts. Passwords are not stored, only a strong cryptographic hash (salted SHA256) thereof. Device login is protected by a login trap that blocks logins for 10 seconds after ten consecutive failed

login attempts using different passwords to protect against brute-force password attacks. Initial password setting is enforced to use strong passwords. Without setting the initial password, the device functionality is locked down. Passwords can be up to 64 characters long and contain any printable UTF-8 character.

To protect usage of the admin password, the admin user can create additional user accounts with an admin role. Those additional user accounts can be disabled as needed. Usernames can be up to 32 characters. The built-in user accounts can be disabled, if custom user accounts with those roles have been created.

9.9 Encryption-At-Rest

Client credentials required for operation (e.g., E-Mail client) are stored in encrypted storage using AES256-CBC with nonce. The secret encryption key is bound to the device and cannot be accessed or read out of the device. Credentials can be exported or imported encrypted by a project password and PBKDF-2.

9.10 Secure Disposal and Decommissioning

Before disposing of, reselling, or returning a LOYTEC device, the user must erase all protected information assets (communication and security configuration, user-set values, personal data, authentication values, and cryptographic keys) to prevent disclosure. To safely terminate use of a LOYTEC device:

1. Back up any required configuration (device backup protected by project password).

2. Perform a **factory reset / restore to defaults** (see LOYTEC Device User Manual). This erases all user data, user-set values, and credentials. The firmware version is retained.

3. If applicable, remove and physically destroy any SD card or removable storage media, or securely erase it.

4. Remove the device from any VPN, 802.1X, or management system (revoke its certificates and credentials in those systems).

5. Dispose of electronic waste in accordance with local regulations (e.g., WEEE in the EU).

Important! *Devices sold or disposed of with protected information assets not erased as described may expose configuration data, credentials, and building automation project data to the new owner of the device.*

9.11 Information Policy

LOYTEC follows a policy for reporting, documenting and informing about potential security vulnerabilities and advisories:

1) The LOYTEC Web site offers a mailing list subscription to receive security-related information in a timely manner.
2) The LOYTEC Web site provides an interface to report any potential security vulnerabilities related to LOYTEC products. Incident reports can also be sent to security@loytec.com. A response will be sent with a trackable identifier. LOYTEC accepts security reports following common responsible disclosure practices containing technical information on how to reproduce the issues, exploit scripts or other information allowing to identify and close critical security issues.

3) LOYTEC commits to providing security fixes for zero-day exploits within 96 hours after their discovery. All other security-related fixes will be made available in the next firmware patch within 30 days.

10 Specifications

10.1 Physical Specifications

10.1.1 LIP-ME201C, LIP-ME202C

Operating Voltage	20-30 VAC/DC
Power Consumption	typ. 2.5W
In rush current	up to 950 mA @ 24 VAC
Operating Temperature (ambient)	0°C to +50°C
Storage Temperature	–10°C to +60°C
Humidity (non condensing) operating	10 to 90 % RH @ 50°C
Humidity (non condensing) storage	10 to 90 % RH @ 50°C
Enclosure	Installation enclosure 107 mm wide, DIN 43 880
Environmental Protection	IP 40 (enclosure); IP 20 (screw terminals)
Installation	DIN rail mounting (EN 50 022) or wall mounting

10.1.2 LIP-ME204C

Operating Voltage	20-30 VAC/DC
Power Consumption	typ. 2.5W
In rush current	up to 950 mA @ 24 VAC
Operating Temperature (ambient)	0°C to +50°C
Storage Temperature	–10°C to +60°C
Humidity (non condensing) operating	10 to 90 % RH @ 50°C
Humidity (non condensing) storage	10 to 90 % RH @ 50°C
Enclosure	Installation enclosure 159 mm wide, DIN 43 880
Environmental Protection	IP 40 (enclosure); IP 20 (screw terminals)
Installation	DIN rail mounting (EN 50 022) or wall mounting

10.2 Resource Limits

Table 3 specifies the resource limits of the LIP-ME models.

Limits \ Model	201C	202C	204C
BDT max recommended	100	100	100
MS/TP ports	1	2	4
LWLAN-800 AP+Mesh max clients	7	7	7

Table 3: Resource limits of the LIP-ME20X

11 References

[1] LOYTEC Device User Manual 8.6, Delta IBT (Europe) GmbH, Document № 88086514, August 2026.

[2] L-INX/L-GATE User Manual 8.6, Delta IBT (Europe) GmbH, Document № 88073033, August 2026.

[3] LWEB-900 User Manual 4.6, Delta IBT (Europe) GmbH, Document № 88081412, March 2026.

12 Revision History

Date	Version	Author	Description
2008-10-07	1.0	AB	Initial revision.
2010-05-07	1.2	TP	Add Operating Interfaces section. Revise Web Interface section.
2011-06-17	2.0	STS	Updated for LIP-ME201 firmware 2.0. Removed Section 4 Console UI, Section 4.2.8: new BDT settings, added Section 4.2.9 BACnet ACL, added Section 6 Network Media, added Section 8.2 Statistics on the Console, added Section 8.2.5 BBMD Communications Test.
2012-06-14	4.5	STS	Updated Section 4.3.3 MS/TP statistics. Added Chapter 9 Security Hardening Guide.
2013-02-12	4.8	STS	Updated Section 4.2.5 BACnet Device Configuration. Added Section 8.3 MS/TP Remote Packet Capture.
2013-09-05	4.9	STS	Added Section 4.2.10 BACnet Slave Proxy Web UI. Updated Section 8.3 Remote Packet Capture with Ethernet capture. Defined BDT limits in Section 10.1.2.
2015-01-26	5.1	STS	Updated for firmware version 5.1. Added LIP-ME204 models. Added Section 1.2 LIP-ME20X Models. Added Section 2.1 New in LIP-ME20X 5.1.0. Added Section 4.6 LCD Display and Jog Dial. Section 5.1 Device Information and Account Management updated. Section 5.2.4 IP Configuration updated. Added Section 5.2.5 Using Multiple IP Ports. Section 5.2.6 IP Host Configuration updated. Added Section 5.2.7 WLAN Configuration. Added Section 5.2.11 BACnet Time Master. Added Section 5.2.15 Firmware. Added Section 5.2.16 SNMP. Added Section 6.2 SNMP Interface. Added Section 7.2 Redundant Ethernet. Added Section 7.3 WLAN.
2015-07-24	5.3	STS	Updated for firmware version 5.3. Added LIP-ME201C, LIP-ME202C models. Updated Section 3.2.2 Configuration on the LCD display. Added Sections 5.2.17 and 5.4 on project documentation. Updated Chapter 10 Security Hardening Guide.
2020-05-27	7.2	STS	Re-organized User Manual structure, branched out common parts into LOYTEC Device User Manual. Updated for firmware version 7.2. Removed LIP-ME201 model.
2021-01-29	7.4	STS	Updated for firmware version 7.4.0. Updated Chapter 9 Security Hardening Guide.
2022-01-30	7.6	STS	Updated for firmware version 7.6.0. Updated Chapter 9 Security Hardening Guide.
2023-03-30	8.0	STS	Updated for firmware version 8.0.0. Added BACnet/SC router in Section 1.2.
2023-12-30	8.2	STS	Updated for firmware version 8.2.0.
2025-07-30	8.4	STS	Updated for firmware version 8.4.0. Updated Chapter 9 Security Hardening Guide.
2026-08-30	8.6	STS	Updated the company name throughout the manual. Updated for firmware 8.6.0. Section 1.2: Added BACnet/SC hub function to models table. Chapter 9 Security Hardening Guide: Added Firmware Upgrade Cyber Security Disclaimer and Secure Disposal and Decommissioning section. Section 10.1 Updated operating voltage specification to 20-30 VAC/VDC.