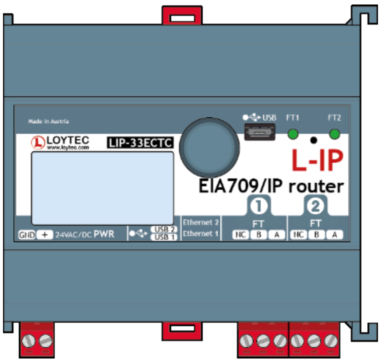
L-IP™

CEA-709/IP Router

User Manual

LOYTEC electronics GmbH



Contact

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

Version 8.4.0

Document № 88065919

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.

Contents

Abbreviations

10Base-T	10 Mbps Ethernet network with RJ-45 plug
Aggregation	Collection of several CEA-709 packets into a single CEA-852 packet
BOOTP	Bootstrap Protocol, RFC 1497
CC	Configuration Client, also known as CEA-852 device
CN	Control Network
CN/IP	Control Network over IP
IP-852 channel	logical IP channels that tunnels CEA-709 packets according CEA-852
CN/IP packet	IP packet that tunnels one or multiple CEA-709 packet(s)
CR	Channel Routing
CS	Configuration Server that manages CEA-852 IP devices
DHCP	Dynamic Host Configuration Protocol, RFC 2131, RFC 2132
DNS	Domain Name Server, RFC 1034
CEA-709	Protocol standard for control networks
CEA-852	Protocol standard for tunneling CEA-709 packets over IP channels
IP	Internet Protocol
LSD Tool	LOYTEC System Diagnostics Tool
MAC	Media Access Control
MD5	Message Digest 5, RFC 1321
NAT	Network Address Translation, RFC 1631
SL	Send List
SNTP	Simple Network Time Protocol
VNI	Virtual Network Interface

1 Introduction

1.1 Overview

1.1.1 L-IP

The L-IP is a high performance, reliable, and secure network infrastructure component for accessing CEA-709 network nodes over the Internet. It can be used to connect remote retail branches over the Internet, build high-speed backbone channels, or to act as a network interface for LNS-based network management tools. Its built-in configuration server manages up to 256 IP devices on one IP channel without the need for a dedicated management PC. The L-IP can be used behind NAT routers and firewalls, which allows seamless integration in already existing Intranet networks. It supports DHCP even with changing IP addresses in an Intranet environment. Easy to understand diagnostic LEDs allow installers and system integrators to install and troubleshoot this device without expert knowledge and dedicated troubleshooting tools. The L-IP 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. Advanced built-in network statistics and network diagnostics capabilities allow fast network installation and guarantee reliable operation over the entire lifetime of the network. The automatic IP connection keep-alive functionality maintains IP connections during bus idle times. The multi-port version of the L-IP combines the functionality of two L-IPs in one device. This device is equipped with a 100-BaseT Ethernet port (CEA-852) and up to four FT-10 ports (CEA-709).

The L-IP perfectly integrates with our L-Switch multi-port router devices to form a high performance, fully manageable, highly reliable network infrastructure for your CEA-709 networks. Its smart routing software automatically detects the bit-rates of the connected channels, learns the configuration of the network (domains, subnet/node addresses, group addresses) and forwards the packets between the different ports. Thus, using the L-IP together with L-Switch devices and structured wiring is an easy and cost effective way to avoid performance problems on the communication media.

Like the L-Switch the L-IP permanently collects statistics information from the attached network channels (channel load, CRC errors, forwarding statistics, etc.). Using this data the L-IP software is able to detect problems on these channels (overload, connections problems, etc.) and warns the system operator via LEDs (see Section 6.4.10). An intuitive user interface allows fast and easy network troubleshooting without any additional analysis tools and deep system knowledge. The LSD Tool can be used for a more detailed view of the collected statistics data. See Chapter 15 for more information on this powerful system diagnostics tool.

The built-in web server allows convenient device configuration through a standard web browser like Internet Explorer or Firefox. The web interface also allows backup and restoring the configuration of the configuration server and it provides statistics information for system installation and network troubleshooting.

Starting with firmware version 2.0 the L-IP supports remote LPA operation. Remote LPA is an advanced trouble shooting tool that streams the CEA-709 packets on the FT-10 or TP-1250 channel over the IP network to a protocol analyzer connected to the IP network. This allows remote troubleshooting of the local CEA-709 channels without actually being physically attached to this channel. Please consult our product literature for the LPA-IP to learn more about this IP protocol analyzer. This tool is a must for every system integrator using IP-852 channels.

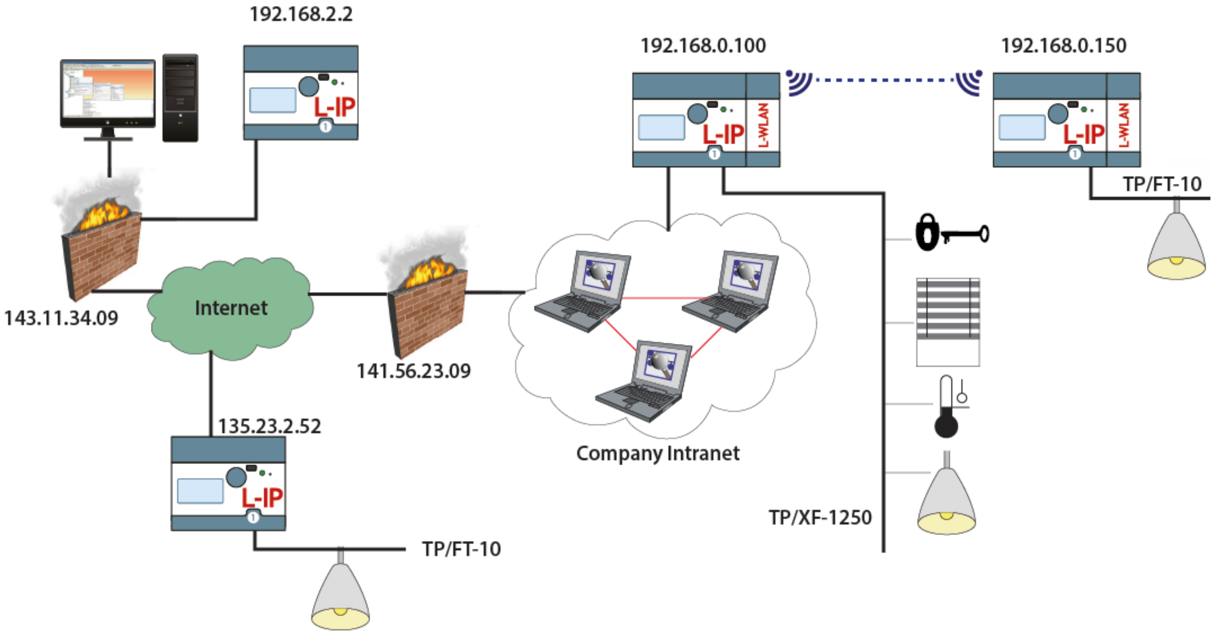


Figure 1: L-IP application example behind and without firewalls and NAT routers

The L-IP series “C” models (product code ending with C) come with two Ethernet ports and the device setup can be done easily on the LCD display. The remote Wireshark packet capture feature is also available.

In addition the L-IP series “C” 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 CEA-852 network can be entirely isolated from the configuration interface. OpenVPN support enables secure remote management.

For perfect integration into building management software such as the LWEB-900 by LOYTEC, the L-IP series “C” models 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 these L-IPs can operate CEA-852 on the WLAN. By setting up an access point on the Ethernet network, the device can be used to distribute FT channels on a wireless network.

The L-IP is used for:

- Tunneling CEA-709 packets over IP channels (Intranet/Internet)
- Connecting CEA-709 networks over the Internet in a secure way
- Building high-performance backbone channels using existing IP infrastructure

- Connecting CEA-709 networks between different sites
- Configuration Server for IP-based devices
- Network interface for LNS based network management tools (LonMaker, NL-220)
- Isolation of local network traffic
- Structuring networks
- Extending channels in their physical dimension and/or number of nodes
- Connecting channels with different communication media types
- Network monitoring and network management
- Remote LPA functionality
- Connecting CEA-709 networks behind NAT routers
- Connecting CEA-709 networks over WLAN

1.1.2 L-IP Redundant

The L-IP Redundant CEA-709/IP Router is a perfect solution for networks where a high reliability in the communication is required. It is a member of the L-IP family, based on the standard L-IP router and adds functionality which allows building redundant network infrastructure.

An L-IP Redundant CEA-709/IP Router can be used as a single device to achieve the redundancy on the CEA-709 (TP/FT-10) channel by building a ring structure. Full Redundancy on the IP-Channel[1] and on the CEA-709 channel can be achieved with two devices installed in parallel. In this case device redundancy is ensured as well by mutual monitoring of paired L-IP Redundant devices.

In addition the L-IP Redundant CEA-709/IP Router monitors the nodes on the TP/FT-10 channel and creates an alarm if a node gets offline. Thereby a cable break on the TP/FT-10 channel can be easily located. The L-IP Redundant only supports the “Configured Router Mode”.

As an IP-Router the L-IP Redundant CEA-709/IP Router can tunnel CEA-709 packets back and forth through an arbitrary IP based network, such as a LAN, an Intranet, or even the Internet. The Router connects to the IP network via an Ethernet channel. The IP configuration can either be obtained via DHCP or entered manually. The user only needs to provide the IP address of an CEA-852 configuration server. If operated behind a router with network address translation (NAT or masquerading), the L-IP Redundant CEA-709/IP Router supports Auto-NAT to work with dynamic public IP addresses. When using the built in CEA-852 configuration server, the user can edit and backup the IP channel configuration through the built-in web server. The configuration is stored persistently and the device operates completely standalone. After installation, the L-IP Redundant CEA-709/IP Router is ready to route packets between the CEA-709 network (ring structure) and the IP network. Thus, all CEA-709 networks connected to L-IP Routers can exchange data over the IP-852 channel. If connected to untrusted networks, such as the Internet, all CEA-852 packets can be authenticated by an MD5 checksum and time stamps. Besides its primary router operation, the L-IP Router is a powerful network diagnostics device. Its simple and intuitive user interface provides an immediate overview over the network status. Both the IP-852 channel

[1] Redundancy on the IP-Channel requires a redundant IP network infrastructure.

and CEA-709 network can be observed with status LEDs. For trouble-shooting, the Router supports the remote LPA (LOYTEC Protocol Analyzer) functionality so that the network can be analyzed from any PC connected to the Internet. With the L-IP Redundant CEA-709/IP Router, setting up a redundant network which is comfortable to maintain becomes an easy task.

The L-IP Redundant is used for:

- Creating redundant CEA-709 network infrastructure
- Monitoring a TP/FT-10 channel (ring structure) on cable break
- Ensuring communication on the TP/FT-10 channel in case of a single cable break
- Monitoring health state of nodes in a CEA-709 network
- Determine location of a cable break
- Full redundancy with two L-IP Redundant CEA-709/IP Router in parallel for the IP-Cannel and the CEA-709 channel
- Device redundancy by mutual monitoring of paired Redundant L-IPs
- Messages and alarming via SNVTs and LonMark-Alarming via Node Object

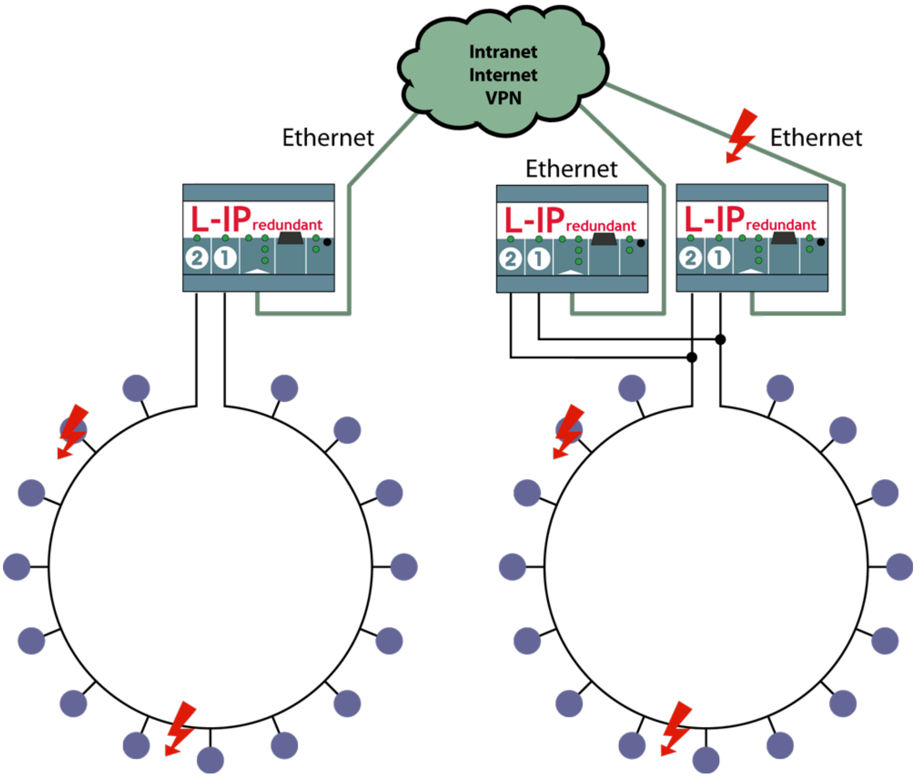


Figure 2: Using L IP Redundant with redundant ring structure and device redundancy

1.2 L-IP Models

This Section provides an overview of the different L-IP 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-33ECRB	LIP-1ECTC	LIP-3ECTC	LIP-13ECTC	LIP-33ECTC	LIP-3333ECTC
CEA-709 Router	✓	✓	✓	✓	✓	✓
Redundant Router	✓					
CEA-709 Ports	2	1	1	2	2	4
Remote LPA	✓	✓	✓	✓	✓	✓
OPC XML-DA		✓	✓	✓	✓	✓
OPC UA		✓	✓	✓	✓	✓
SNMP		✓	✓	✓	✓	✓
LCD Display		✓	✓	✓	✓	✓
Serial Console, DIP switches	✓					
USB		✓	✓	✓	✓	✓
Ethernet Switch/Hub		✓	✓	✓	✓	✓
WLAN, LTE		✓[1]	✓[1]	✓[1]	✓[1]	✓[1]
SSH, HTTPS, Firewall, VPN		✓	✓	✓	✓	✓

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

Table 1: Available features in different L-IP models.

1.3 Scope

This document covers L-IP devices with firmware version 8.4.0.

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 16) 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.

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 L-IP

4.1 New in L-IP 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.

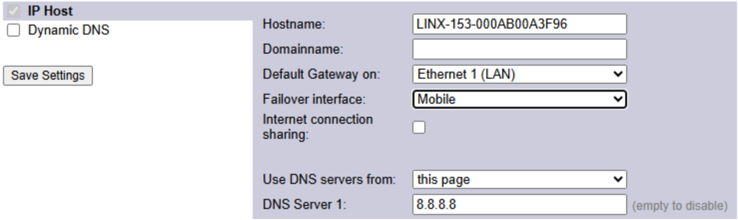
The new “view” role has been added that allows a user to view configuration settings only. A view user cannot change any configuration settings.

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.



☑ IP Host
☐ Dynamic DNS

Hostname: LINX-153-000AB00A3F96
Domainname:
Default Gateway on: Ethernet 1 (LAN)
Failover interface: Mobile
Internet connection sharing: ☐
Use DNS servers from: this page
DNS Server 1: 8.8.8.8 (empty to disable)

Figure 3: Configuration of an Internet failover interface.

4.2 New in L-IP 8.2.8

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

Support new LIP-13ECTC model

The LIP-13ECTC is a multi-port L-IP router with one TP-1250 port, one FT-10 port and an IP-852 channel.

Add L-Switch Mode

A new device operation mode has been added: L-Switch mode. This mode is available for multi-port L-IP models (i.e., that have more than one CEA-709 port). In L-Switch mode, the IP-852 interface is disabled and the device behaves like an L-Switch between the CEA-709 ports. This mode is fully plug-and-play and can be setup on the LCD display. No further configuration on the Web interface is required. That makes the L-IP an ideal drop-in replacement for common third-party LON routers.

4.3 New in L-IP 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

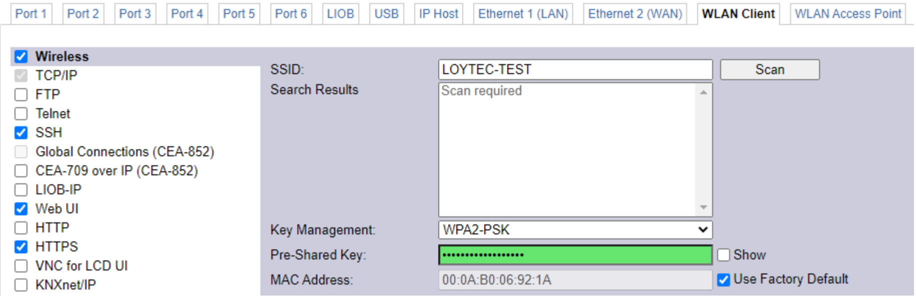
The new L-IP models based on A64 hardware are now supported. The new firmware also contains a major security upgrade to OpenSSL 3.1.

4.4 New in L-IP 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

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.



☑ Wireless
☑ TCP/IP
☐ FTP
☐ Telnet
☑ SSH
☐ Global Connections (CEA-852)
☐ CEA-709 over IP (CEA-852)
☐ LIOB-IP
☑ Web UI
☐ HTTP
☑ HTTPS
☐ VNC for LCD UI
☐ KNXnet/IP

SSID: LOYTEC-TEST
Search Results: Scan required
Key Management: WPA2-PSK
Pre-Shared Key: •••••••••••••••••• ☐ Show
MAC Address: 00:0A:B0:06:92:1A ☑ Use Factory Default

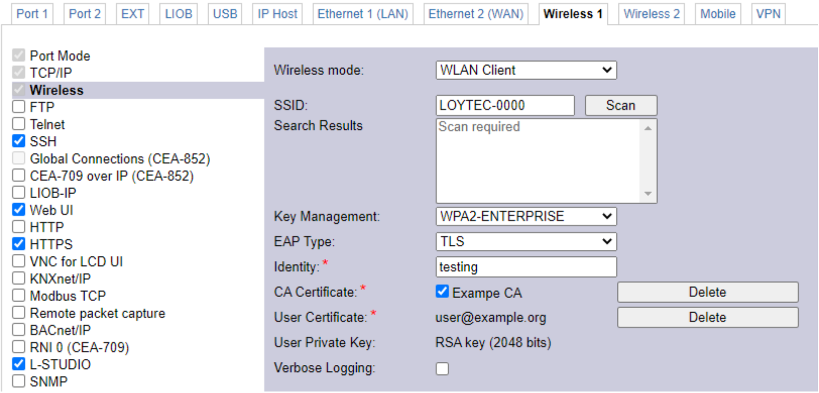
Figure 4: New WLAN configuration tabs

4.5 New in L-IP 7.6.0

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

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.



☑ Port Mode
☑ TCP/IP
☑ Wireless
□ FTP
□ Telnet
☑ SSH
□ Global Connections (CEA-852)
□ CEA-709 over IP (CEA-852)
□ LIOB-IP
☑ Web UI
□ HTTP
☑ HTTPS
□ VNC for LCD UI
□ KNXnet/IP
□ Modbus TCP
□ Remote packet capture
□ BACnet/IP
□ RNI 0 (CEA-709)
☑ L-STUDIO
□ SNMP

Wireless mode: WLAN Client
SSID: LOYTEC-0000 Scan
Search Results: Scan required
Key Management: WPA2-ENTERPRISE
EAP Type: TLS
Identity: * testing
CA Certificate: * ☑ Exampe CA Delete
User Certificate: * user@example.org Delete
User Private Key: RSA key (2048 bits)
Verbose Logging: □

Figure 5: Configure WiFi Enterprise

4.6 New in L-IP 7.4.0

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

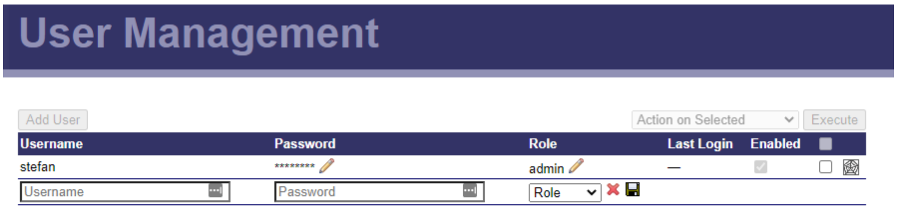
New Menu Structure on Web UI

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.



User Management

Add User | Action on Selected | Execute

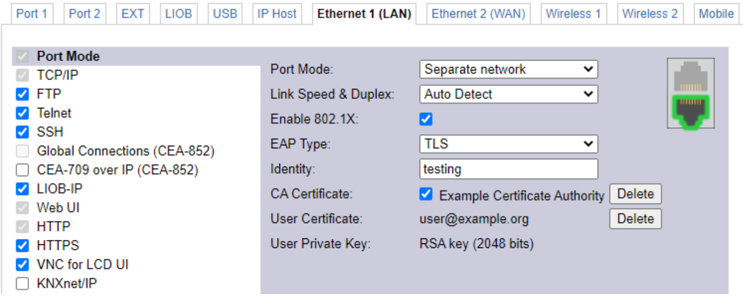
Username	Password	Role	Last Login	Enabled	□
stefan	********	admin	—	☑	□
Username	Password	Role			

Figure 6: 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.



Port 1 | Port 2 | EXT | LIOB | USB | IP Host | **Ethernet 1 (LAN)** | Ethernet 2 (WAN) | Wireless 1 | Wireless 2 | Mobile

☑ Port Mode
☑ TCP/IP
☑ FTP
☑ Telnet
☑ SSH
□ Global Connections (CEA-852)
□ CEA-709 over IP (CEA-852)
☑ LIOB-IP
☑ Web UI
☑ HTTP
☑ HTTPS
☑ VNC for LCD UI
□ KNXnet/IP

Port Mode:	Separate network
Link Speed & Duplex:	Auto Detect
Enable 802.1X:	☑
EAP Type:	TLS
Identity:	testing
CA Certificate:	☑ Example Certificate Authority Delete
User Certificate:	user@example.org Delete
User Private Key:	RSA key (2048 bits)

Figure 7: Configure 802.1X port authentication

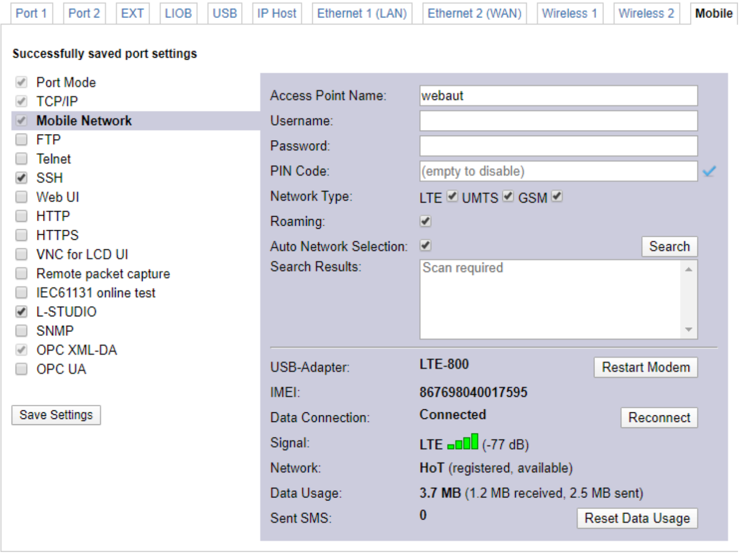
4.7 New in L-IP 7.2.0

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

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.



Successfully saved port settings

☑ Port Mode
☑ TCP/IP
☑ Mobile Network
□ FTP
□ Telnet
☑ SSH
□ Web UI
□ HTTP
□ HTTPS
□ VNC for LCD UI
□ Remote packet capture
□ IEC61131 online test
☑ L-STUDIO
□ SNMP
☑ OPC XML-DA
□ OPC UA

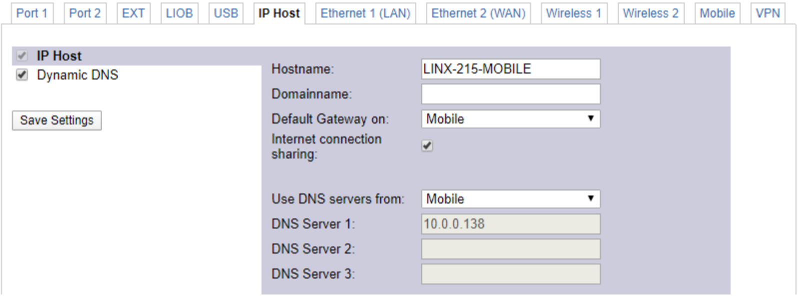
Access Point Name: webaut
Username:
Password:
PIN Code: (empty to disable) ✓
Network Type: LTE ☑ UMTS ☑ GSM ☑
Roaming: ☑
Auto Network Selection: ☑
Search Results: Scan required

USB-Adapter: LTE-800
IMEI: 867698040017595
Data Connection: Connected
Signal: LTE (-77 dB)
Network: HoT (registered, available)
Data Usage: 3.7 MB (1.2 MB received, 2.5 MB sent)
Sent SMS: 0

Figure 8: 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.



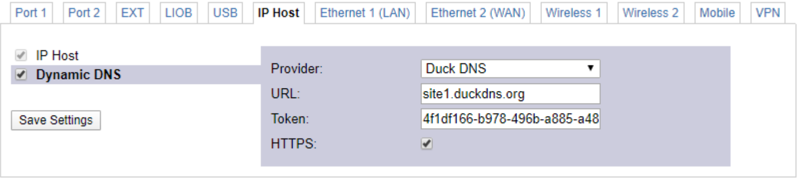
☑ IP Host
☑ Dynamic DNS

Hostname: LINX-215-MOBILE
Domainname:
Default Gateway on: Mobile
Internet connection sharing: ☑
Use DNS servers from: Mobile
DNS Server 1: 10.0.0.138
DNS Server 2:
DNS Server 3:

Figure 9: 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 public 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 10.



☑ IP Host
☑ Dynamic DNS

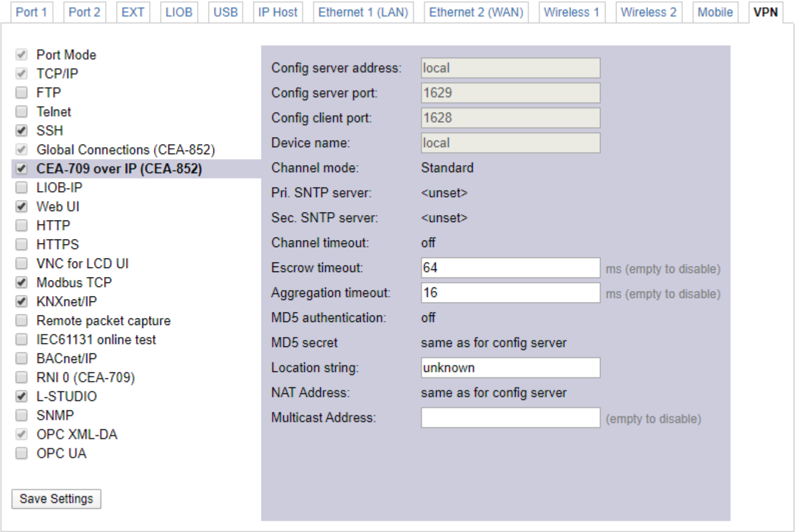
Provider: Duck DNS
URL: site1.duckdns.org
Token: 4f1df166-b978-496b-a885-a48
HTTPS: ☑

Figure 10: 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 CEA-852. 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 the CEA-852 configuration server on the VPN interface and add all other CEA-852 clients on 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.



☑ Port Mode
☑ TCP/IP
☐ FTP
☐ Telnet
☑ SSH
☑ Global Connections (CEA-852)
☑ **CEA-709 over IP (CEA-852)**
☐ LIOB-IP
☑ Web UI
☐ HTTP
☐ HTTPS
☐ VNC for LCD UI
☑ Modbus TCP
☑ KNXnet/IP
☐ Remote packet capture
☐ IEC61131 online test
☐ BACnet/IP
☐ RNI 0 (CEA-709)
☑ L-STUDIO
☐ SNMP
☑ OPC XML-DA
☐ OPC UA

Config server address:	local	
Config server port:	1629	
Config client port:	1628	
Device name:	local	
Channel mode:	Standard	
Pri. SNTP server:	<unset>	
Sec. SNTP server:	<unset>	
Channel timeout:	off	
Escrow timeout:	64	ms (empty to disable)
Aggregation timeout:	16	ms (empty to disable)
MD5 authentication:	off	
MD5 secret	same as for config server	
Location string:	unknown	
NAT Address:	same as for config server	
Multicast Address:		(empty to disable)

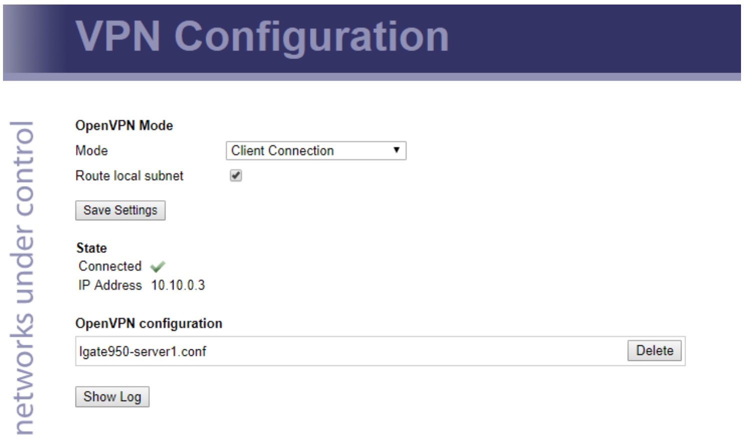
Figure 11: VPN tab on the port configuration interface.

4.8 New in L-IP 7.0.0

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

VPN

LOYTEC devices support joining a virtual private network (VPN). This feature is based on the widely-used and open-protocol OpenVPN technology. An OpenVPN configuration file (.ovpn) can be installed on the Web interface and makes the LOYTEC device a VPN client and dial into the OpenVPN server defined by that file. Any standard OpenVPN configuration file can be used, which is auto-login, i.e. does not require entering a password when connecting. After having registered, the LOYTEC device can be reached via its VPN address.



OpenVPN Mode

Mode: Client Connection

Route local subnet: ☑

State

Connected ✓

IP Address 10.10.0.3

OpenVPN configuration

lgate950-server1.conf

Figure 12: VPN client configuration on the Web interface

Setting up a VPN client on the LOYTEC device may solve NAT router issues, because no port forwarding rules need to be configured. The device dials out to the OpenVPN server running on a public IP and establishes the VPN channel. This VPN channel provides a secure connection for building automation protocols, such as BACnet/IP, Modbus TCP or CEA-852. Being part of a VPN the LOYTEC device is also reachable over multi-NAT access networks, such as LTE.

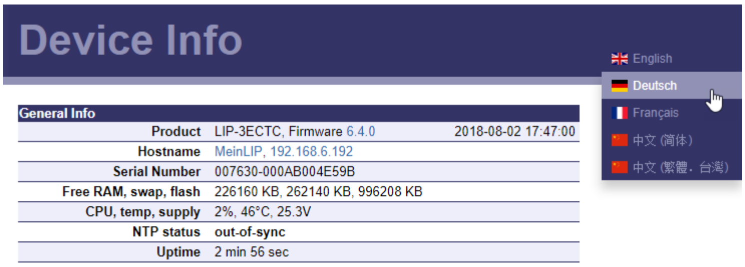
An alternative method is to enable simple server mode on the LOYTEC device. In this mode, the device provides an OpenVPN server and allows downloading a client configuration file from the Web interface. This file can be installed on any OpenVPN client and allows that client connect to the LOYTEC device over the secure VPN channel. Only one client may connect at a time.

4.9 New in L-IP 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.

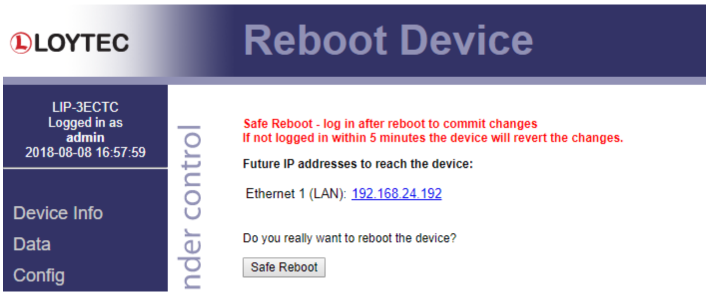


General Info		
Product	LIP-3ECTC, Firmware 6.4.0	2018-08-02 17:47:00
Hostname	MeinLIP, 192.168.6.192	
Serial Number	007630-000AB004E59B	
Free RAM, swap, flash	226160 KB, 262140 KB, 996208 KB	
CPU, temp, supply	2%, 46°C, 25.3V	
NTP status	out-of-sync	
Uptime	2 min 56 sec	

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.



Safe Reboot - log in after reboot to commit changes
If not logged in within 5 minutes the device will revert the changes.

Future IP addresses to reach the device:

Ethernet 1 (LAN): 192.168.24.192

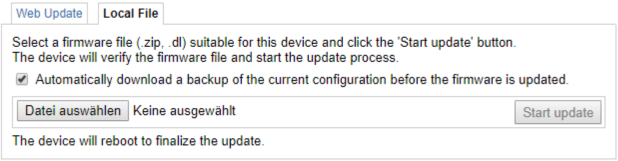
Do you really want to reboot the device?

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.



Select a firmware file (.zip, .dl) suitable for this device and click the 'Start update' button.
The device will verify the firmware file and start the update process.

☑ Automatically download a backup of the current configuration before the firmware is updated.

Keine ausgewählt

The device will reboot to finalize the update.

Figure 15: Backup before Upgrade on the Web interface.

LCD Interface

The user interface on the LCD display has been localized for the Chinese simplified and traditional language sets. The language can be selected from the main page and is switched immediately without a device reboot.

The user interface on the LCD display has been extended by a firmware upgrade menu. This menu allows installing a new firmware image from an attached USB memory stick. This is beneficial for WLAN-only devices. When plugging in a USB memory stick, a menu pops up (Figure 16) on the LCD interface that shows selected quick options, including firmware upgrade and backup.

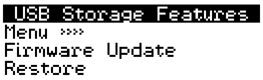


Figure 16: LCD pop-up menu for USB storage

4.10 New in L-IP 6.1.0

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

New L-IP Models

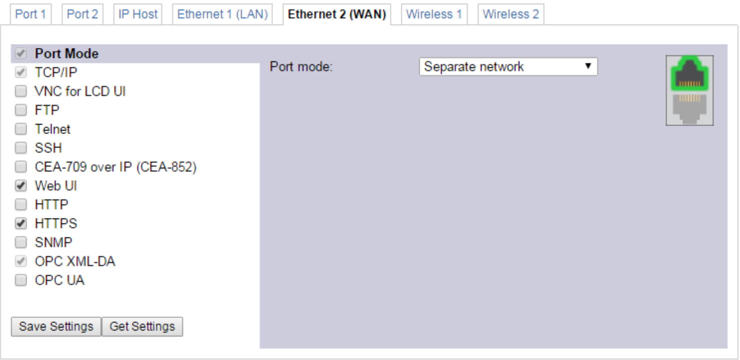
The new L-IP models with their product code ending in "C" are now supported. Equipped with dual Ethernet, a built-in firewall and LCD display, these new models serve as a plug-in replacement for the older series "B" devices. Existing device backups can be used without modification. In addition, the new models also support the wireless LAN technology.

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. Read Section 7.6.3 to learn more about project documentation on the device.

Dual-Ethernet with Separate Networks

Series "C" L-IP models with two Ethernet interfaces can 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 17 shows a WAN interface with HTTPS and OPC UA only, while CEA-709 over IP (CEA-852) are still bound to Ethernet 1 (LAN). For more information on how to use multiple Ethernet ports please refer to Section 7.3.4.



☑ Port Mode
☑ TCP/IP
☐ VNC for LCD UI
☐ FTP
☐ Telnet
☐ SSH
☐ CEA-709 over IP (CEA-852)
☑ Web UI
☐ HTTP
☑ HTTPS
☐ SNMP
☑ OPC XML-DA
☐ OPC UA

Port mode: Separate network

Figure 17: 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. Please refer to Section 7.3.8 to learn more about the WLAN interface.

SNMP

For accessing vital operational data in standard IT equipment, L-IP series “C” 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. For more information on configuring and using SNMP with a LOYTEC device please refer to Section 11.1.

OPC Server

The L-IP series “C” devices are equipped with an OPC server, which can speak the well-known OPC XML-DA and OPC UA protocols. The OPC server is used for perfect integration with the LWEB-900 building management software for device maintenance.

Wireshark Packet Capture

The L-IP series “C” models have the Wireshark packet capture feature. Using this feature local packet logs can be made and stored on the L-IP. It is also possible to connect a running Wireshark protocol analyzer on the PC to the L-IP and run a life packet capture. For more information on how to set up packet capture, please refer to Section 14.9.

5 Quick-Start Guide

This Chapter shows step-by-step instructions on how to configure the L-IP for a simple network architecture in a LAN environment.

5.1 Hardware Installation

5.1.1 L-IP

Connect power 12-35 VDC or 12-24 VAC, the CEA-709 network, and the Ethernet cable as shown in the installation sheet. More detailed instructions are shown in Chapter 6.

5.1.2 L-IP Redundant

Connect power 12-35 VDC or 12-24 VAC, the Ethernet cable and the CEA-709 network the installation sheet. Depending on the desired redundancy mode choose one of the cabling topologies as shown in Figure 18 to Figure 20. More detailed instructions are shown in Chapter 6.

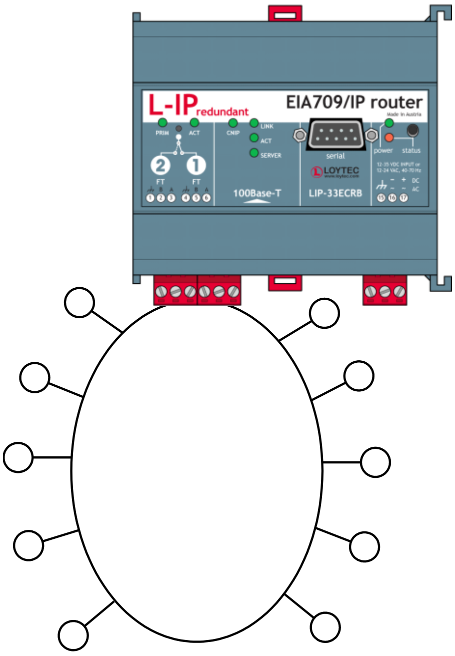


Figure 18: L-IP Redundant Standalone with Bus Loop Monitoring

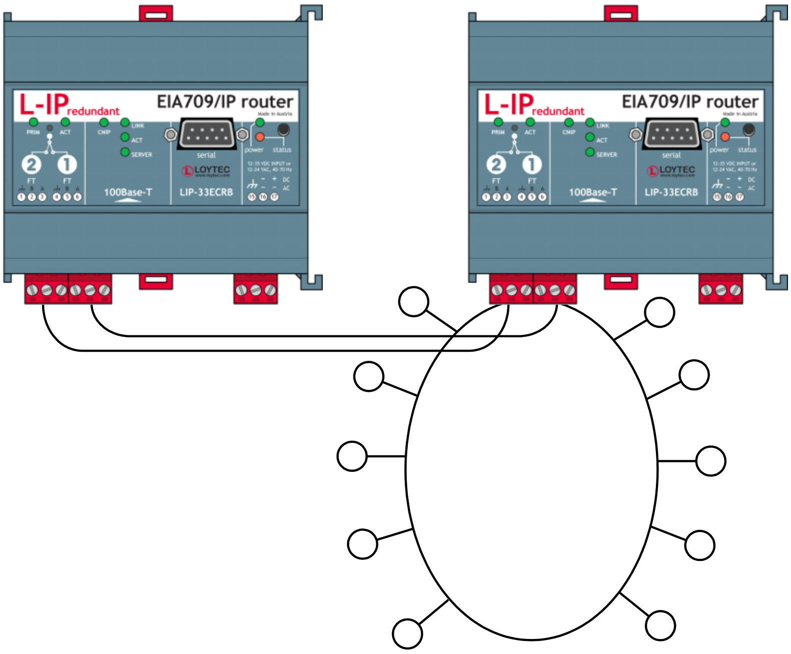


Figure 19: L-IP Redundant in Twin Router mode with Bus Loop Monitoring

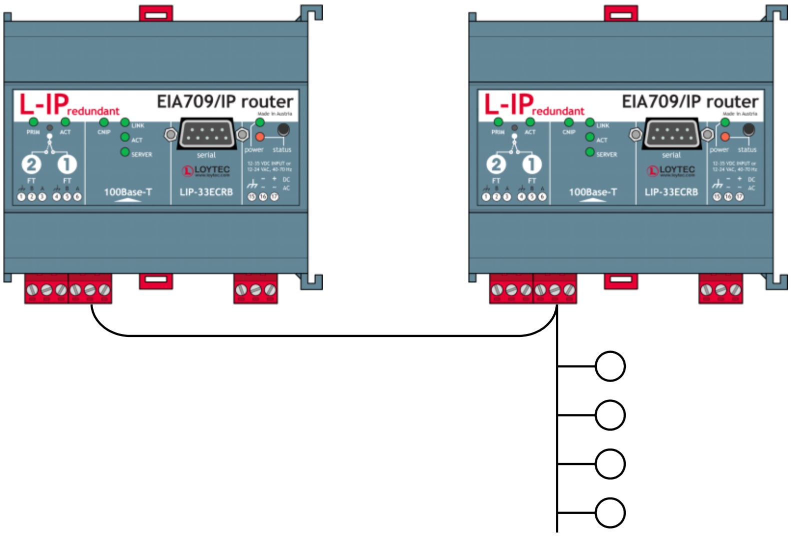


Figure 20: L-IP Redundant in Twin Router mode without Bus Loop Monitoring

5.2 IP Configuration of the Client Device

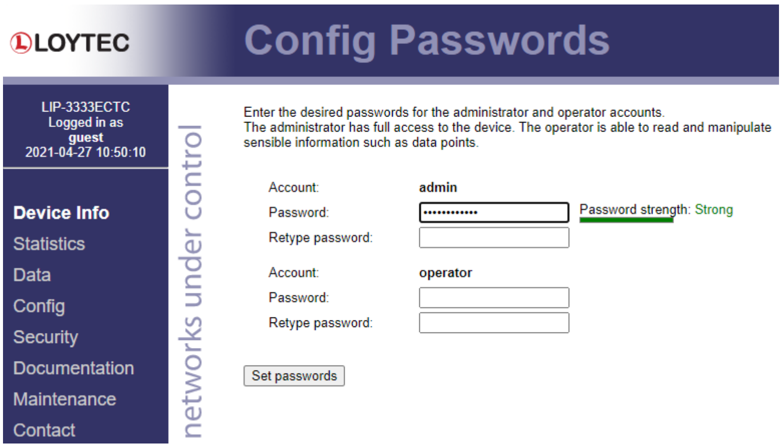
5.2.1 Configuration via the Web-Interface

LOYTEC devices are shipped with DHCP and will acquire an IP address as soon as they are connected to the network. To use a static IP, you can use the Web interface to configure the client device. In a Web browser enter the IP address of the device which can be read on the LCD display. Note that your PC must be attached to the same subnet as the device. For devices with a default IP address choose the setup on the LCD display.

To Configure a Static IP

1. 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 the passwords for the

administrator and operator accounts before proceeding. Only strong passwords are accepted.



Enter the desired passwords for the administrator and operator accounts.
The administrator has full access to the device. The operator is able to read and manipulate sensible information such as data points.

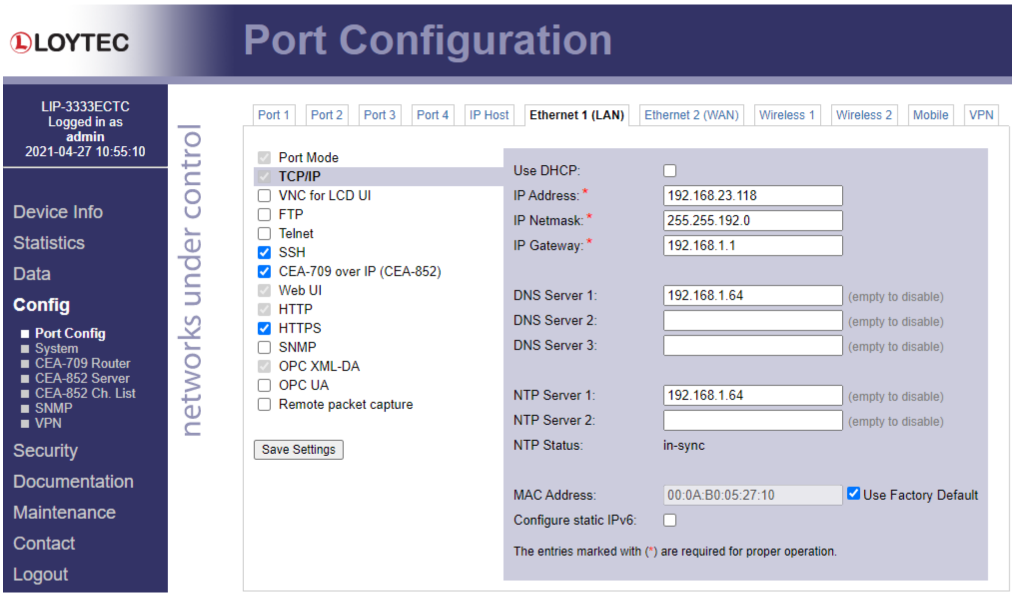
Account: admin
Password: •••••••••••• Password strength: Strong
Retype password:

Account: operator
Password:
Retype password:

Set passwords

Figure 21: Enter passwords for admin and operator accounts.

2. Then click on the **Config** menu. Click on **Port Config** and change to the tab **Ethernet**. The TCP/IP settings are selected as shown in Figure 22. Enter the IP address, the IP netmask, and IP gateway for this device.



☑ Port Mode
☑ TCP/IP
☐ VNC for LCD UI
☐ FTP
☐ Telnet
☑ SSH
☑ CEA-709 over IP (CEA-852)
☑ Web UI
☑ HTTP
☑ HTTPS
☐ SNMP
☑ OPC XML-DA
☐ OPC UA
☐ Remote packet capture

Save Settings

Use DHCP: ☐
IP Address:* 192.168.23.118
IP Netmask:* 255.255.192.0
IP Gateway:* 192.168.1.1

DNS Server 1: 192.168.1.64 (empty to disable)
DNS Server 2: (empty to disable)
DNS Server 3: (empty to disable)

NTP Server 1: 192.168.1.64 (empty to disable)
NTP Server 2: (empty to disable)
NTP Status: in-sync

MAC Address: 00:0A:B0:05:27:10 ☑ Use Factory Default
Configure static IPv6: ☐

The entries marked with (*) are required for proper operation.

Figure 22: Enter IP address and gateway.

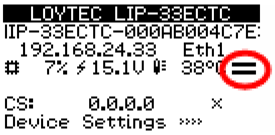
3. Press **Save Settings** and then reset the device by selecting **Reset** in the highlighted text. This changes the IP settings of the device.

5.2.2 Configuration via 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.

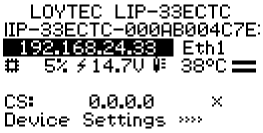
To Set the IP Address on the LCD Display

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



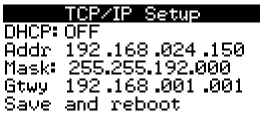
```
   LOYTEC LIP-33ECTC
LIP-33ECTC-000AB004C7E:
  192.168.24.33   Eth1
#  7% ⚡15.1V   38°C =

CS:      0.0.0.0     ×
Device Settings »»
```

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



```
   LOYTEC LIP-33ECTC
LIP-33ECTC-000AB004C7E:
  192.168.24.33   Eth1
#  5% ⚡14.7V   38°C =

CS:      0.0.0.0     ×
Device Settings »»
```

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



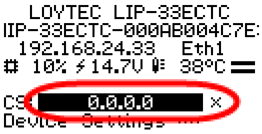
```
      TCP/IP Setup
DHCP: OFF
Addr  192.168.024.150
Mask: 255.255.192.000
Gtwy  192.168.001.001
Save and reboot
```

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

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

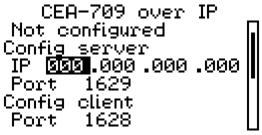
To Register with a Configuration Server

1. On the LCD main screen navigate to the address field next to CS and click on it.



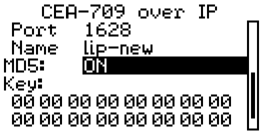
```
   LOYTEC LIP-33ECTC
LIP-33ECTC-000AB004C7E:
  192.168.24.33   Eth1
# 10% ⚡14.7V   38°C =

CS:      0.0.0.0     ×
Device Settings »»
```

2. This leads to the **CEA-709 over IP** menu. Navigate to the **Config Server IP** and enter the IP address into the four fields. Optionally adapt **Config Server Port**.



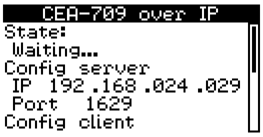
```
    CEA-709 over IP
 Not configured
Config server
 IP  000.000.000.000
 Port   1629
Config client
 Port   1628
```

3. If the channel requires MD5 authentication, set MD5 to ON and enter the secret key below.



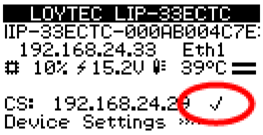
```
    CEA-709 over IP
 Port   1628
 Name   lip-new
MD5:    ON
Key:
 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00
```

4. Finally navigate to the bottom, click **Save** and acknowledge with **YES**. The device now tries to register with the configuration server. Observe the status information to see, if the registration completes.



```
 CEA-709 over IP
State:
 Waiting...
Config server
 IP 192.168.024.029
 Port  1629
Config client
```

5. Back in the home screen the configuration server is shown with a checkmark.

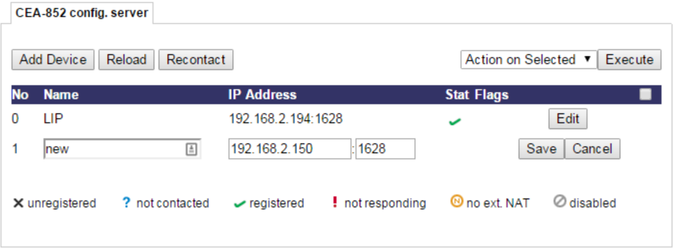


```
 LOYTEC LIP-33ECTC
lIP-33ECTC-000AB004C7E:
  192.168.24.33   Eth1
# 10% ⚡15.2V    39°C

CS:  192.168.24.29  ✓
Device Settings  >>>
```

5.3 Configuration Server Settings

If the L-IP should also act as the configuration server for the IP-852 channel, open the Web interface and go to the menu **CEA-852 Server**. In the drop-down box **Config server status** select **enabled** and click on **Save Settings** to activate the configuration server. Then the configuration server settings page shows all settings.

Then go to the menu **CEA-852 Ch. List** and click on the **Add Device** button to add a new client device. Enter name and IP address and click the **Save** button as shown in Figure 23. Client devices include all other L-IPs and all PCs, which should participate in the communication on the IP-852 channel.

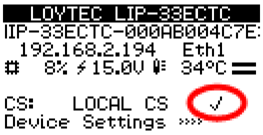


No	Name	IP Address	Stat	Flags
0	LIP	192.168.2.194:1628	✓	
1	new	192.168.2.150 : 1628		

✕ unregistered ? not contacted ✓ registered ! not responding ⊙ no ext. NAT ⊘ disabled

Figure 23: Add new client devices to the channel.

Verify in the channel list that the device(s) have been registered successfully and show a green checkmark. The CNIP-LED on all L-IP devices that have one should be green and the SERVER-LED on the configuration server L-IP should be green as well. L-IP devices with an LCD display will show the configuration server address (or LOCAL) and a checkmark if registered correctly at the configuration server as shown in Figure 24.



```
 LOYTEC LIP-33ECTC
lIP-33ECTC-000AB004C7E:
  192.168.2.194   Eth1
#  8% ⚡15.0V    34°C

CS:    LOCAL CS   ✓
Device Settings  >>>
```

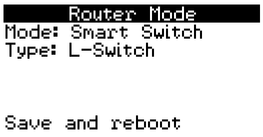
Figure 24: L-IP LCD display for a registered CNIP client.

Add the L-IP router to your network drawing and commission the L-IP. Note that we provide shapes for LonMaker. You should now be able to communicate via an IP-852 channel. For detailed instructions on how to configure the configuration server please refer to Section 7.3.14.

5.4 Configure as LON Router Drop-In Replacement

A multi-port L-IP (e.g., LIP-13ECTC or LIP-33ECTC) can be configured as drop-in replacement for third-party LON routers that route between TP-1250/FT-10 or FT-10/FT-10, respectively. For doing so, go to the LCD menu **Device Settings** »» and navigate to **CEA-709** »» **Router Mode** »».

Select the **Mode** “Smart Switch” and the device **Type** “L-Switch” and then choose **Save and reboot** (see Figure 25). In this setting the device acts as a self-learning router between the two CEA-709 ports, while IP-852 is disabled. Using Smart Switch™ router mode, no re-commissioning is required in the LNS database. If it is required that the router is visible in LNS, choose “Conf. Router” mode instead.



```
      Router Mode
Mode: Smart Switch
Type: L-Switch


Save and reboot
```

Figure 25: Router Mode menu on the LCD display.

The IP settings are not required in this operation mode. For firmware upgrade and other device maintenance on the Web interface, however, it is recommended to setup the IP address as well.

5.5 L-IP Redundant Configuration

The L-IP Redundant can only be used as Configured Router and thus requires to be commissioned with a network management tool (e.g. LonMaker). Smart Switch Mode, Repeater Mode and Bridge Mode are not supported.

The L-IP Redundant comes preconfigured to support bus loop monitoring (see Figure 18). For operating the device in twin router mode (device redundancy, see Figure 19) some additional steps have to be performed:

- Add one router shape for each L-IP Redundant. Connect both to the same IP-Channel on one side and to the same FT-10 Channel on the other side of the router.

- Add one L-IP Redundant built-in monitoring node “L-IP Redundant Diagnostic FT-10” device shape for each L-IP Redundant on the FT-10 channel. The corresponding device template will be installed with the L-IP Redundant Plug-In available from the LOYTEC webpage http://www.loytec.com.

- Add a “Twin Router” functional block for each L-IP Redundant monitoring node.

- Connect *nvoRedRtr* of one L-IP Redundant with the *nviRedRtr* of its paired L-IP Redundant and vice versa.

If using LonMaker for Windows the resulting drawing should look like shown in Figure 26. Furthermore, the PRIM LED on one of the two L-IP Redundant devices should be green and should be off on the other one.

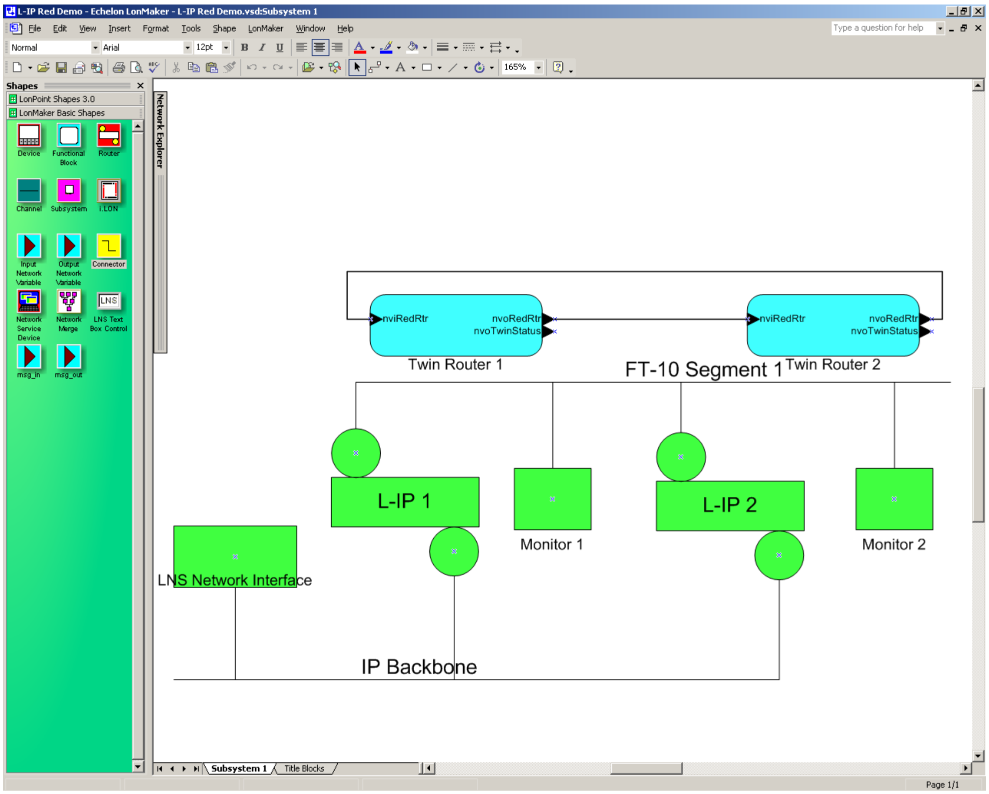


Figure 26: A pair of L IP Redundant devices configured for twin router operation

For detailed instructions on how to configure the L-IP Redundant refer to Section 10.

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 L-IP contains the following information:

- L-IP order number with bar-code (e.g. LIP-3ECTC, LIP-33ECTC, or LIP-33ECRB),
- serial number with bar-code (Ser#),
- unique node ID and virtual ID of each port (NIDx and VIDx) with bar-code,
- Ethernet MAC ID with bar-code (MAC1).

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

A virtual ID (VID) is a Node ID on the IP channel. Internally the 2-Port (LIP-xxECTB, LIP-xxECTC) and the 4-Port (LIP-xxxxECTB, LIP-xxxxECTC) version of the L-IP use up to 5 individual routers which are connected over a TP/XP-1250 backbone (see Figure 27 and Figure 29). On the attached label, only the external NIDs (number 1-3 or 1-5) are printed. Since the NIDs are organized in a continuous number block, the internal NIDs can be derived by incrementing the numbers printed on the label (number 4-6 or 6-10, see Figure 28 and Figure 30).

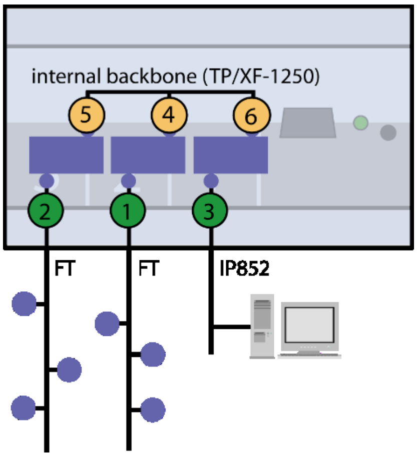


Figure 27: Internal assignment of NIDs on LIP-xxECTB.

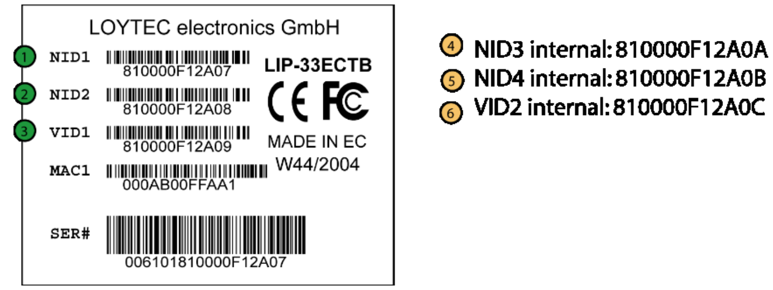


Figure 28: Example of internal NID order on LIP-xxECTB.

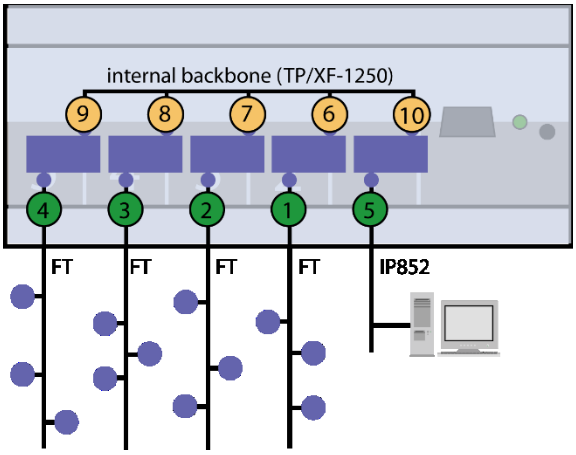


Figure 29: Internal assignment of NIDs on LIP-xxxxECTB.

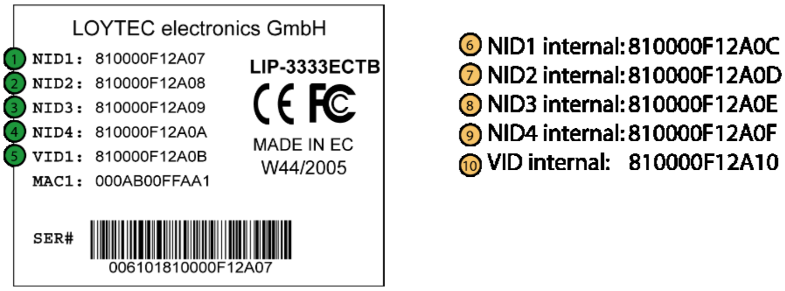


Figure 30: Example of internal NID order on LIP-xxxxECTB.

6.3 Mounting

The device comes prepared for mounting on DIN rails following DIN EN 50 022. The device can be mounted in any position. However, an installation place with proper airflow must be selected to ensure that the L-IP temperature does not exceed the specified range.

6.4 LED signals

Available LEDs and their location on the respective device model can be found on the product's installation sheet. The installation sheet can be found in the product's box.

6.4.1 Power LED

The power LED lights up green when power is supplied to the power terminals.

6.4.2 Status LED

The L-IP is equipped with a red status LED (see installation sheet). This LED is normally off. If the fall-back image is executed the status LED flashes red once every second.

6.4.3 CEA-709 Activity LED

The CEA-709 port on the L-IP has a three color LED (green, red and orange, see installation sheet). Table 2 shows different LED patterns of the port and their meaning.

Behavior	Description	Comment
GREEN flashing fast	Traffic	
GREEN flashing at 1Hz	Port unconfigured	Only if L-IP operated as configured CEA-709 router (see Section 8.1.1)
RED permanent	Port damaged	
RED flashing fast	Traffic with high amount of errors L-IP redundant: Loop open (see Section 6.4.10)	
RED flashing at 1 Hz (all ports)	Firmware image corrupt Please upload new firmware	
ORANGE permanent	Port disabled	e.g. using LSD Tool (see Chapter 15)
ORANGE flashing fast	Traffic on port configured as management port	e.g. using LSD Tool (see Chapter 15)
ORANGE flashing at 1 Hz	Bit-rate auto-detection	RS-485 ports only
ORANGE permanent (all ports)	Status button pressed for more than 20 seconds L-IP forwarding tables will be reset once button is released	

Table 2: CEA-709 Activity LED patterns.

6.4.4 Twin Router Status LED (L-IP Redundant only)

The L-IP Redundant has a three color LED (green, red and orange, see installation sheet) showing the twin router status of the device. This LED is labeled “PRIM”. Table 3 shows different LED patterns and their meaning.

Behavior	Description	Comment
GREEN	Device is active	Standalone mode or primary device in twin router mode
OFF	Device is inactive	Secondary in twin router mode
ORANGE	Device is active, but problem with twin router detected	Primary: Secondary not reachable Secondary: Primary failed, secondary has taken over and is active
RED	Device is inactive due to error detected	Device is primary, but secondary has taken over

Table 3: Twin Router Status LED patterns.

Every time the L-IP Redundant contacts its twin router the LED is switched off shortly to signal this activity.

6.4.5 Ethernet Link LED

The Ethernet Link LED lights up green whenever an Ethernet cable is plugged-in and a physical connection with a switch, hub, or PC can be established.

6.4.6 Ethernet Activity LED

The Ethernet Activity LED lights up green for 6ms whenever a packet is transmitted or received or when a collision is detected on the network cable.

6.4.7 CEA-852 Status LED (CNIP LED)

The CNIP LED is a three color LED that indicates different operating states of the L-IP device.

Green: The CEA-852 device is fully functional and all CEA-852 configuration data (channel routing info, channel membership list, send list) are up-to-date.

Green flicker: If a valid CEA-709 packet is received or transmitted over the IP channel the CNIP LED turns off for 50 ms. Only valid CEA-709 IP packets sent to the IP address of the L-IP can be seen. Stale packets or packets not addressed to the device are not seen.

Yellow: Device is functional but some configuration data is not up-to-date (device cannot contact configuration server but has configuration data saved in Flash memory)

Red: Device is non-functional because it was rejected from the CEA-852 IP channel or shut-down itself due to an internal error condition.

Off: Device is non-functional because the CEA-852 device has not started. This can be the case if the device uses DHCP and it has not received a valid IP configuration (address) from the DHCP server.

Flashing red at 1 Hz: Device is non-functional because the CEA-852 device is started but has not been configured. Please add the device to a CEA-852 IP channel (register in configuration server).

Flashing green or orange at 1 Hz: The device's CEA-709 side of the gateway has not been commissioned yet. The color indicates the CEA-852 IP channel status as described above.

6.4.8 Configuration Server LED

The Configuration Server LED illuminates green whenever the configuration server is activated on the L-IP device.

6.4.9 Wink Action

If the L-IP receives a wink command on any of its network ports, it shows a blink pattern on the CNIP and the CEA-709 activity LEDs. The CEA-709 activity and the CNIP LED turn green/orange/red (each 0.15 s). This pattern is repeated six times. After that the CNIP LED flashes orange six times if the wink command was received on the IP channel or the CEA-709 activity LED flashes orange six times if the wink command was received on the CEA-709 channel. After that the L-IP LEDs return to their normal behavior.

6.4.10 Network Diagnostics

The L-IP provides simple network diagnostics via its CEA-709 activity LED:

- If the LED does not light up at all this port is not connected to any network segment or the connected network segment currently shows no traffic.

- If the LED is flashing green the network segment connected to this port is ok.

- If the LED is flashing red a potential problem exists on the network segment connected to this port. This state is referred to as overload condition.

A port overload condition occurs if

- the average bandwidth utilization of this port was higher than 70% or
- the collision rate was higher than 5% or
- more than 15% CRC errors have occurred on a port with a power-line transceiver or more than 5% on a port with a transceiver other than power-line or
- the L-IP was not able to process all available messages.
- the L-IP Redundant has detected an open loop (L-IP Redundant only, see Section 10).

For a deeper analysis of the reason of the overload condition it is recommended to use a protocol analyzer (e.g. LOYTEC's LPA) or a similar tool. The exact reason of the overload condition can also be determined with the LSD Tool (see Chapter 15).

6.5 Status Button

The L-IP is equipped with a status button (see installation sheet). When pressing the status button shortly during normal operation of the L-IP it sends a "Service Pin Message" on all network ports. Note that every L-IP port has its own unique node ID ("Neuron ID"). As alternative to pressing the status button a service pin message can be sent via the web interface (see Section 7.1).

Pressing the status button longer than 2 seconds will allow you to select the port to sends out the "Service Pin Message" message: The port LED of the currently selected port will light up orange. After 2 seconds the next available port will be selected. When the status button is released the "Service Pin Message" is sent out on the currently selected port.

Pressing the status button during normal operation for more than 20 seconds resets the switching tables (see Section 6.5.1).

6.5.1 Resetting Forwarding Tables

In order to reset the forwarding tables, the status button needs to be pressed for at least 20 seconds during normal operation of the L-IP. Resetting forwarding tables defaults means:

- Clearing the group forwarding, the subnet/node forwarding and the router domain table when used in smart switch mode.
- Setting all ports to unconfigured.
- Clearing the L-IP status and statistic data.
- But **does not** clear the IP address and CEA-852 configuration settings.

All this is done when the button is released. Afterwards a reset is performed to let the changes take effect. Once the button is held down for more than 20 seconds the CEA-709 activity and the CNIP LED are switched to orange and stay orange until the button is released and the L-IP is reset. This indicates that the forwarding tables will be reset.

Alternatively to holding down the status button the forwarding tables can be reset in the **Device Management** menu on the LCD display (see Section 6.6.1).

Important: ***If the L-IP is operated in smart switch mode and is moved from one location to another or if major changes to the configuration of the network are made, it is recommended to reset the L-IP forwarding tables.***

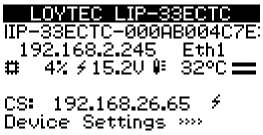
Important: ***Wait at least 30 seconds after power-up of the L-IP before pressing the Status Button to ensure that the L-IP has booted properly!***

6.6 LCD Display and Jog Dial

6.6.1 Device Setup

The L-IP series “C” 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 31. 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.

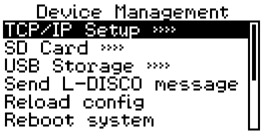
Below are menu items. Turn the jog dial to navigate between menu items and press to enter a menu or go into selection mode. When in selection mode turn the jog dial to alter the value and press again to quit the selection.



```
  LOYTEC LIP-33ECTC
IIP-33ECTC-000AB004C7E:
 192.168.2.245  Eth1
#  4% ⚡15.2V    32°C

CS: 192.168.26.65  ⚡
Device Settings »»
```

Figure 31: 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 32.



```
   Device Management
TCP/IP Setup »»
SD Card »»
USB Storage »»
Send L-DISCO message
Reload config
Reboot system
```

Figure 32: 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.

- **CEA-709 over IP**: This menu allows editing the CNIP client settings that are needed to register with a configuration server. See Section 6.6.3 for details.

- **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-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.

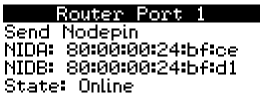
- **Contrast**: This menu allows adjusting the display's contrast.

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

- **Reset switch tables**: Choose this item to reset the forwarding tables in the switch.

6.6.2 Sending a Node Pin Message

The **Device Settings »»** menu also allows configuring basic CEA-709 router settings. Navigate to the **CEA-709 »»** sub-menu and choose one of the router menus, which is displayed in Figure 32.



```
     Router Port 1
Send Nodepin
NIDA: 80:00:00:24:bf:ce
NIDB: 80:00:00:24:bf:d1
State: Online
```

Figure 33: CEA-709 router menu on the LCD UI.

This menu gives you the following options for the CEA-709 router port:

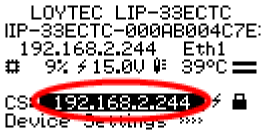
- **Send Nodepin**: This menu allows sending a node pin message to the CEA-709 network.

- **NIDA, NIDB**: These items show the Node IDs of the two ports on the selected router.

- **State**: This item shows, if the selected router is online or offline.

6.6.3 CEA-852 Device Settings

To change the CEA-852 client settings and register with a configuration server navigate to the IP address item on the main menu next to **CS:** and press the button as shown in Figure 34.



```
   LOYTEC LIP-33ECTC
IIP-33ECTC-000AB004C7E:
 192.168.2.244   Eth1
#   9% ⚡15.0V    39°C =

CS: 192.168.2.244 ⚡ 🔒
Device Settings »»
```

Figure 34: Setting the CS address on the LCD UI.

This opens the **CEA-709 over IP** menu with the following settings:

- **Config Server IP**: Enter the IP address of the configuration server into the four separate input fields.

- **Config Server Port**: Enter the configuration server port. The default 1629 can be left unchanged in most cases.

- **Config Client Port**: Enter the configuration client port. The default 1628 can be left unchanged in most cases.

- **MD5**: The default is off. Turn this on, if MD5 authentication shall be used on the channel for security purposes.

- **Key**: If MD5 is turned on enter the MD5 secret key into the 16 input fields.

The title page also shows the CEA-852 client state as a symbol next to the CS address. It can be normal (✓), waiting for the configuration server (⚡), or not registered (×). If MD5 is enabled on this device a lock icon 🔒 is shown.

6.6.4 Router Mode Settings

The **Router Mode** menu is a sub-menu of the CEA-709 device settings. It allows configuring the basic router modes:

- **Mode**: This setting configures the router operating mode as described in Section 8.1:

    - Config. Router: This is the default mode for a configured CEA-709 router that needs commissioning in the LNS database.

    - Smart Switch: In Smart Switch™ mode the device acts as a plug-and-play self-learning router that doesn't need LNS setup.

    - Repeater: In this mode the device is a store-and-forward repeater.

    - Switch (SN learn): This mode is similar to the Smart Switch™ mode, but only subnet learning is on and subnet broadcasts are not flooded (see details in Section 8.1).

- **Type**: This settings defines the basic device type. 'L-IP' is the default type and the device acts as a router or smart-switch between the CEA-709 ports (TP-1250 or FT-10) and the IP-852 channel. As an 'L-Switch' type, the device acts as a router between its CEA-709 ports only and has IP-852 disabled.

If configured as an L-Switch type device in Smart Switch™ mode, the L-IP can be used as a plug-and-play drop-in replacement for common third-party LON routers.

6.7 Wiring

6.7.1 L-IP

Every network segment connected to the L-IP needs to be terminated according to the rules found in the specification of the transceiver (see Chapter 12).

Important: ***All used and unused ports must be properly terminated. LOYTEC recommends the use of the LOYTEC L-Term series network terminators (LT-13 or LT-33 respectively). For unused ports, it is recommended to use a 100 Ohm 0.25 W resistor between terminals A and B as termination.***

Important: ***When using shielded network cables, only one side of the cable should be connected to earth ground. Thus, the shield must be connected to earth ground either at the L-IP terminals or somewhere else in the network (see Figure 35)!***

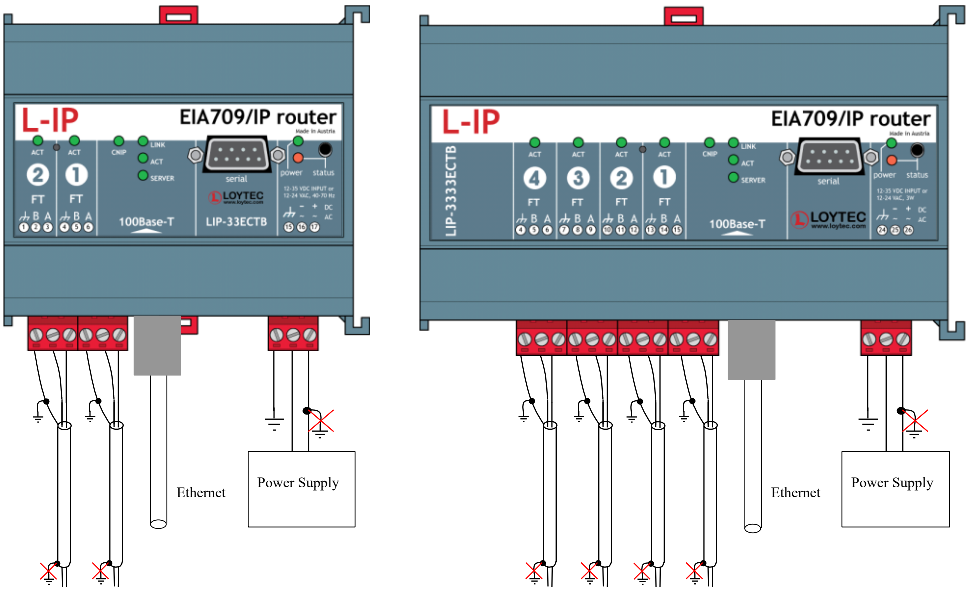


Figure 35: Connecting the Earth Ground to the L-IP series "B".

6.7.2 L-IP Redundant

Every network segment connected to the L-IP needs to be terminated according to the rules found in the specification of the transceiver (see Chapter 12).

Important: ***All used and unused ports must be properly terminated. LOYTEC recommends the use of the LOYTEC L-Term series network terminators (LT-13 or LT-33 respectively). For unused ports, it is recommended to use a 100 Ohm 0.25 W resistor between terminals A and B as termination.***

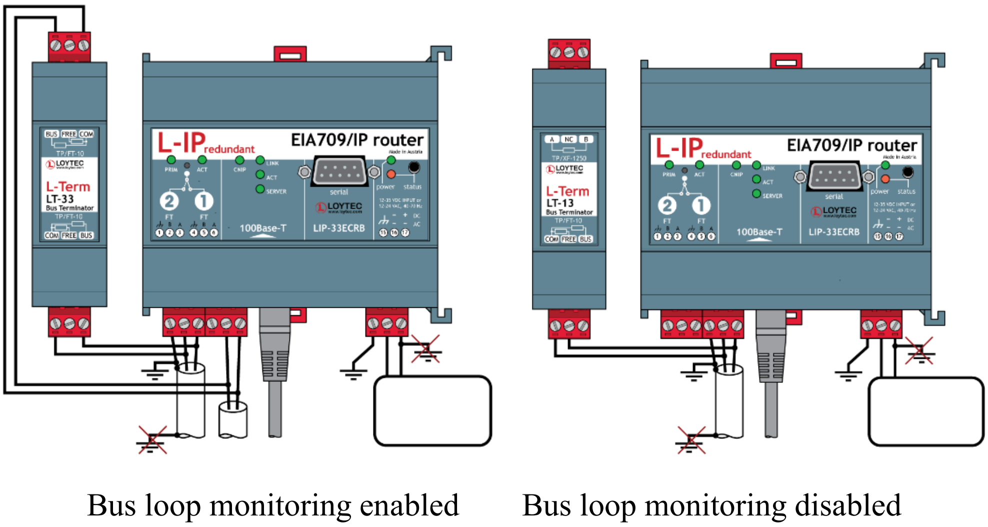


Figure 36: L-IP Redundant with and without Bus loop Monitoring

Important: ***When using shielded network cables, only one side of the cable should be connected to earth ground. Thus, the shield must be connected to earth ground either at the L-IP terminal (loop port 1) or somewhere else in the network, but never at more than one place (see Figure 36)!***

Important: ***If operated with bus loop monitoring enabled (loop port 1 and loop port 2 connected), both sides of the loop must be terminated at the L-IP terminals (see Figure 36). In this case two terminators for bus topology must be used.***

Important: ***If operated with bus loop monitoring enabled, the loop must not contain any repeaters!***

7 Web Interface

The L-IP comes 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 and other configuration settings.

7.1 Device Information and Account Management

7.1.1 Device Setup

In a Web browser, enter the default IP address 192.168.1.254 of the device. Note that if your PC has an IP address in a subnet other than 192.168.1.xxx, you must open a command tool and enter the following route command to add a route to the device.

To Add a Route to the Device

1. Windows **START → Run**

2. Enter ‘cmd’ and click **OK**.

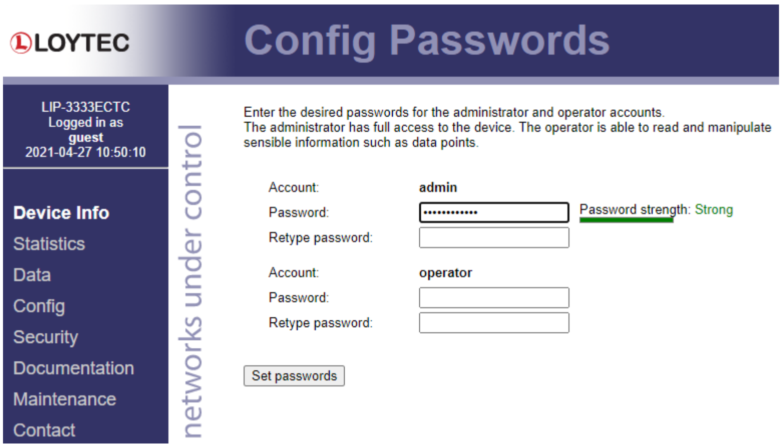
3. In the command window enter the command line

   ```
   route add 192.168.1.254 %COMPUTERNAME%
   ```

   In Windows7 replace %COMPUTERNAME% with the PC's actual IP address.

4. Then open your Web browser and type in the default IP address ‘192.168.1.254’.

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 37 and then click on **Set passwords**.



Enter the desired passwords for the administrator and operator accounts.
The administrator has full access to the device. The operator is able to read and manipulate sensible information such as data points.

Account: admin
Password: •••••••••••• Password strength: Strong
Retype password:

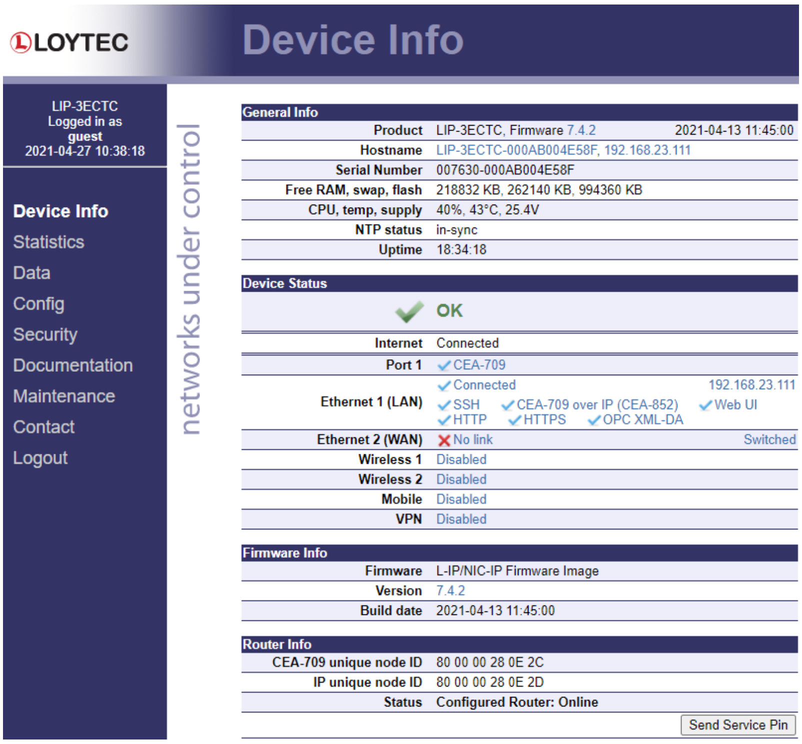
Account: operator
Password:
Retype password:

Figure 37: 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 7.4.1.

7.1.2 Device Information

The device information page (Figure 38) 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.



General Info		
Product	LIP-3ECTC, Firmware 7.4.2	2021-04-13 11:45:00
Hostname	LIP-3ECTC-000AB004E58F, 192.168.23.111	
Serial Number	007630-000AB004E58F	
Free RAM, swap, flash	218832 KB, 262140 KB, 994360 KB	
CPU, temp, supply	40%, 43°C, 25.4V	
NTP status	in-sync	
Uptime	18:34:18	

Device Status		
	✓ OK	
Internet	Connected	
Port 1	✓CEA-709	
Ethernet 1 (LAN)	✓Connected ✓SSH ✓CEA-709 over IP (CEA-852) ✓Web UI ✓HTTP ✓HTTPS ✓OPC XML-DA	192.168.23.111
Ethernet 2 (WAN)	✗No link	Switched
Wireless 1	Disabled	
Wireless 2	Disabled	
Mobile	Disabled	
VPN	Disabled	

Firmware Info	
Firmware	L-IP/NIC-IP Firmware Image
Version	7.4.2
Build date	2021-04-13 11:45:00

Router Info	
CEA-709 unique node ID	80 00 00 28 0E 2C
IP unique node ID	80 00 00 28 0E 2D
Status	Configured Router: Online

Figure 38: 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. Shown below are further a summary on the active protocols on the respective ports. All items are links that lead directly to their configuration page.

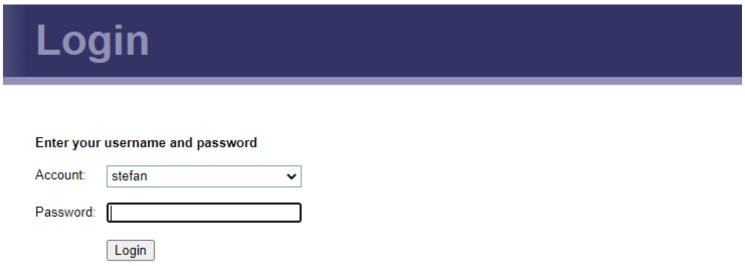
Below the general status information more specific sections are displayed depending on the model. The **Firmware Info** provides version and build times of the primary and fallback firmware images installed on the device.

The page also includes the unique node IDs ("Neuron IDs") of the CEA-709 network interfaces. The multi-port L-IP displays the external node IDs as well as the node IDs for the internal backbone in separate. 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.

7.1.3 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 39. 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.



Enter your username and password

Account: stefan

Password:

Figure 39: Enter the user name and password.

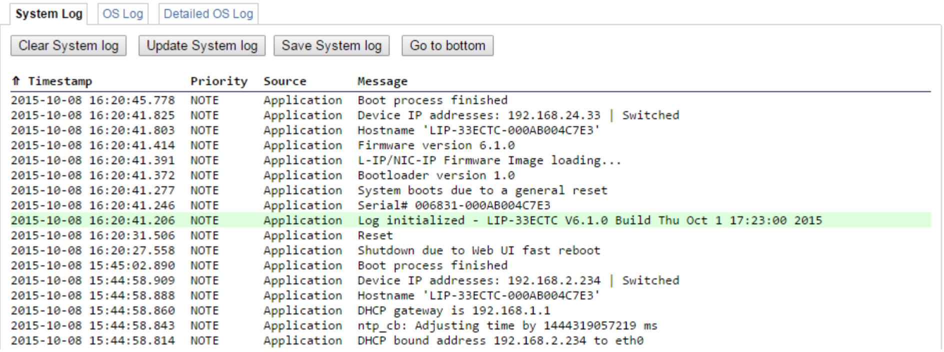
7.2 Device Statistics

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

7.2.1 System Log

The **System Log** page prints all messages stored in the system log of the device. An example is shown in Figure 40. 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.

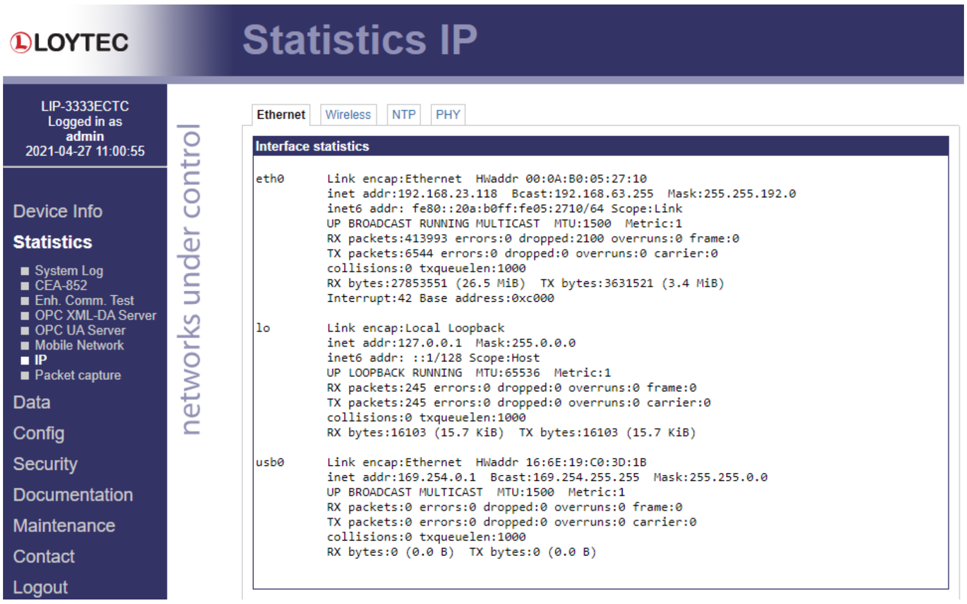


```
⇑ Timestamp               Priority  Source       Message
2015-10-08 16:20:45.778   NOTE      Application  Boot process finished
2015-10-08 16:20:41.825   NOTE      Application  Device IP addresses: 192.168.24.33 | Switched
2015-10-08 16:20:41.803   NOTE      Application  Hostname 'LIP-33ECTC-000AB004C7E3'
2015-10-08 16:20:41.414   NOTE      Application  Firmware version 6.1.0
2015-10-08 16:20:41.391   NOTE      Application  L-IP/NIC-IP Firmware Image loading...
2015-10-08 16:20:41.372   NOTE      Application  Bootloader version 1.0
2015-10-08 16:20:41.277   NOTE      Application  System boots due to a general reset
2015-10-08 16:20:41.246   NOTE      Application  Serial# 006831-000AB004C7E3
2015-10-08 16:20:41.206   NOTE      Application  Log initialized - LIP-33ECTC V6.1.0 Build Thu Oct 1 17:23:00 2015
2015-10-08 16:20:31.506   NOTE      Application  Reset
2015-10-08 16:20:27.558   NOTE      Application  Shutdown due to Web UI fast reboot
2015-10-08 15:45:02.890   NOTE      Application  Boot process finished
2015-10-08 15:44:58.909   NOTE      Application  Device IP addresses: 192.168.2.234 | Switched
2015-10-08 15:44:58.888   NOTE      Application  Hostname 'LIP-33ECTC-000AB004C7E3'
2015-10-08 15:44:58.860   NOTE      Application  DHCP gateway is 192.168.1.1
2015-10-08 15:44:58.843   NOTE      Application  ntp_cb: Adjusting time by 1444319057219 ms
2015-10-08 15:44:58.814   NOTE      Application  DHCP bound address 192.168.2.234 to eth0
```

Figure 40: System Log Page.

7.2.2 IP Statistics

Figure 41 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.



Interface statistics

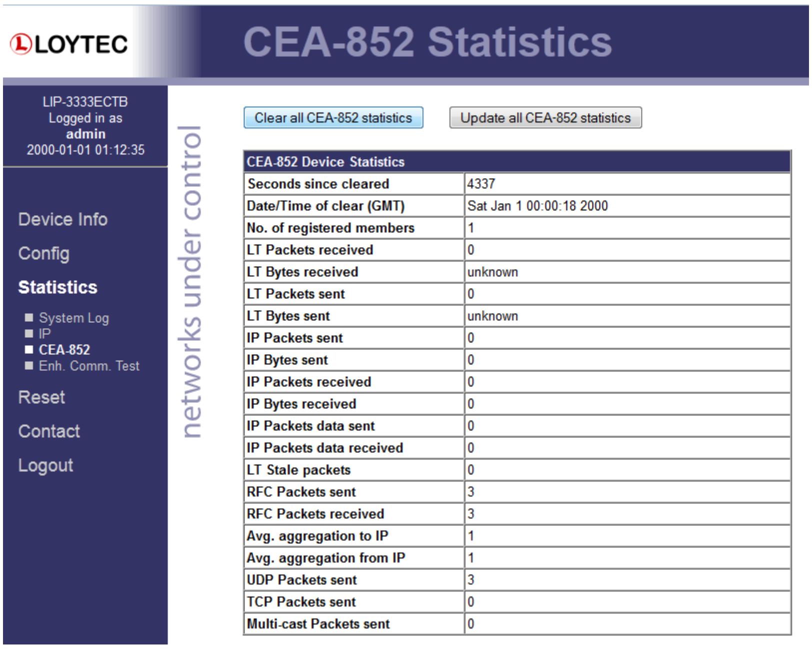
```
eth0      Link encap:Ethernet  HWaddr 00:0A:B0:05:27:10
          inet addr:192.168.23.118  Bcast:192.168.63.255  Mask:255.255.192.0
          inet6 addr: fe80::20a:b0ff:fe05:2710/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:413993 errors:0 dropped:2100 overruns:0 frame:0
          TX packets:6544 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:27853551 (26.5 MiB)  TX bytes:3631521 (3.4 MiB)
          Interrupt:42 Base address:0xc000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:245 errors:0 dropped:0 overruns:0 frame:0
          TX packets:245 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16103 (15.7 KiB)  TX bytes:16103 (15.7 KiB)

usb0      Link encap:Ethernet  HWaddr 16:6E:19:C0:3D:1B
          inet addr:169.254.0.1  Bcast:169.254.255.255  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Figure 41: 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.

7.2.3 CEA-852 Statistics

The CEA-852 statistics page displays the statistics data of the CEA-852 device on the device. The upper part of the CEA-852 statistics page is depicted in Figure 42. 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.

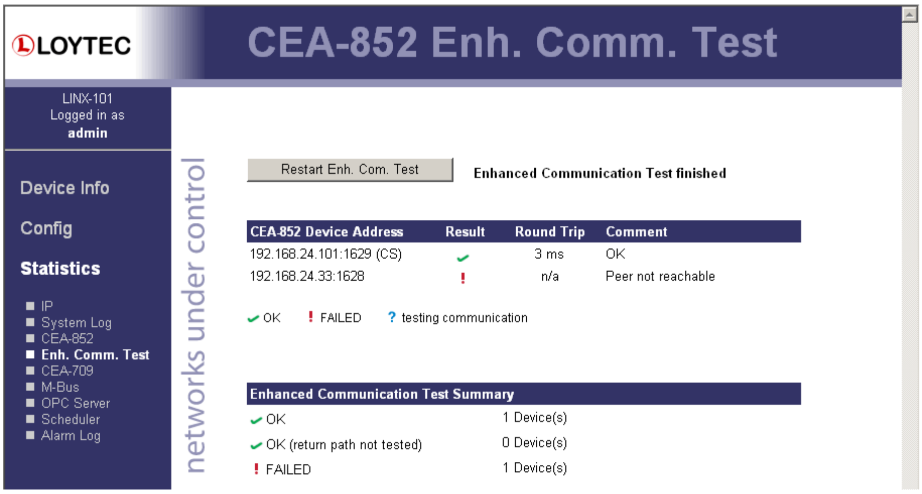


CEA-852 Device Statistics	
Seconds since cleared	4337
Date/Time of clear (GMT)	Sat Jan 1 00:00:18 2000
No. of registered members	1
LT Packets received	0
LT Bytes received	unknown
LT Packets sent	0
LT Bytes sent	unknown
IP Packets sent	0
IP Bytes sent	0
IP Packets received	0
IP Bytes received	0
IP Packets data sent	0
IP Packets data received	0
LT Stale packets	0
RFC Packets sent	3
RFC Packets received	3
Avg. aggregation to IP	1
Avg. aggregation from IP	1
UDP Packets sent	3
TCP Packets sent	0
Multi-cast Packets sent	0

Figure 42: Part of the CEA-852 Statistics Page.

7.2.4 Enhanced Communications Test

The Enhanced Communications Test allows testing the CEA-852 communication path between the CEA-852 device on the L-IP 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 43.



Enhanced Communication Test finished

CEA-852 Device Address	Result	Round Trip	Comment
192.168.24.101:1629 (CS)	✓	3 ms	OK
192.168.24.33:1628	!	n/a	Peer not reachable

✓ OK ! FAILED ? testing communication

Enhanced Communication Test Summary	
✓ OK	1 Device(s)
✓ OK (return path not tested)	0 Device(s)
! FAILED	1 Device(s)

Figure 43: 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 4.

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.

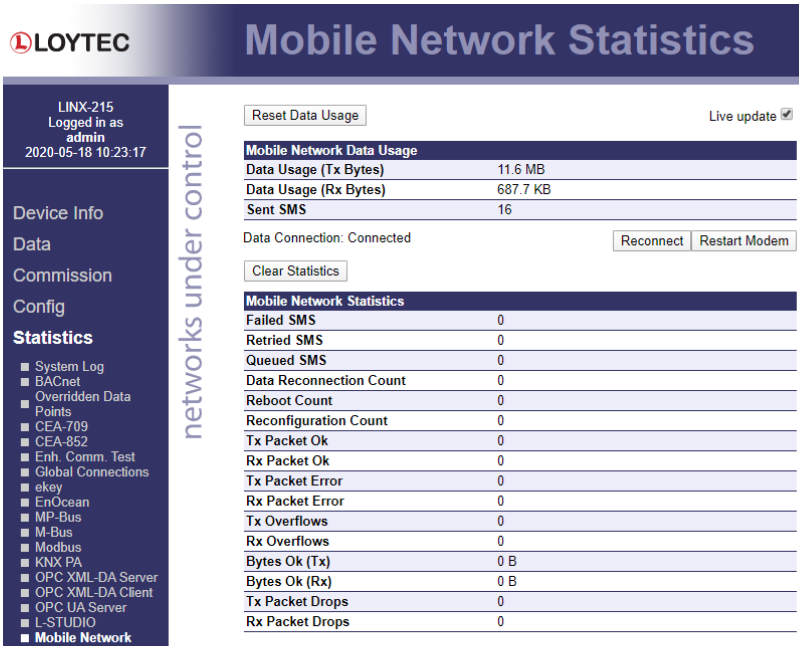
Table 4: Possible Communication Problems.

7.2.5 Packet Capture

The packet capture feature allows configuring and running a local packet capture for the Ethernet ports. Please refer to Section 14.9 for more information on how to set up local capture and configure remote packet capture with Wireshark.

7.2.6 Mobile Network

The **Mobile Network** statistics page shows traffic statistics over the LTE-800 mobile interface as shown in Figure 44. 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.



Mobile Network Data Usage	
Data Usage (Tx Bytes)	11.6 MB
Data Usage (Rx Bytes)	687.7 KB
Sent SMS	16

Data Connection: Connected

Mobile Network Statistics	
Failed SMS	0
Retried SMS	0
Queued SMS	0
Data Reconnection Count	0
Reboot Count	0
Reconfiguration Count	0
Tx Packet Ok	0
Rx Packet Ok	0
Tx Packet Error	0
Rx Packet Error	0
Tx Overflows	0
Rx Overflows	0
Bytes Ok (Tx)	0 B
Bytes Ok (Rx)	0 B
Tx Packet Drops	0
Rx Packet Drops	0

Figure 44: 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.

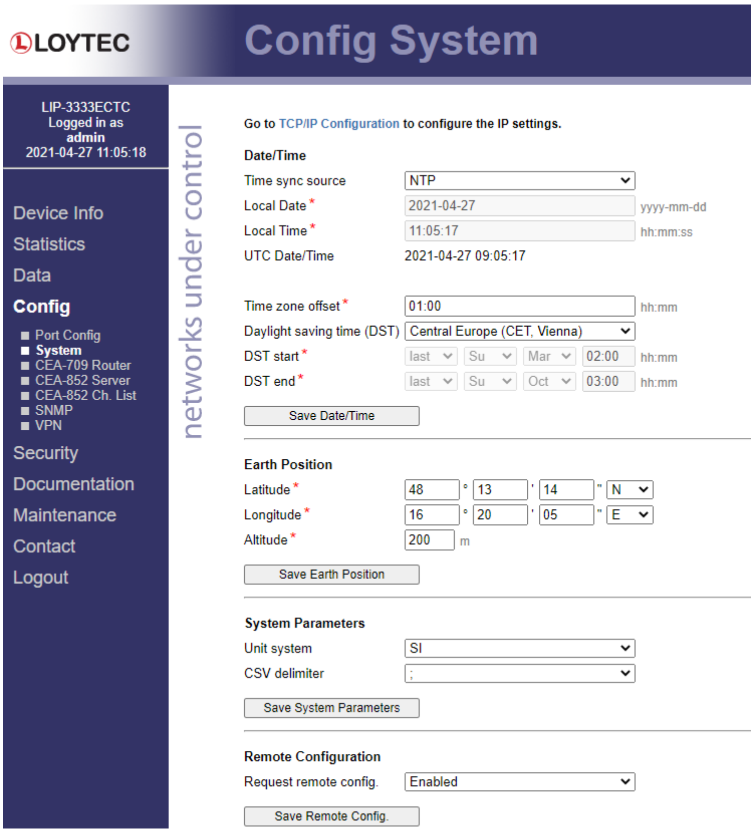
7.3 Device Configuration

The device configuration pages allow viewing and changing the device settings. Here are some general rules for setting IP addresses, port numbers, and time values:

- An empty IP address field disables the entry.
- An empty port number field sets the default port number.
- An empty time value field disables the time setting.

7.3.1 System Configuration

The system configuration page is shown in Figure 45. 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.



Go to TCP/IP Configuration to configure the IP settings.

Date/Time

Time sync source: NTP
Local Date *: 2021-04-27 yyyy-mm-dd
Local Time *: 11:05:17 hh:mm:ss
UTC Date/Time: 2021-04-27 09:05:17

Time zone offset *: 01:00 hh:mm
Daylight saving time (DST): Central Europe (CET, Vienna)
DST start *: last Su Mar 02:00 hh:mm
DST end *: last Su Oct 03:00 hh:mm

Earth Position

Latitude *: 48 ° 13 ' 14 " N
Longitude *: 16 ° 20 ' 05 " E
Altitude *: 200 m

System Parameters

Unit system: SI
CSV delimiter: ;

Remote Configuration

Request remote config.: Enabled

Figure 45: System Configuration Page, e.g., for Vienna, Austria.

The time sync source can be set to **auto**, **manual** or **NTP**. In the **auto** mode, the device switches to the first external time source that is discovered. 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 7.6.1).

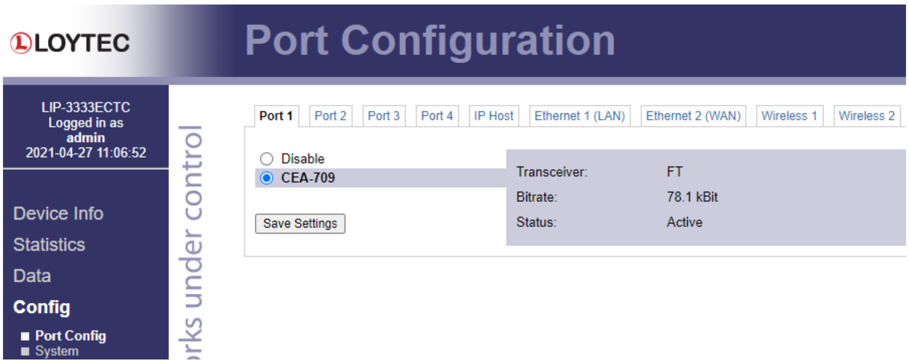
The time zone offset must be defined independently of the time source. It is specified as the offset to GMT in hours and minutes (e.g., Vienna/Austria is +01:00, New York/USA is -06:00). For setting the daylight saving time (DST) predefined choices are offered for Europe and USA/Canada. DST can be switched 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.

In **Remote Configuration** it can be configured, whether a replaced device shall automatically request its configuration from an LWEB-900 server.

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.

7.3.2 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 46. 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.



○ Disable
● CEA-709

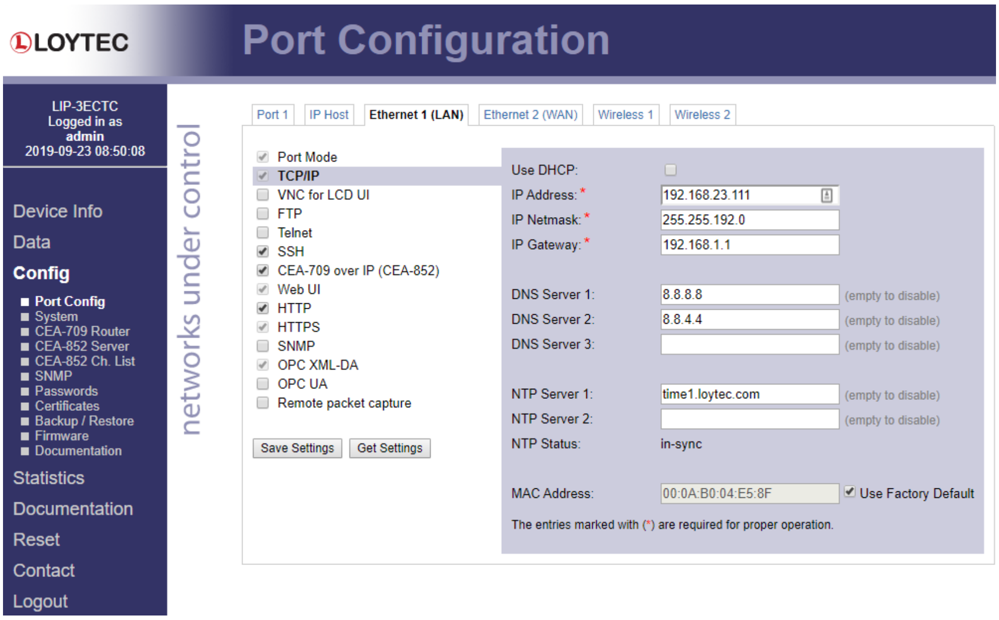
Transceiver: FT
Bitrate: 78.1 kBit
Status: Active

Figure 46: 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. Pressing **Get Settings** retrieves the current settings from the device.

7.3.3 IP Configuration

The TCP/IP configuration is done under the Ethernet port tab as shown in Figure 47. The mandatory IP settings, which are needed to operate 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.



☑ Port Mode
☑ TCP/IP
☐ VNC for LCD UI
☐ FTP
☐ Telnet
☑ SSH
☑ CEA-709 over IP (CEA-852)
☑ Web UI
☑ HTTP
☑ HTTPS
☐ SNMP
☑ OPC XML-DA
☐ OPC UA
☐ Remote packet capture

Use DHCP: ☐
IP Address:* 192.168.23.111
IP Netmask:* 255.255.192.0
IP Gateway:* 192.168.1.1

DNS Server 1: 8.8.8.8 (empty to disable)
DNS Server 2: 8.8.4.4 (empty to disable)
DNS Server 3: (empty to disable)

NTP Server 1: time1.loytec.com (empty to disable)
NTP Server 2: (empty to disable)
NTP Status: in-sync

MAC Address: 00:0A:B0:04:E5:8F ☑ Use Factory Default

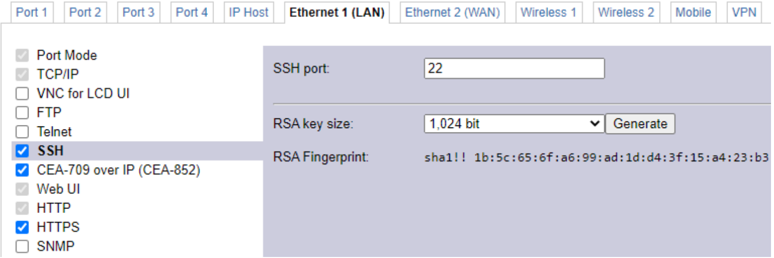
The entries marked with (*) are required for proper operation.

Figure 47: 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.

The settings for DNS and NTP servers should be made in the IP host settings (see Section 7.3.6). 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 the Ethernet interface are SSH, FTP, Telnet, 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 for SSH in Figure 48. Note that HTTP for the Web server can only be disabled on the LCD display or when opening the Web interface using HTTPS.



☑ Port Mode
☑ TCP/IP
□ VNC for LCD UI
□ FTP
□ Telnet
☑ SSH
☑ CEA-709 over IP (CEA-852)
☑ Web UI
☑ HTTP
☑ HTTPS
□ SNMP

SSH port: 22

RSA key size: 1,024 bit

RSA Fingerprint: sha1!! 1b:5c:65:6f:a6:99:ad:1d:d4:3f:15:a4:23:b3

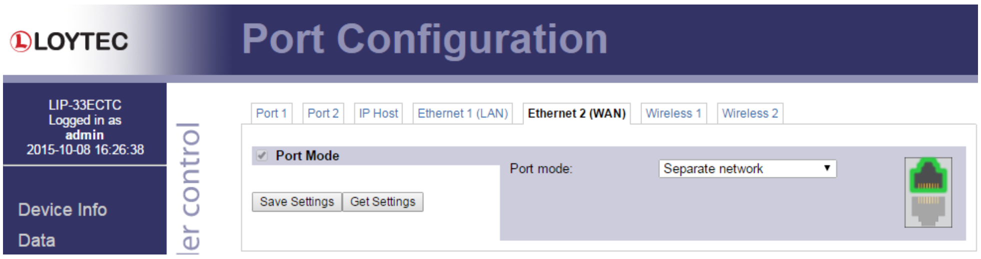
Figure 48: SSH server configuration on the Ethernet port.

7.3.4 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 49 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).

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). Physically, the two Ethernet ports will be plugged into different Ethernet switches.



LIP-33ECTC
Logged in as
admin
2015-10-08 16:26:38

☑ Port Mode

Port mode: Separate network

Figure 49: 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.

7.3.5 802.1X Port Authentication

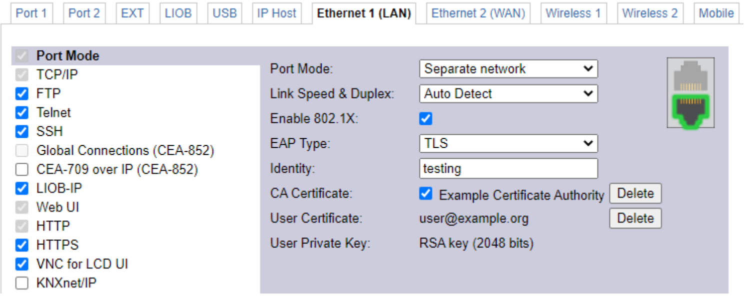
To further increase security in a network installation, IT departments support the 802.1X port authentication method. This standard requires a device to authenticate its port on the network switch, before traffic into the network is allowed.

LOYTEC devices can enable 802.1X port authentication in the **Port Mode** settings on the **Ethernet** tabs of the port configuration (see Figure 50). 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.



☑ Port Mode
☑ TCP/IP
☑ FTP
☑ Telnet
☑ SSH
□ Global Connections (CEA-852)
□ CEA-709 over IP (CEA-852)
☑ LIOB-IP
☑ Web UI
☑ HTTP
☑ HTTPS
☑ VNC for LCD UI
□ KNXnet/IP

Port Mode: Separate network
Link Speed & Duplex: Auto Detect
Enable 802.1X: ☑
EAP Type: TLS
Identity: testing
CA Certificate: ☑ Example Certificate Authority
User Certificate: user@example.org
User Private Key: RSA key (2048 bits)

Figure 50: 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.

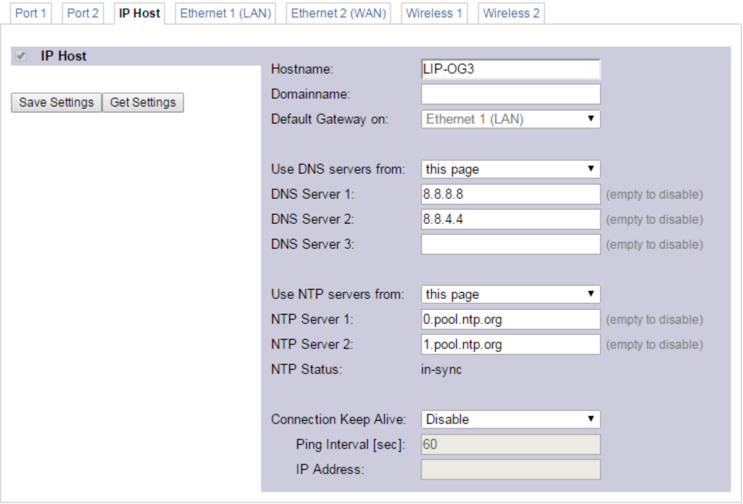
7.3.6 IP Host Configuration

The L-IP 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 51. 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.

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.



Hostname: LIP-OG3
Domainname:
Default Gateway on: Ethernet 1 (LAN)

Use DNS servers from: this page
DNS Server 1: 8.8.8.8 (empty to disable)
DNS Server 2: 8.8.4.4 (empty to disable)
DNS Server 3: (empty to disable)

Use NTP servers from: this page
NTP Server 1: 0.pool.ntp.org (empty to disable)
NTP Server 2: 1.pool.ntp.org (empty to disable)
NTP Status: in-sync

Connection Keep Alive: Disable
Ping Interval [sec]: 60
IP Address:

Figure 51: Setting on the IP Host tab.

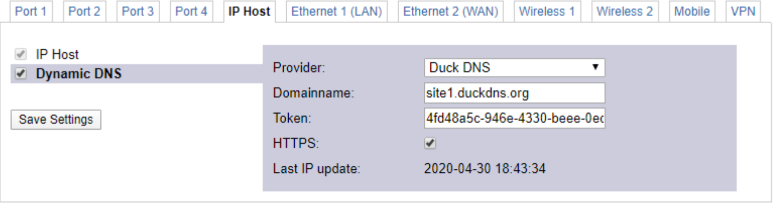
The device can be configured to synchronize its clock with NTP time. Enter the IP address of a primary and, optionally, a secondary NTP server. The device will use NTP as a time source if the time sync source in the system configuration page is set to **NTP** (see Section 7.3.1). The field **NTP status** 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.

7.3.7 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 10. 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.



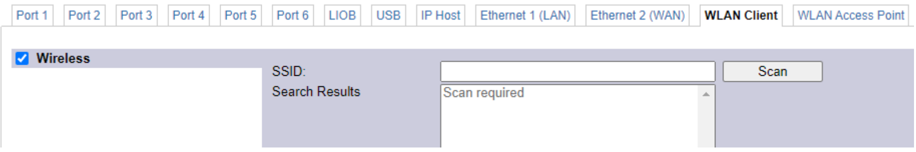
Provider: Duck DNS
Domainname: site1.duckdns.org
Token: 4fd48a5c-946e-4330-beee-0ec
HTTPS: ☑
Last IP update: 2020-04-30 18:43:34

Figure 52: Dynamic DNS Settings

7.3.8 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

12.5. Depending on the required wireless modes, select the WLAN Client or WLAN 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 53.



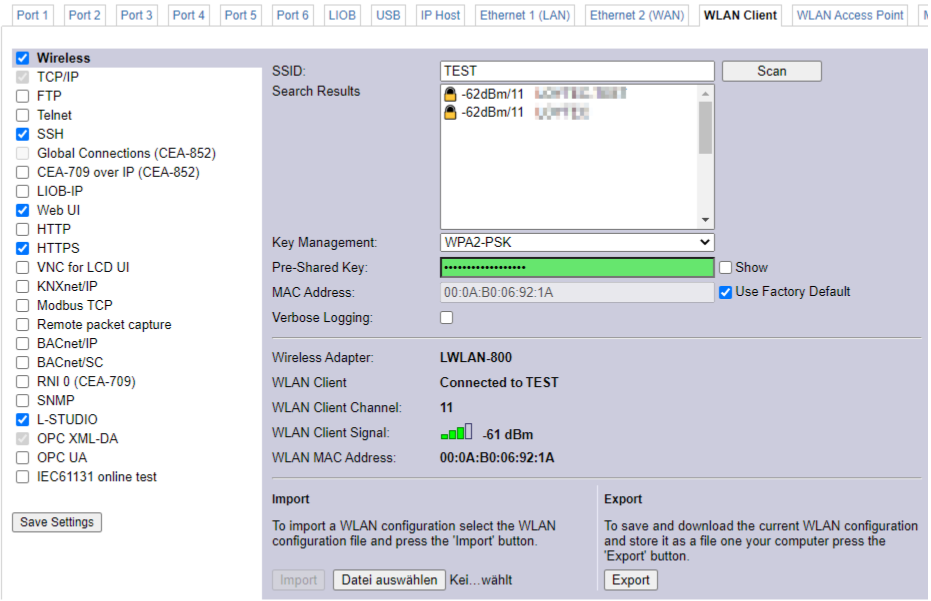
☑ Wireless

SSID:

Search Results: Scan required

Figure 53: Wireless Port Mode

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 54.



☑ Wireless
☑ TCP/IP
□ FTP
□ Telnet
☑ SSH
□ Global Connections (CEA-852)
□ CEA-709 over IP (CEA-852)
□ LIOB-IP
☑ Web UI
□ HTTP
☑ HTTPS
□ VNC for LCD UI
□ KNXnet/IP
□ Modbus TCP
□ Remote packet capture
□ BACnet/IP
□ BACnet/SC
□ RNI 0 (CEA-709)
□ SNMP
☑ L-STUDIO
☑ OPC XML-DA
□ OPC UA
□ IEC61131 online test

SSID: TEST

Search Results:
-62dBm/11 [redacted]
-62dBm/11 [redacted]

Key Management: WPA2-PSK

Pre-Shared Key: •••••••••••••••••• □ Show

MAC Address: 00:0A:B0:06:92:1A ☑ Use Factory Default

Verbose Logging: □

Wireless Adapter: LWLAN-800

WLAN Client: Connected to TEST

WLAN Client Channel: 11

WLAN Client Signal: -61 dBm

WLAN MAC Address: 00:0A:B0:06:92:1A

Import

To import a WLAN configuration select the WLAN configuration file and press the 'Import' button.

Export

To save and download the current WLAN configuration and store it as a file one your computer press the 'Export' button.

Figure 54: 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.

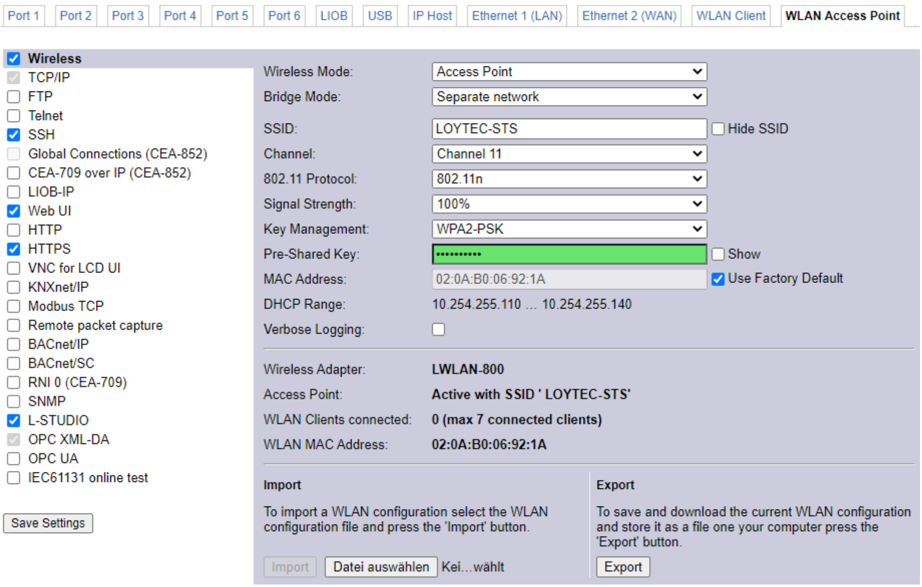
The page displays the following information:

- **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 7.3.9).

An access point has the settings shown in Figure 55.



☑ Wireless
☑ TCP/IP
☐ FTP
☐ Telnet
☑ SSH
☐ Global Connections (CEA-852)
☐ CEA-709 over IP (CEA-852)
☐ LIOB-IP
☑ Web UI
☐ HTTP
☑ HTTPS
☐ VNC for LCD UI
☐ KNXnet/IP
☐ Modbus TCP
☐ Remote packet capture
☐ BACnet/IP
☐ BACnet/SC
☐ RNI 0 (CEA-709)
☐ SNMP
☑ L-STUDIO
☑ OPC XML-DA
☐ OPC UA
☐ IEC61131 online test

Wireless Mode: Access Point
Bridge Mode: Separate network
SSID: LOYTEC-STS ☐ Hide SSID
Channel: Channel 11
802.11 Protocol: 802.11n
Signal Strength: 100%
Key Management: WPA2-PSK
Pre-Shared Key: •••••••••• ☐ Show
MAC Address: 02:0A:B0:06:92:1A ☑ Use Factory Default
DHCP Range: 10.254.255.110 ... 10.254.255.140
Verbose Logging: ☐

Wireless Adapter: **LWLAN-800**
Access Point: **Active with SSID ' LOYTEC-STS'**
WLAN Clients connected: **0 (max 7 connected clients)**
WLAN MAC Address: **02:0A:B0:06:92:1A**

Import

To import a WLAN configuration select the WLAN configuration file and press the 'Import' button.

Export

To save and download the current WLAN configuration and store it as a file one your computer press the 'Export' button.

Figure 55: 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 7.3.4. 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 13 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.

- **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.

- **Encryption Type**: This list selects between different encryption options, e.g. AES or TKIP.

- **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.

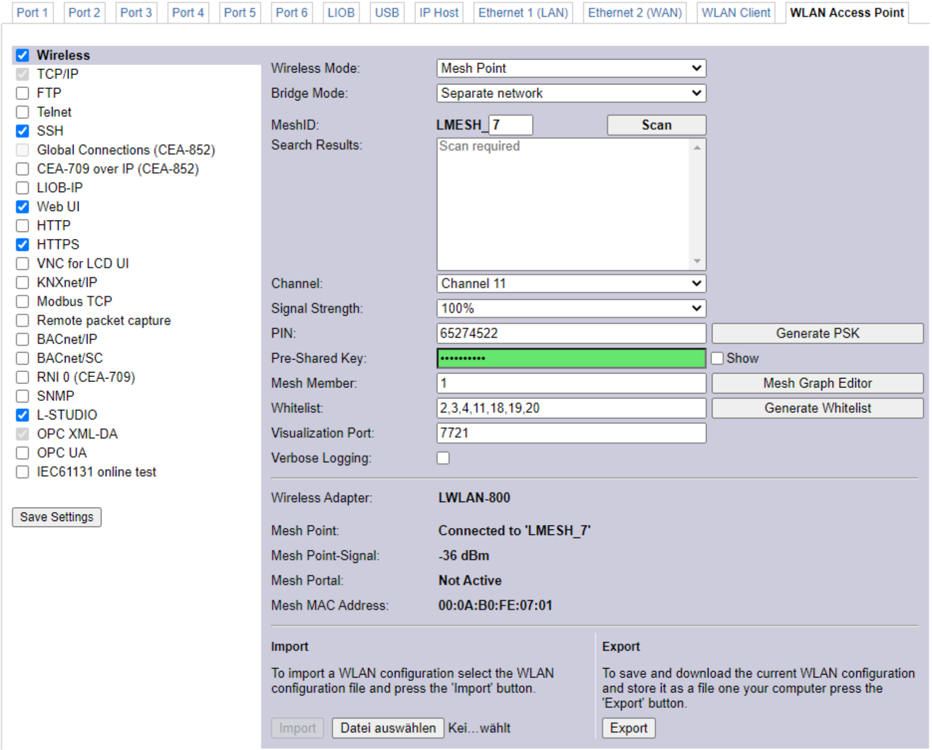
- **WLAN MAC-Address**: Displays the MAC address of the wireless adapter.

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.***

7.3.9 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 12.5.2 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 7.3.8. The configuration settings for the Mesh Point or Mesh Portal mode are shown in Figure 56.



☑ **Wireless**
☑ TCP/IP
□ FTP
□ Telnet
☑ SSH
□ Global Connections (CEA-852)
□ CEA-709 over IP (CEA-852)
□ LIOB-IP
☑ Web UI
□ HTTP
☑ HTTPS
□ VNC for LCD UI
□ KNXnet/IP
□ Modbus TCP
□ Remote packet capture
□ BACnet/IP
□ BACnet/SC
□ RNI 0 (CEA-709)
□ SNMP
☑ L-STUDIO
☑ OPC XML-DA
□ OPC UA
□ IEC61131 online test

Wireless Mode: Mesh Point
Bridge Mode: Separate network
MeshID: LMESH_ 7
Search Results: Scan required
Channel: Channel 11
Signal Strength: 100%
PIN: 65274522
Pre-Shared Key: ••••••••••
Mesh Member: 1
Whitelist: 2,3,4,11,18,19,20
Visualization Port: 7721
Verbose Logging: □

Wireless Adapter: **LWLAN-800**
Mesh Point: **Connected to 'LMESH_7'**
Mesh Point-Signal: **-36 dBm**
Mesh Portal: **Not Active**
Mesh MAC Address: **00:0A:B0:FE:07:01**

Import

To import a WLAN configuration select the WLAN configuration file and press the 'Import' button.

Kei...wählt

Export

To save and download the current WLAN configuration and store it as a file one your computer press the 'Export' button.

Figure 56: 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 7.3.4.

- **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.

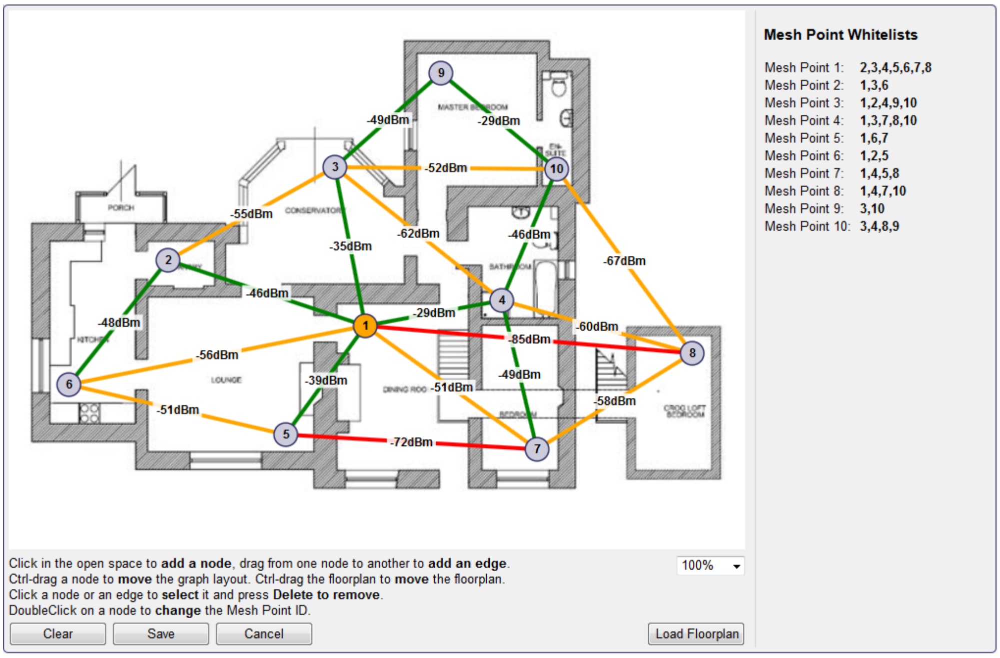
Mesh Graph Editor. This is a visual editor to assist a simple configuration of whitelists in the Mesh network as shown in Figure 57 and Figure 58. Depending on the configuration of Mesh points and connections between them in the Mesh graph, the resulting whitelist for this Mesh network graph is displayed. 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.



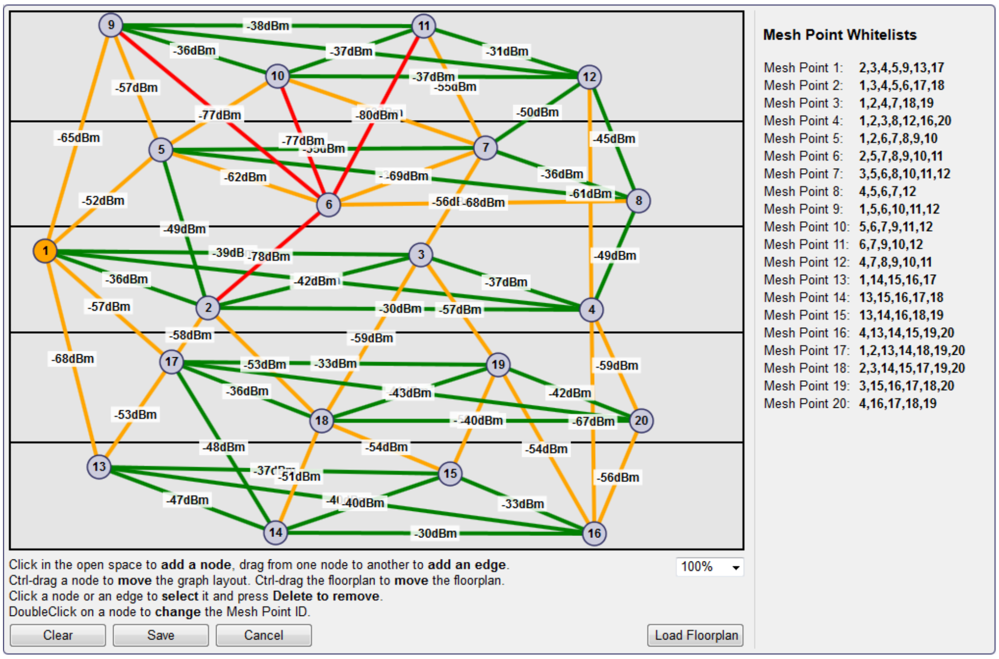
Mesh Point Whitelists

Mesh Point 1:	2,3,4,5,6,7,8
Mesh Point 2:	1,3,6
Mesh Point 3:	1,2,4,9,10
Mesh Point 4:	1,3,7,8,10
Mesh Point 5:	1,6,7
Mesh Point 6:	1,2,5
Mesh Point 7:	1,4,5,8
Mesh Point 8:	1,4,7,10
Mesh Point 9:	3,10
Mesh Point 10:	3,4,8,9

Click in the open space to **add a node**, drag from one node to another to **add an edge**.
Ctrl-drag a node to **move** the graph layout. Ctrl-drag the floorplan to **move** the floorplan.
Click a node or an edge to **select** it and press **Delete to remove**.
DoubleClick on a node to **change** the Mesh Point ID.

Figure 57: 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 57 shows the Mesh network visualization using a floorplan from the top view of the building. In contrast Figure 58 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.



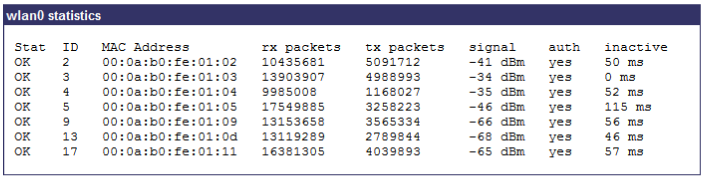
Mesh Point Whitelists

Mesh Point 1:	2,3,4,5,9,13,17
Mesh Point 2:	1,3,4,5,6,17,18
Mesh Point 3:	1,2,4,7,18,19
Mesh Point 4:	1,2,3,8,12,16,20
Mesh Point 5:	1,2,6,7,8,9,10
Mesh Point 6:	2,5,7,8,9,10,11
Mesh Point 7:	3,5,6,8,10,11,12
Mesh Point 8:	4,5,6,7,12
Mesh Point 9:	1,5,6,10,11,12
Mesh Point 10:	5,6,7,9,11,12
Mesh Point 11:	6,7,9,10,12
Mesh Point 12:	4,7,8,9,10,11
Mesh Point 13:	1,14,15,16,17
Mesh Point 14:	13,15,16,17,18
Mesh Point 15:	13,14,16,18,19
Mesh Point 16:	4,13,14,15,19,20
Mesh Point 17:	1,2,13,14,18,19,20
Mesh Point 18:	2,3,14,15,17,19,20
Mesh Point 19:	3,15,16,17,18,20
Mesh Point 20:	4,16,17,18,19

Click in the open space to **add a node**, drag from one node to another to **add an edge**.
Ctrl-drag a node to **move** the graph layout. Ctrl-drag the floorplan to **move** the floorplan.
Click a node or an edge to **select** it and press **Delete** to **remove**.
DoubleClick on a node to **change** the Mesh Point ID.

Figure 58: 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 59 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.



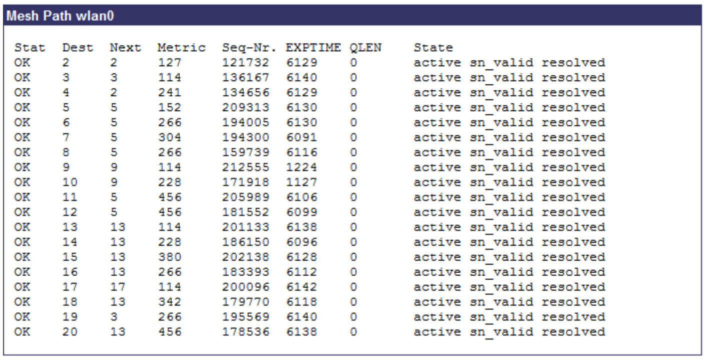
wlan0 statistics

```
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 59: 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 60 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
```

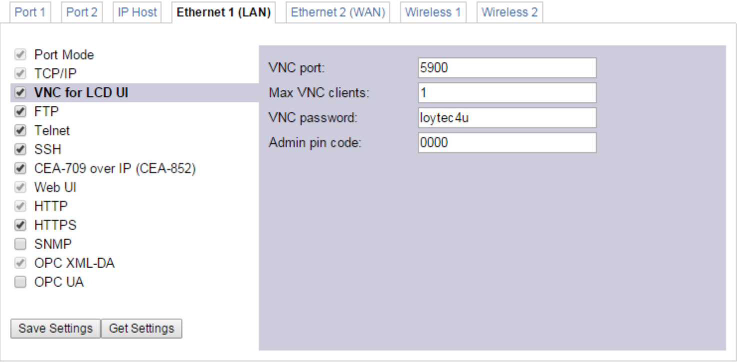
Figure 60: Mesh Path Statistics.

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.

7.3.10 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 61. 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'.



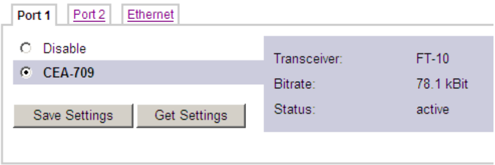
☑ Port Mode
☑ TCP/IP
☑ VNC for LCD UI
☑ FTP
☑ Telnet
☑ SSH
☑ CEA-709 over IP (CEA-852)
☑ Web UI
☑ HTTP
☑ HTTPS
□ SNMP
☑ OPC XML-DA
□ OPC UA

VNC port: 5900
Max VNC clients: 1
VNC password: loytec4u
Admin pin code: 0000

Figure 61: VNC Configuration.

7.3.11 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 62. 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.



○ Disable
● CEA-709

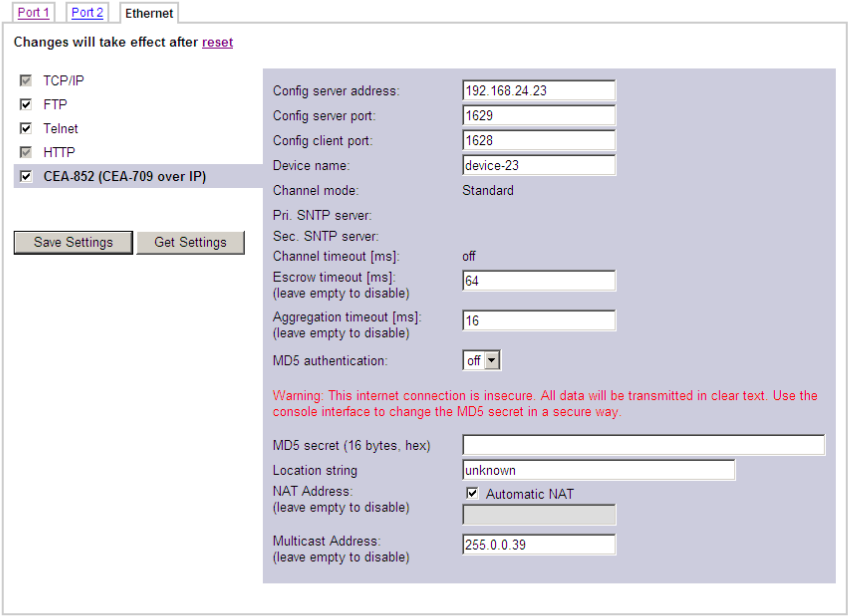
Transceiver: FT-10
Bitrate: 78.1 kBit
Status: active

Figure 62: CEA-709 Configuration Page.

7.3.12 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.

The CEA-852 protocol settings are displayed in the settings box on the right-hand side as shown in Figure 63. 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-IP and sends its configuration.



Changes will take effect after reset

☑ TCP/IP
☑ FTP
☑ Telnet
☑ HTTP
☑ CEA-852 (CEA-709 over IP)

Config server address: 192.168.24.23
Config server port: 1629
Config client port: 1628
Device name: device-23
Channel mode: Standard
Pri. SNTP server:
Sec. SNTP server:
Channel timeout [ms]: off
Escrow timeout [ms]: (leave empty to disable) 64
Aggregation timeout [ms]: (leave empty to disable) 16
MD5 authentication: off

Warning: This internet connection is insecure. All data will be transmitted in clear text. Use the console interface to change the MD5 secret in a secure way.

MD5 secret (16 bytes, hex)
Location string: unknown
NAT Address: (leave empty to disable) ☑ Automatic NAT
Multicast Address: (leave empty to disable) 255.0.0.39

Figure 63: 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-IP and the IP channel. The field **Config client port** represents the IP port of the device'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 Section 8.3 to learn more about NAT configuration.

In the field **Device name** the user can enter a descriptive name for the L-IP, 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 Section 8.3 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-IP 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 L-IP.

The field **MD5 authentication** enables or disables MD5 authentication. 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.

Note: *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.*

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-IP 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-IP 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 Section 8.4.

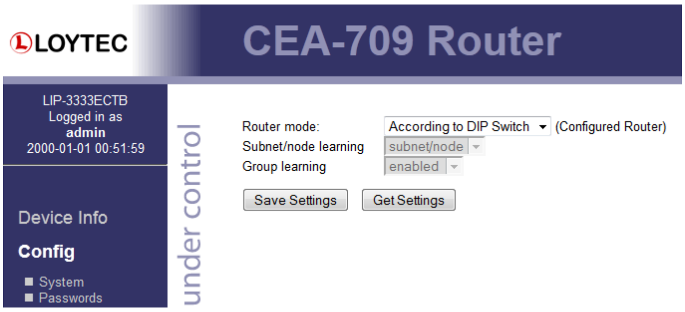
7.3.13 CEA-709 Router Configuration

The CEA-709 router configuration page allows configuring the built-in router mode. Available modes are **Configured Router** and **Smart Switch**. The device must be rebooted to let the changes on this page take effect.

Choose Configured Router mode if you want to use the L-IP as a standard configured CEA-709 router that can be commissioned and 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 device’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**.

Per default the router mode is set according to the DIP switches. See Section 8.1 for more information on the different router modes.



Router mode: According to DIP Switch (Configured Router)
Subnet/node learning: subnet/node
Group learning: enabled

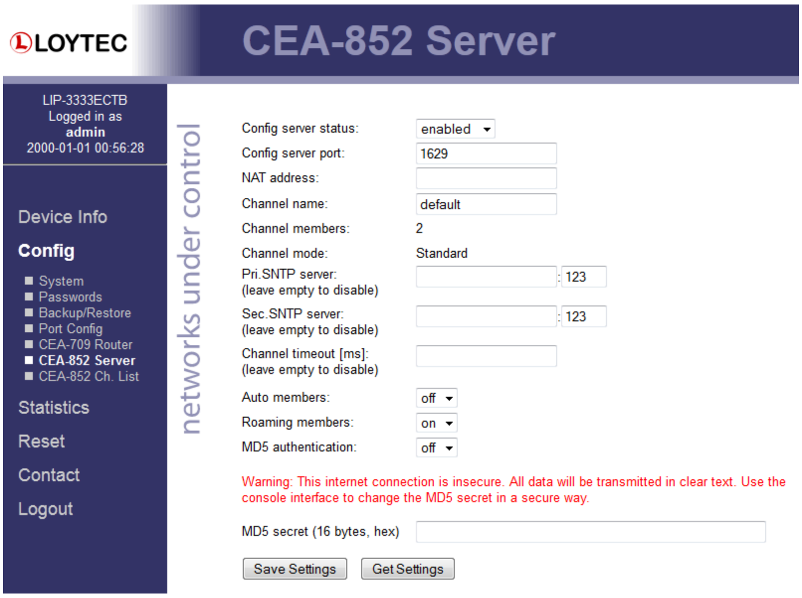
Figure 64: CEA-709 Router Configuration Page.

7.3.14 CEA-852 Server Configuration

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. Then the configuration server settings page appears as shown in Figure 65. If the configuration server is enabled the green configuration server LED labeled **Server** 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-IP 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 8.3.2 to learn more about the implications of this mode.



Config server status: enabled
Config server port: 1629
NAT address:
Channel name: default
Channel members: 2
Channel mode: Standard
Pri.SNTP server: (leave empty to disable) : 123
Sec.SNTP server: (leave empty to disable) : 123
Channel timeout [ms]: (leave empty to disable)
Auto members: off
Roaming members: on
MD5 authentication: off

Warning: This internet connection is insecure. All data will be transmitted in clear text. Use the console interface to change the MD5 secret in a secure way.

MD5 secret (16 bytes, hex)

Figure 65: Configuration server settings.

Enter NTP timer server address and ports in the fields **Primary SNTP** and **Secondary SNTP**. The L-IP 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 8.5. 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 device'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 8.3.1. 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. 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.

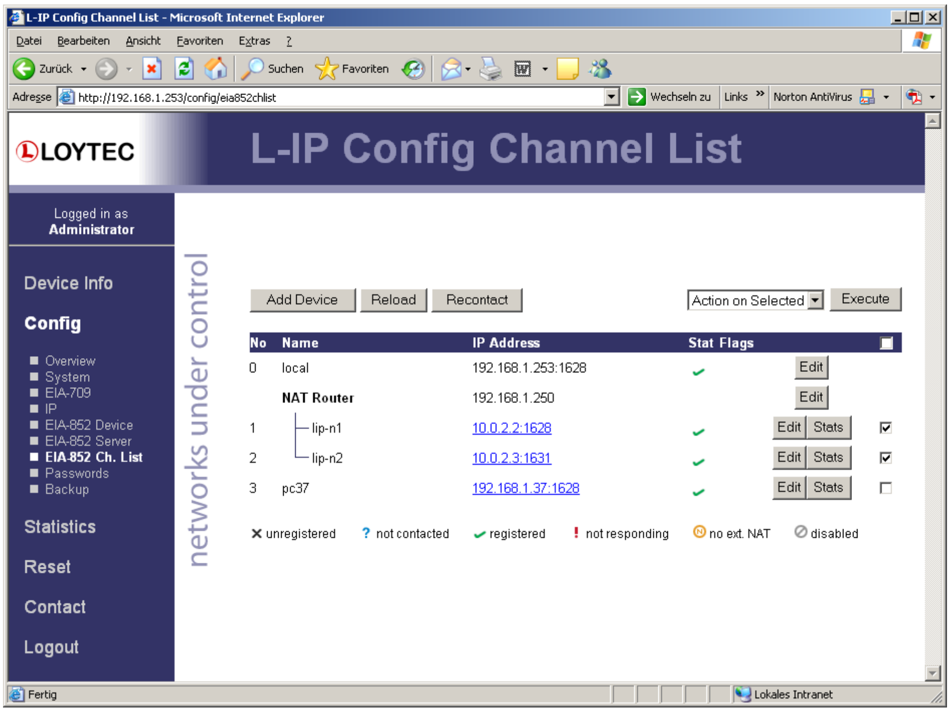
Note: *MD5 authentication cannot be used together with the Echelon's i.LON 1000 since the i.LON 1000 is not fully compliant with the CEA-852 authentication method. MD5 can be used with the i.LON 600.*

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.

7.3.15 CEA-852 Channel List

If the configuration server is enabled on the device, the CEA-852 device list can be seen in the CEA-852 Channel list menu. An example is given in Figure 66.

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 8.3.2.



No	Name	IP Address	Stat	Flags		
0	local	192.168.1.253:1628	✓	Edit		
	NAT Router	192.168.1.250		Edit		
1	lip-n1	10.0.2.2:1628	✓	Edit	Stats	☑
2	lip-n2	10.0.2.3:1631	✓	Edit	Stats	☑
3	pc37	192.168.1.37:1628	✓	Edit	Stats	□

✗ unregistered ? not contacted ✓ registered ! not responding Ⓝ no ext. NAT ⊘ disabled

Figure 66: IP-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 5. 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 5: Possible Communication Problems in the Configuration Server.

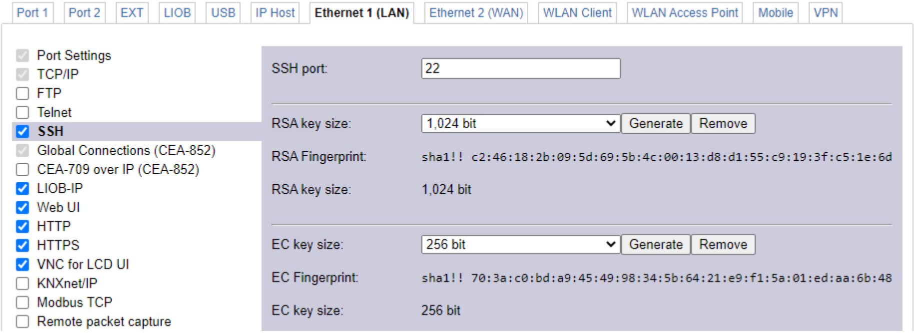
7.3.16 SSH Server Configuration

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 67.

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 keys 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.



☑ Port Settings
☑ TCP/IP
☐ FTP
☐ Telnet
☑ **SSH**
☑ Global Connections (CEA-852)
☐ CEA-709 over IP (CEA-852)
☑ LIOB-IP
☑ Web UI
☑ HTTP
☑ HTTPS
☑ VNC for LCD UI
☐ KNXnet/IP
☐ Modbus TCP
☐ Remote packet capture

SSH port: 22

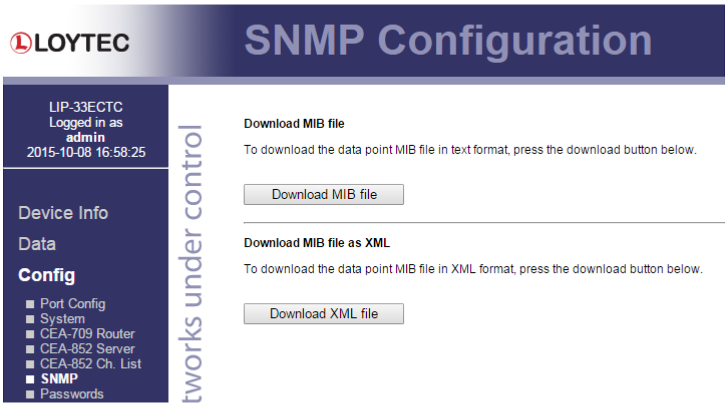
RSA key size: 1,024 bit [Generate] [Remove]
RSA Fingerprint: sha1!! c2:46:18:2b:09:5d:69:5b:4c:00:13:d8:d1:55:c9:19:3f:c5:1e:6d
RSA key size: 1,024 bit

EC key size: 256 bit [Generate] [Remove]
EC Fingerprint: sha1!! 70:3a:c0:bd:a9:45:49:98:34:5b:64:21:e9:f1:5a:01:ed:aa:6b:48
EC key size: 256 bit

Figure 67: SSH Configuration.

7.3.17 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 68. 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 11.1.



LIP-33ECTC
Logged in as
admin
2015-10-08 16:58:25

Download MIB file

To download the data point MIB file in text format, press the download button below.

Download MIB file as XML

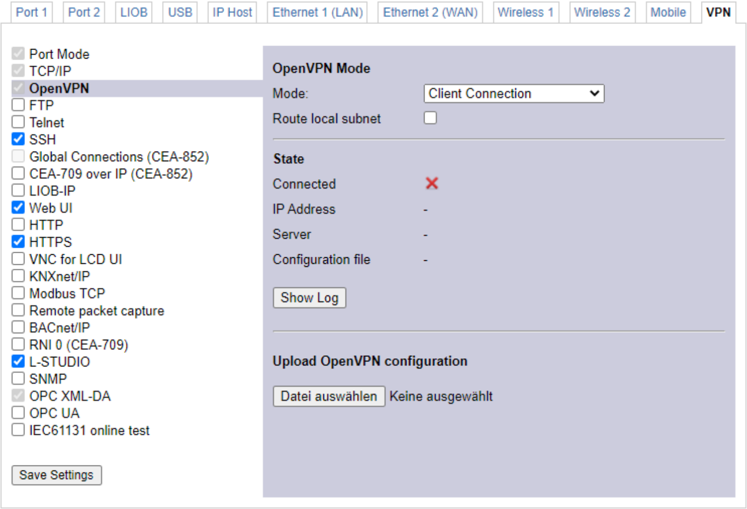
To download the data point MIB file in XML format, press the download button below.

Figure 68: Get the SNMP MIB from the Web interface

7.3.18 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 69.

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).



Port 1 | Port 2 | LIOB | USB | IP Host | Ethernet 1 (LAN) | Ethernet 2 (WAN) | Wireless 1 | Wireless 2 | Mobile | VPN

- ☑ Port Mode
- ☑ TCP/IP
- ☑ OpenVPN
- ☐ FTP
- ☐ Telnet
- ☑ SSH
- ☐ Global Connections (CEA-852)
- ☐ CEA-709 over IP (CEA-852)
- ☐ LIOB-IP
- ☑ Web UI
- ☐ HTTP
- ☑ HTTPS
- ☐ VNC for LCD UI
- ☐ KNXnet/IP
- ☐ Modbus TCP
- ☐ Remote packet capture
- ☐ BACnet/IP
- ☐ RNI 0 (CEA-709)
- ☑ L-STUDIO
- ☐ SNMP
- ☑ OPC XML-DA
- ☐ OPC UA
- ☐ IEC61131 online test

Save Settings

OpenVPN Mode

Mode: Client Connection

Route local subnet ☐

State

Connected ✗

IP Address -

Server -

Configuration file -

Show Log

Upload OpenVPN configuration

Datei auswählen Keine ausgewählt

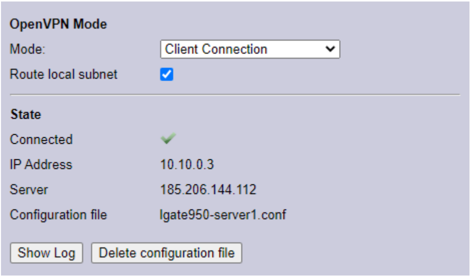
Figure 69: OpenVPN client configuration.

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 70. 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.



OpenVPN Mode

Mode: Client Connection

Route local subnet ☑

State

Connected ✓

IP Address 10.10.0.3

Server 185.206.144.112

Configuration file lgate950-server1.conf

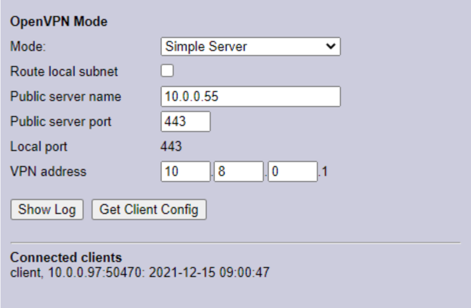
Show Log | Delete configuration file

Figure 70: 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 71). 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.



OpenVPN Mode

Mode: Simple Server

Route local subnet □

Public server name 10.0.0.55

Public server port 443

Local port 443

VPN address 10 . 8 . 0 . 1

Connected clients

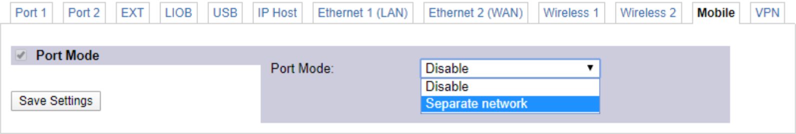
client, 10.0.0.97:50470: 2021-12-15 09:00:47

Figure 71: 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.

7.3.19 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 72 and click **Save Settings**.

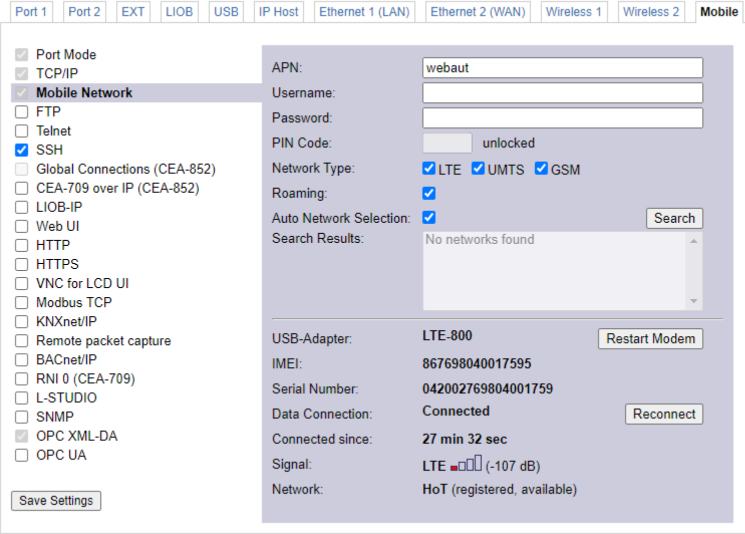


Port Mode

Port Mode: Disable

Figure 72: Enable LTE via port mode

This enables the LTE interface and jumps to the **Mobile network** settings section as shown in Figure 73. 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.



☑ Port Mode
☑ TCP/IP
☑ **Mobile Network**
□ FTP
□ Telnet
☑ SSH
□ Global Connections (CEA-852)
□ CEA-709 over IP (CEA-852)
□ LIOB-IP
□ Web UI
□ HTTP
□ HTTPS
□ VNC for LCD UI
□ Modbus TCP
□ KNXnet/IP
□ Remote packet capture
□ BACnet/IP
□ RNI 0 (CEA-709)
□ L-STUDIO
□ SNMP
☑ OPC XML-DA
□ OPC UA

Save Settings

APN: webaut
Username:
Password:
PIN Code: unlocked
Network Type: ☑ LTE ☑ UMTS ☑ GSM
Roaming: ☑
Auto Network Selection: ☑ Search
Search Results: No networks found

USB-Adapter: LTE-800 Restart Modem
IMEI: 867698040017595
Serial Number: 042002769804001759
Data Connection: Connected Reconnect
Connected since: 27 min 32 sec
Signal: LTE (-107 dB)
Network: HoT (registered, available)

Figure 73: 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 7.2.6).

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 74.

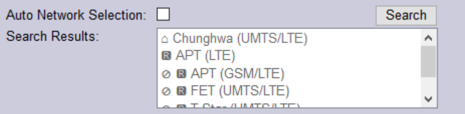

Auto Network Selection: □ Search
Search Results:
⌂ Chunghwa (UMTS/LTE)
🅁 APT (LTE)
⊘ 🅁 APT (GSM/LTE)
⊘ 🅁 FET (UMTS/LTE)
⊘ 🅁 T Star (UMTS/LTE)

Figure 74: Scan result of mobile networks

The icons in the result list have the following meaning:

⌂ Home network

⊘ Not allowed (foreign network)

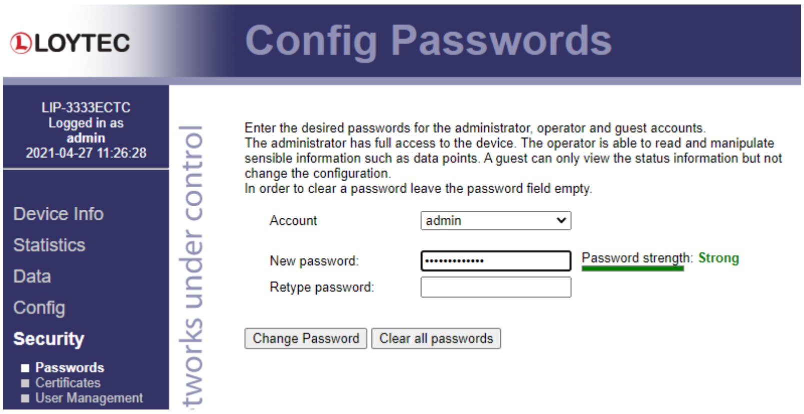
🅁 Roaming: To use this network also select the Roaming checkbox.

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

7.4 Security

7.4.1 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 75.



Enter the desired passwords for the administrator, operator and guest accounts.
The administrator has full access to the device. The operator is able to read and manipulate sensible information such as data points. A guest can only view the status information but not change the configuration.
In order to clear a password leave the password field empty.

Account: admin

New password: ••••••••••••• Password strength: Strong

Retype password:

Figure 75: 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.

7.4.2 Certificate Management

Some L-IP 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.

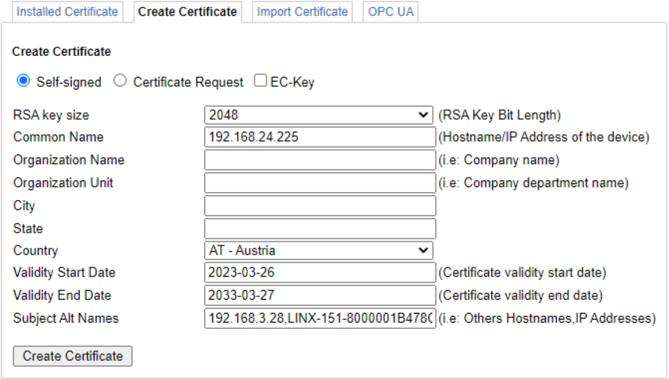
When connecting with a web browser to the LOYTEC device you will be warned that the server uses a self-signed certificate. You need to accept the certificate in order to continue. In some browsers this is also called “adding an exception”.

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 76. 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.



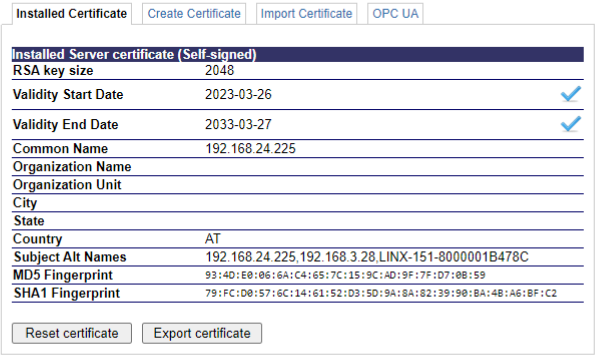
Create Certificate

● Self-signed ○ Certificate Request □ EC-Key

RSA key size	2048	(RSA Key Bit Length)
Common Name	192.168.24.225	(Hostname/IP Address of the device)
Organization Name		(i.e: Company name)
Organization Unit		(i.e: Company department name)
City		
State		
Country	AT - Austria	
Validity Start Date	2023-03-26	(Certificate validity start date)
Validity End Date	2033-03-27	(Certificate validity end date)
Subject Alt Names	192.168.3.28,LINX-151-8000001B478(	(i.e: Others Hostnames,IP Addresses)

Figure 76: 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 77 below). Reboot the device to activate the change.



Installed Server certificate (Self-signed)		
RSA key size	2048	
Validity Start Date	2023-03-26	✓
Validity End Date	2033-03-27	✓
Common Name	192.168.24.225	
Organization Name		
Organization Unit		
City		
State		
Country	AT	
Subject Alt Names	192.168.24.225,192.168.3.28,LINX-151-8000001B478C	
MD5 Fingerprint	93:4D:E0:06:6A:C4:65:7C:15:9C:AD:9F:7F:D7:0B:59	
SHA1 Fingerprint	79:FC:D0:57:6C:14:61:52:D3:5D:9A:8A:82:39:90:BA:4B:A6:BF:C2	

Figure 77: New created self-signed certificate

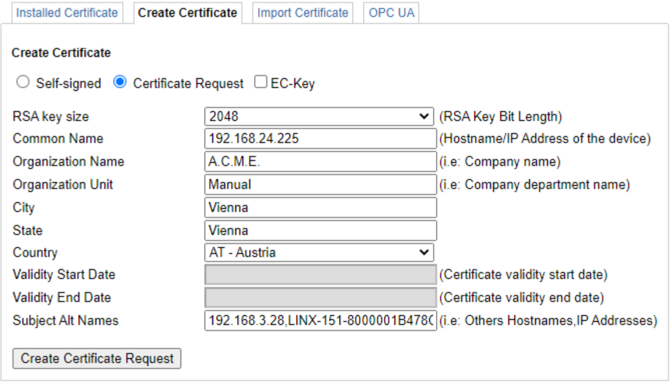
To widen acceptance of the LOYTEC server in a hostile environment (e.g. when using over the Internet), consider installing a server certificate signed by a certification authority to prevent man-in-the-middle attacks. HTTPS and OPC UA servers use X.509 certificates to authenticate themselves to clients. 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 78. 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**.



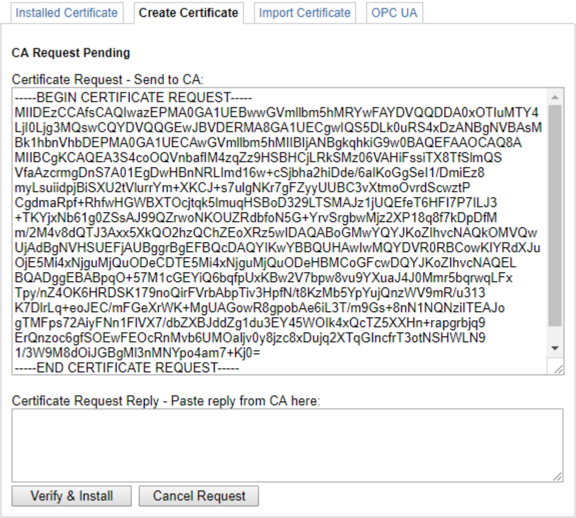
Create Certificate

○ Self-signed ● Certificate Request □ EC-Key

RSA key size	2048	(RSA Key Bit Length)
Common Name	192.168.24.225	(Hostname/IP Address of the device)
Organization Name	A.C.M.E.	(i.e: Company name)
Organization Unit	Manual	(i.e: Company department name)
City	Vienna	
State	Vienna	
Country	AT - Austria	
Validity Start Date		(Certificate validity start date)
Validity End Date		(Certificate validity end date)
Subject Alt Names	192.168.3.28,LINX-151-8000001B478(	(i.e: Others Hostnames,IP Addresses)

Figure 78: Create a CA certificate request.

2. Copy the X.509 certificate request from the Web page as shown in Figure 79 and follow up with the instructions provided by the certification authority.



CA Request Pending

Certificate Request - Send to CA:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDEzCCAfsCAQIwazEPMA0GA1UEBwwGVmllbm5hMRYwFAYDVQQDDA0xOTIuMTY4
LjI0Ljg3MQswCQYDVQQGEwJBVDERMA8GA1UECgwIQS5DLk0uRS4xDzANBgNVBAsM
Bk1hbnVhbDEPMA0GA1UECAwGVmllbm5hMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA3S4coOQVnbafIM4zqZz9HSBHCjLRkSMz06VAHiFssiTX8TfSlmQS
VfaAzcrmgDnS7A01EgDwHBnNRLImd16w+cSjbha2hiDde/6aIKoGgSeI1/DmiEz8
myLsuiidpjBiSXU2tVlurrYm+XKCJ+s7ulgNKr7gFZyyUUBC3vXtmoOvrdScwztP
CgdmaRpf+RhfwHGWBXTOcjtqk5lmuqHSBoD329LTSMAJz1jUQEfeT6HFI7P7ILJ3
+TKYjxNb61g0ZSsAJ99QZrwoNKOUZRdbfoN5G+YrvSrgbwMjz2XP18q8f7kDpDfM
m/2M4v8dQTJ3Axx5XkQO2hzQChZEoXRz5wIDAQABoGMwYQYJKoZIhvcNAQkOMVQw
UjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwMQYDVR0RBCowKIYRdXJu
OjE5Mi4xNjguMjQuODeCDTE5Mi4xNjguMjQuODeHBMCoGFcwDQYJKoZIhvcNAQEL
BQADggEBABpqO+57M1cGEYiQ6bqfpUxKBw2V7bpw8vu9YXuaJ4J0Mmr5bqrwqLFx
Tpy/nZ4OK6HRDSK179noQirFVrbAbpTiv3HpfN/t8KzMb5YpYujQnzWV9mR/u313
K7DIrLq+eoJEC/mFGeXrWK+MgUAGowR8gpobAe6iL3T/m9Gs+8nN1NQNziITEAJo
gTMFps72AiyFNn1FIVX7/dbZXBJddZg1du3EY45WOIk4xQcTZ5XXHn+rapgrbjq9
ErQnzoc6gfSOEwFEOcRnMvb6UMOaljv0y8jzc8xDujq2XTqGIncfrT3otNSHWLN9
1/3W9M8dOiJGBgMI3nMNYpo4am7+Kj0=
-----END CERTIFICATE REQUEST-----
```

Certificate Request Reply - Paste reply from CA here:

Figure 79: 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 79 and click **Verify & Install**.

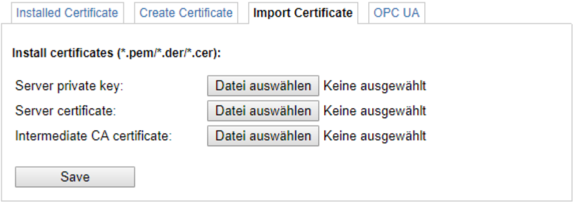
6. After next reboot, the server uses the imported certificate, so that the web browsers will indicate the page as trustworthy.

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 80 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.



Install certificates (*.pem/*.der/*.cer):

Server private key:	Datei auswählen	Keine ausgewählt
Server certificate:	Datei auswählen	Keine ausgewählt
Intermediate CA certificate:	Datei auswählen	Keine ausgewählt

Figure 80: Install a certificate on the Web interface.

7.4.3 User Management

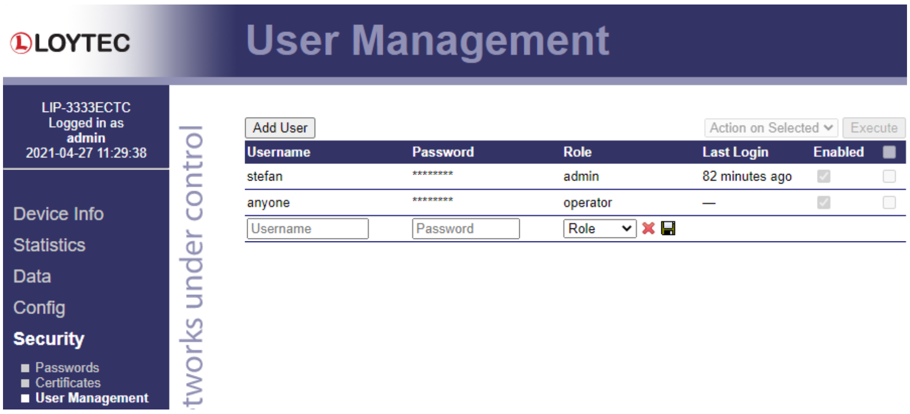
The device has three pre-defined user accounts: (1) **guest** allows the user to view certain information only, e.g., the device info page. By default the guest user has no password. (2) **operator** is able to read more sensible information such as calendar data. (3) **admin** has full access to the 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.

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 81). 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.



LIP-3333ECTC
Logged in as
admin
2021-04-27 11:29:38

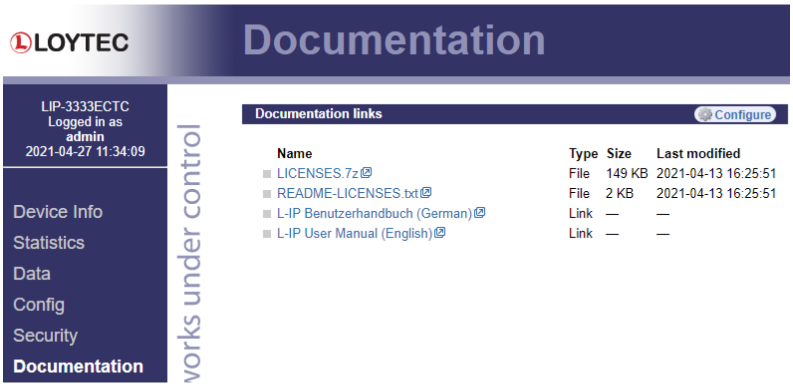
Username	Password	Role	Last Login	Enabled	□
stefan	********	admin	82 minutes ago	☑	□
anyone	********	operator	—	☑	□
Username	Password	Role			

Figure 81: 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.

7.5 Documentation

The documentation page allows to access documentation related to the device. See Section 7.6.3 on how to configure documentation links and upload documentation files accessible via this page.



Name	Type	Size	Last modified
LICENSES.7z	File	149 KB	2021-04-13 16:25:51
README-LICENSES.txt	File	2 KB	2021-04-13 16:25:51
L-IP Benutzerhandbuch (German)	Link	—	—
L-IP User Manual (English)	Link	—	—

Figure 82: Documentation Page.

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

7.6 Maintenance

7.6.1 Backup and Restore

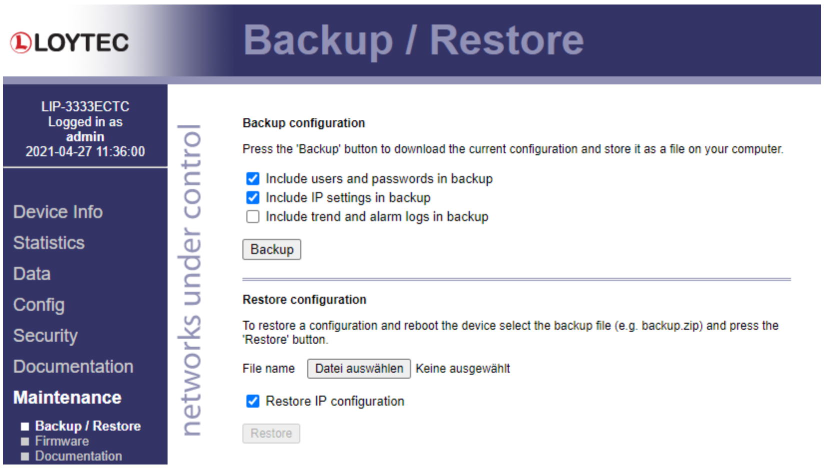
A configuration backup of the device can be downloaded via the Web interface. Press the backup link as shown in Figure 83 to start the download. The device assembles a single file including all required files. A file requestor dialog allows specifying the location where the backup file shall be stored.

Some contents of the backup archive can be controlled by the option check boxes. By default passwords and IP settings are included. When clearing the check box from passwords or IP settings, the respective items are excluded from the backup archive. 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, etc.),
- CEA-709 commissioning information,
- CEA-852 device and configuration server information (if enabled),

- L-IP redundant configuration data (node list, parameters, etc),
- Uploaded documentation and documentation links.



Backup configuration

Press the 'Backup' button to download the current configuration and store it as a file on your computer.

☑ Include users and passwords in backup
☑ Include IP settings in backup
☐ Include trend and alarm logs in backup

Restore configuration

To restore a configuration and reboot the device select the backup file (e.g. backup.zip) and press the 'Restore' button.

File name Keine ausgewählt

☑ Restore IP configuration

Figure 83: Backup/Restore page.

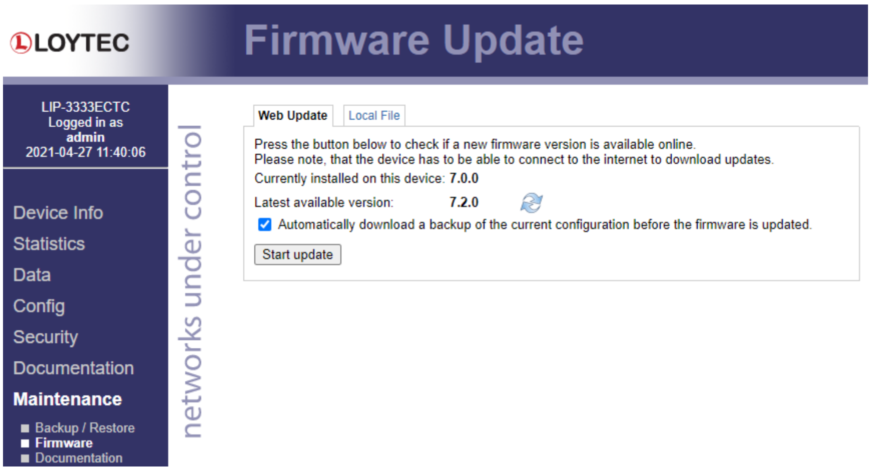
Note: *Backups created with firmware versions prior to version 6.0 cannot be restored on firmware versions 6.0 and up! Please make sure you re-create backups when upgrading the firmware!*

7.6.2 Firmware

The firmware page allows upgrading the device's firmware over the Web interface using genuine LOYTEC firmware images, ensured by a signature check. Integrity of the image is ensured by a firmware signature. The Web interface 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.



Press the button below to check if a new firmware version is available online.
Please note, that the device has to be able to connect to the internet to download updates.
Currently installed on this device: **7.0.0**

Latest available version: **7.2.0**

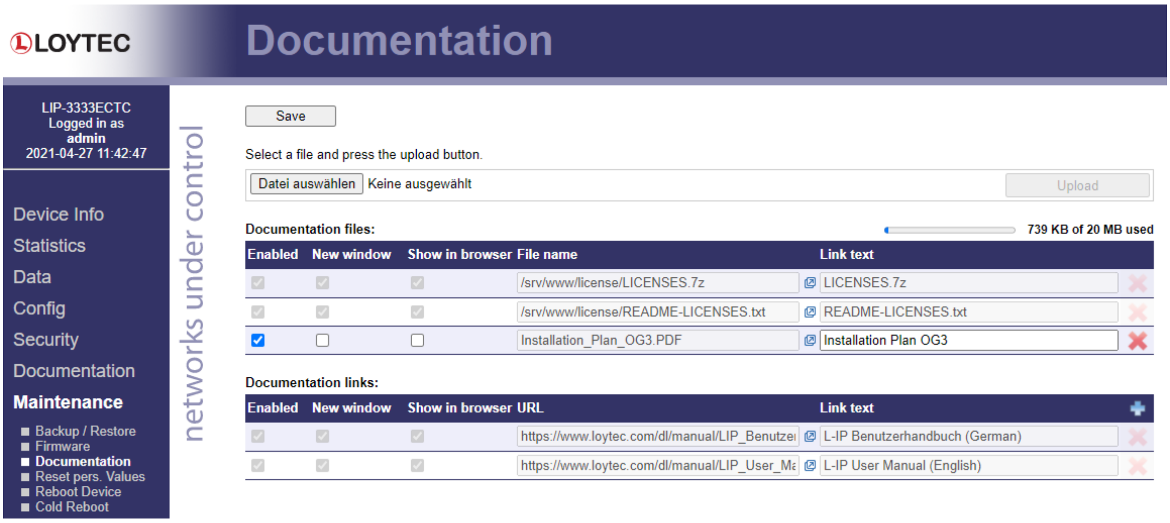
☑ Automatically download a backup of the current configuration before the firmware is updated.

Figure 84: 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**.

7.6.3 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 7.5).



Select a file and press the upload button.

Keine ausgewählt

Documentation files: 739 KB of 20 MB used

Enabled	New window	Show in browser	File name	Link text
☑	☑	☑	/srv/www/license/LICENSES.7z	LICENSES.7z
☑	☑	☑	/srv/www/license/README-LICENSES.txt	README-LICENSES.txt
☑	☐	☐	Installation_Plan_OG3.PDF	Installation Plan OG3

Documentation links:

Enabled	New window	Show in browser	URL	Link text
☑	☑	☑	https://www.loytec.com/dl/manual/LIP_Benutzer	L-IP Benutzerhandbuch (German)
☑	☑	☑	https://www.loytec.com/dl/manual/LIP_User_Ma	L-IP User Manual (English)

Figure 85: 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.

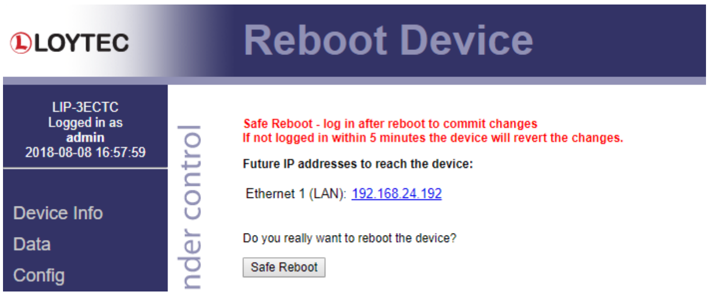
7.6.4 Rebooting and Clearing Data

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.

7.6.5 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 86.



Safe Reboot - log in after reboot to commit changes
If not logged in within 5 minutes the device will revert the changes.

Future IP addresses to reach the device:

Ethernet 1 (LAN): 192.168.24.192

Do you really want to reboot the device?

Figure 86: 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.

7.7 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.

8 Operating Modes

The L-IP routes CEA-709 packets over IP (Internet/Intranet) networks. Depending on the use case the L-IP supports different operating modes how packets are routed between the CEA-709 side and the IP side. The L-IP can be used as a client device on the IP channel, as a configuration server on the IP channel, or as a client device and configuration server at the same time.

8.1 CEA-709 Router - Operating Modes

Depending on the DIP switch settings of DIP switch 1 and 2 the L-IP supports 4 different methods to route packets between the CEA-709 and the IP channel. The 4 operating modes are listed below and described in more detail in the subsequent sections.

- OFF-OFF: The L-IP acts like a standard CEA-709 configured router (i.LON 1000/600 alike)

- ON-ON: The L-IP acts as a self-learning plug&play router ("smart switch mode")

- ON-OFF: The L-IP acts as a store-and-forward repeater

- OFF-ON: The L-IP learns the network topology but doesn't flood subnet broadcasts

Important: ***The L-IP Redundant supports only Configured Router Mode!***

8.1.1 Configured Router Mode

In this operating mode the L-IP 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.

Figure 87 shows the proper DIP-switch settings for configured router mode, assuming all other DIP-switches remain in the factory default position. This DIP-switch setting is the factory default setting. The series "C" L-IP models do not have DIP switches.

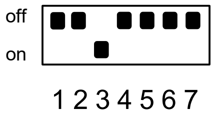


Figure 87: OFF-OFF: DIP-switch settings for configured router mode (factory default).

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.

8.1.2 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).

Figure 88 shows the proper DIP-switch setting to put the L-IP into smart switch mode. The series "C" L-IP models do not have DIP switches.

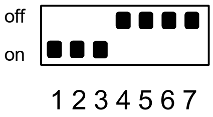


Figure 88: ON-ON: DIP-switch setting for smart switch mode.

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 (see Section 6.5.1).***

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 8.1.4).

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 8.1.1 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 8.4 on how to configure the device to use multi-cast.

8.1.3 Store-and-Forward Repeater Mode

The L-IP can be configured to operate in a repeater mode, where all messages are forwarded regardless of the address format. To put the L-IP into repeater mode the following steps need to be performed:

- DIP-switch number 1 must be on, refer to the installation sheet of the product.
- DIP-switch number 2 must be off, refer to the installation sheet of the product.
- The forwarding tables must be reset by pressing the status button for at least 20 seconds (see Section 6.5.1).

Figure 89 shows the proper DIP-switch settings for repeater mode, assuming all other DIP switches remain in the factory default position. The series "C" L-IP models do not have DIP switches.

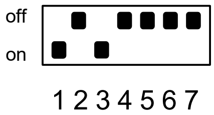


Figure 89: ON-OFF: DIP-switch settings for repeater mode.

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 L-IP 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 8.4 on how to configure the device to use multi-cast.

8.1.4 Smart Switch Mode with No Subnet Broadcast Flooding

This operating is the same as the smart switch mode from Section 8.1.2 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 either with a router shape or with an L-IP LonMaker shape provided by LOYTEC. Please download the L-IP LonMaker shapes from our website at www.loytec.com.

Figure 90 shows the proper DIP switch settings for smart switch mode without subnet broadcast flooding, assuming all other DIP switches remain in the factory default position. The series "C" L-IP models do not have DIP switches.

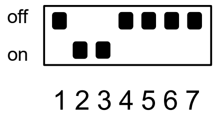


Figure 90: OFF-ON: DIP-switch settings for smart switch mode without subnet broadcast flooding.

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 L-IP 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 8.4 on how to configure the device to use multi-cast.

8.2 CEA-852 Operating Modes

Every logical IP-852 channel requires one configuration server that manages all CEA-852 devices (L-INX, L-IP, LOYTEC NIC852, *i*.LON 1000, *i*.LON 600, LonMaker, etc.) on this channel. A simple network from Figure 91 uses two L-IP devices to connect two CEA-709 channels. One L-IP acts as router and as configuration server for this IP channel. The second L-IP acts as a normal CEA-709 to IP router.

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-IP contains an embedded configuration server and can therefore replace the PC.

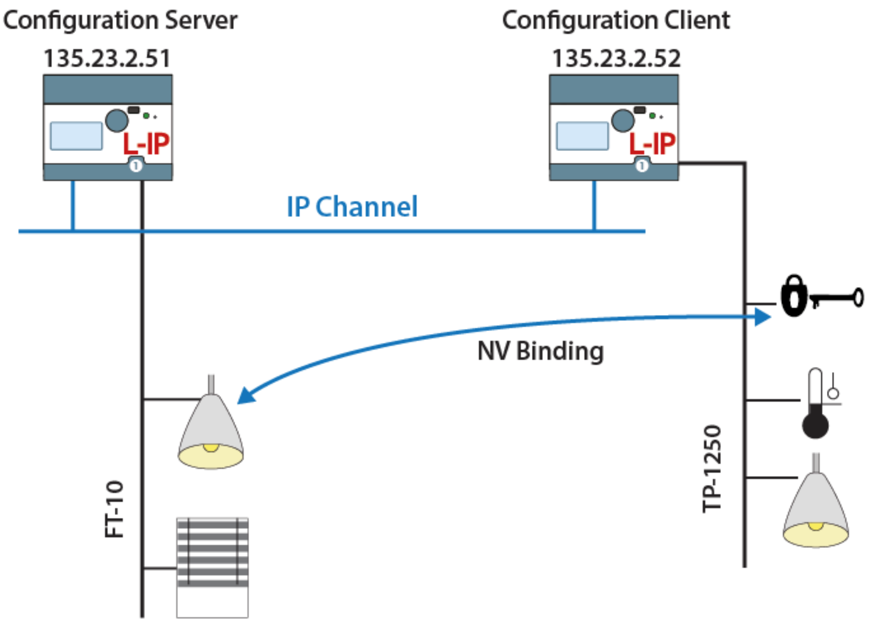


Figure 91: IP channel that consists of two IP devices. The left L-IP with IP address 135.23.2.51 acts as router and as a configuration server for this IP channel. It manages both IP devices 135.23.2.51 and 135.23.2.52.

8.2.1 CEA-852 Device

Every L-IP 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 logical IP-852 channel it needs to have the following parameters:

- IP address/netmask/gateway (either via DHCP or manual entry), see Section 7.3.3
- Auto-NAT or manual NAT address if used behind a firewall/NAT router, see Section 7.3.12
- MD5 secret if authentication is required, see Section 7.3.12

Please consult Sections 7.3.3 and 7.3.12 on how to setup a CEA-852 device.

8.2.2 CEA-852 Configuration Server

Any CEA-709 device that is directly connected to an IP channel (Intranet, Internet) must be managed by a so-called configuration server (see Figure 92). 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.

The L-IP can be used together with the PC based i.LON Configuration Server utility or with the built-in configuration server. The built-in configuration server can be enabled in the CEA-852 server configuration menu in Section 7.3.14. 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 7.6.1
- NAT address if used behind a firewall/NAT router, see Section 7.3.12
- MD5 secret if authentication is required, see Section 7.3.12
- Enable the configuration server, see Section 7.3.14 (server LED lights up green)
- A list of IP-852 channel members, see Section 7.3.15.

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

There are two different scenarios how a device can join an IP-852 channel. Either the device has a valid IP address of a configuration server stored and contacts the configuration server direct or the configuration server has a list of the IP addresses of the devices and the configuration server contacts the device.

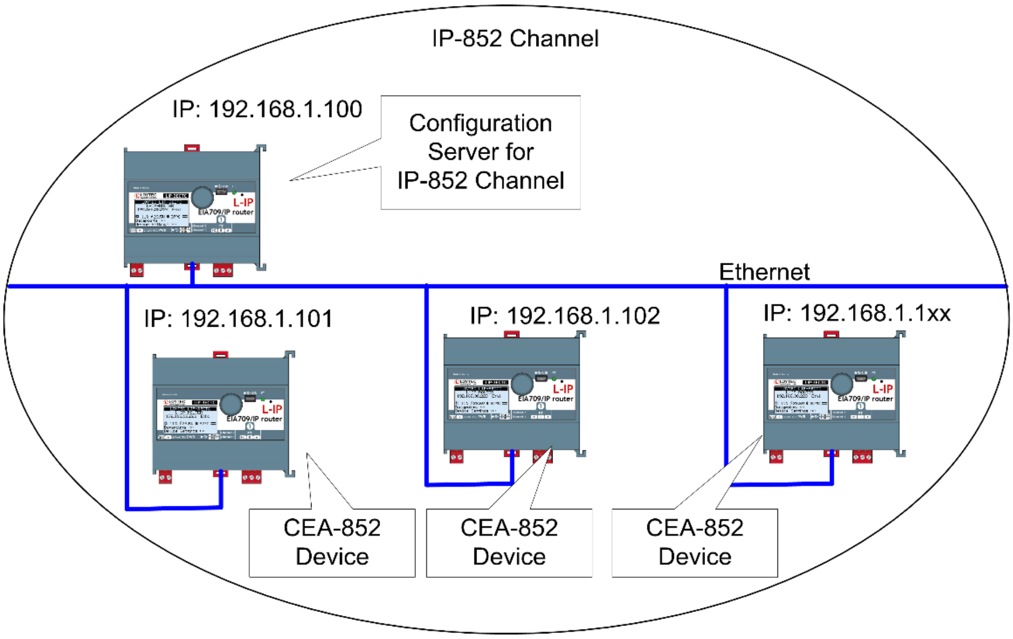


Figure 92: The configuration server manages the devices on an IP-852 channel.

8.2.2.1 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 7.3.3
- Auto-NAT or manual NAT address if used behind a firewall/NAT router, see Section 7.3.12
- MD5 secret if authentication is required, see Section 7.3.12

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

8.2.2.2 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 7.3.3
- Auto-NAT or manual NAT address if used behind a firewall/NAT router, see Section 7.3.12
- MD5 secret if authentication is required, see Section 7.3.12
- Configuration server IP address and port number, see Section 7.3.12

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.

8.2.2.3 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 7.3.15). 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 8.3.2). 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.

8.2.2.4 Using the i.LON Configuration Server

The L-IP can be used with the i.LON Configuration Server utility. If the L-IPs are communicating across firewalls/NAT routers or if MD5 authentication is enabled on the L-IP, the i.LON Configuration Server utility version 2.00.24 and up must be used. The configuration server channel mode must be set to “Standard CEA-852”. Note that this mode does not support i.LON 1000 and LNS 3.0 VNI. However, LNS 3.0 applications (e.g. LonMaker) can use MD5 authentication and the NAT feature in standard mode when using the LOYTEC NIC852 legacy driver.

The i.LON configuration server utility version 2.00.24 and up also supports the extended NAT mode (see Section 8.3.2) to add more than one device behind a NAT router. The L-IP can be used with the i.LON configuration server in this mode. Note, that the i.LON configuration server channel mode needs to be manually switched to “Extended NAT” mode.

Note: *If the L-IP is used behind a NAT router with the i.LON configuration server, the Auto-NAT feature must be disabled and the correct NAT address must be entered manually.*

8.3 Firewall and NAT Router Configuration

The L-IP can be used behind a firewall and/or NAT (Network Address Translation) router as shown in Figure 93. 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 8.2.2.3 on compatibility with the *i*.LON 600.

8.3.1 Automatic NAT Configuration

In order to use the L-IP behind a firewall the public NAT address and the local IP address must be set in the IP configuration menu (see Section 7.3.3). By default the NAT address is determined automatically when adding the L-IP 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-IP (192.168.1.100 in Figure 93). In summary we can say the following parameters must be set in order to operate an L-IP 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.

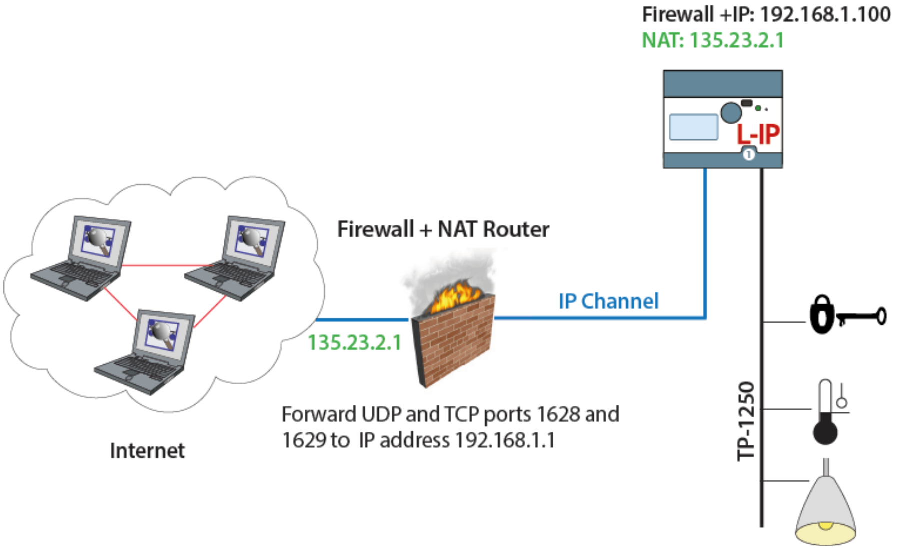

Firewall +IP: 192.168.1.100
NAT: 135.23.2.1
L-IP
Firewall + NAT Router
IP Channel
135.23.2.1
Forward UDP and TCP ports 1628 and 1629 to IP address 192.168.1.1
Internet
TP-1250

Figure 93: Operating an L-IP behind a NAT router and firewall.

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

8.3.2 Multiple L-IPs 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-IP configuration server is to use the extended NAT mode. This mode requires that all devices support this feature. Currently these are L-IP, *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 8.3.3 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-IP, change the client port in the CEA-852 device configuration menu. Figure 94 shows an example configuration for three L-IP 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-IP which has port-forwarding to 1628 and 1629. In the example in Figure 94, the L-IP with private address 192.168.1.100 also acts as a configuration server.

If the CS is activated on a L-IP behind a NAT router, the NAT router must have a fixed public IP address. The L-IP 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 7.2.4).

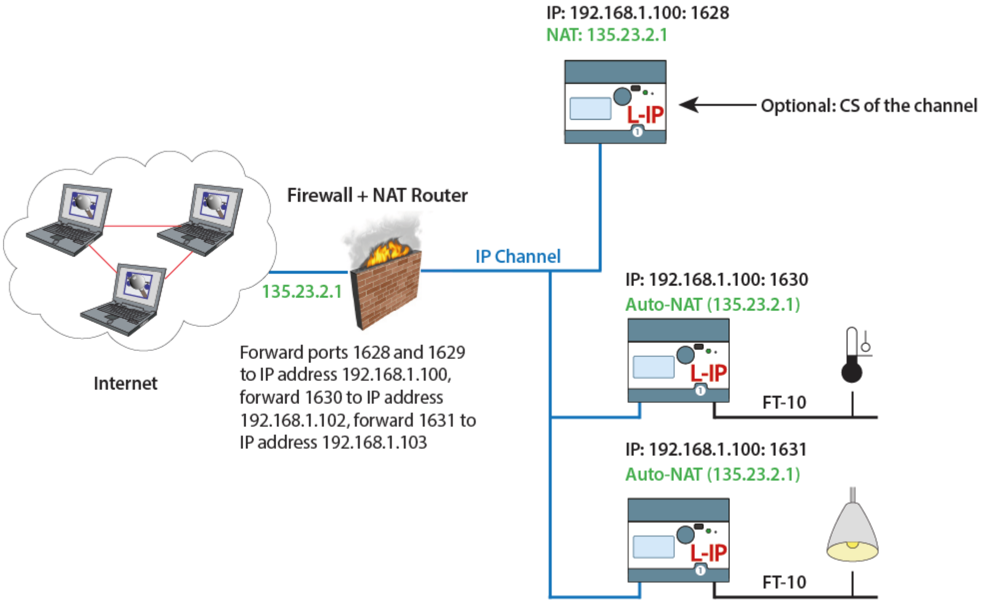
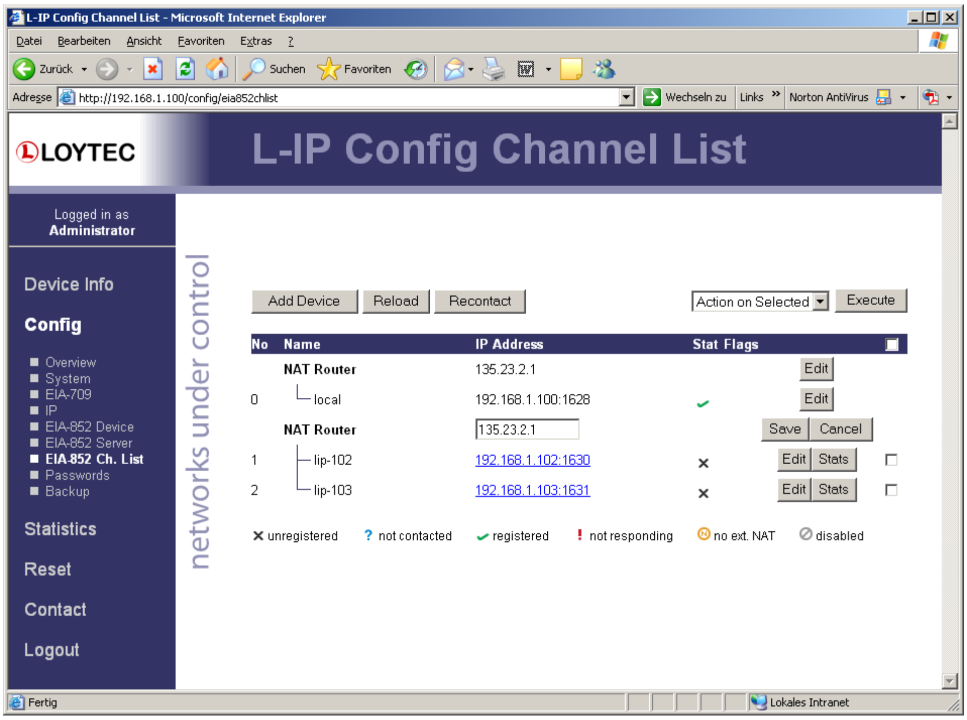


Figure 94 Multiple L-IP devices behind a NAT: Extended NAT Mode.

After the NAT router has been configured with the port-forwardings and the CS has been turned on, the channel members can be added. This can be done either on the console UI or 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 94 through the Web UI is depicted in Figure 95. To remove a device from a NAT router but not delete it, select it and choose **Remove from NAT** as the action.



L-IP Config Channel List

No	Name	IP Address	Stat	Flags	☐
	NAT Router	135.23.2.1		Edit	
0	└local	192.168.1.100:1628	✓	Edit	
	NAT Router	135.23.2.1		Save Cancel	
1	└lip-102	192.168.1.102:1630	×	Edit Stats	☐
2	└lip-103	192.168.1.103:1631	×	Edit Stats	☐

× unregistered ? not contacted ✓ registered ! not responding ⊙ no ext. NAT ⊘ disabled

Figure 95: Adding a member with extended NAT Mode on the Web UI.

8.3.3 Multiple L-IPs behind a NAT: Classic Method

If more than one L-IP 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 96.

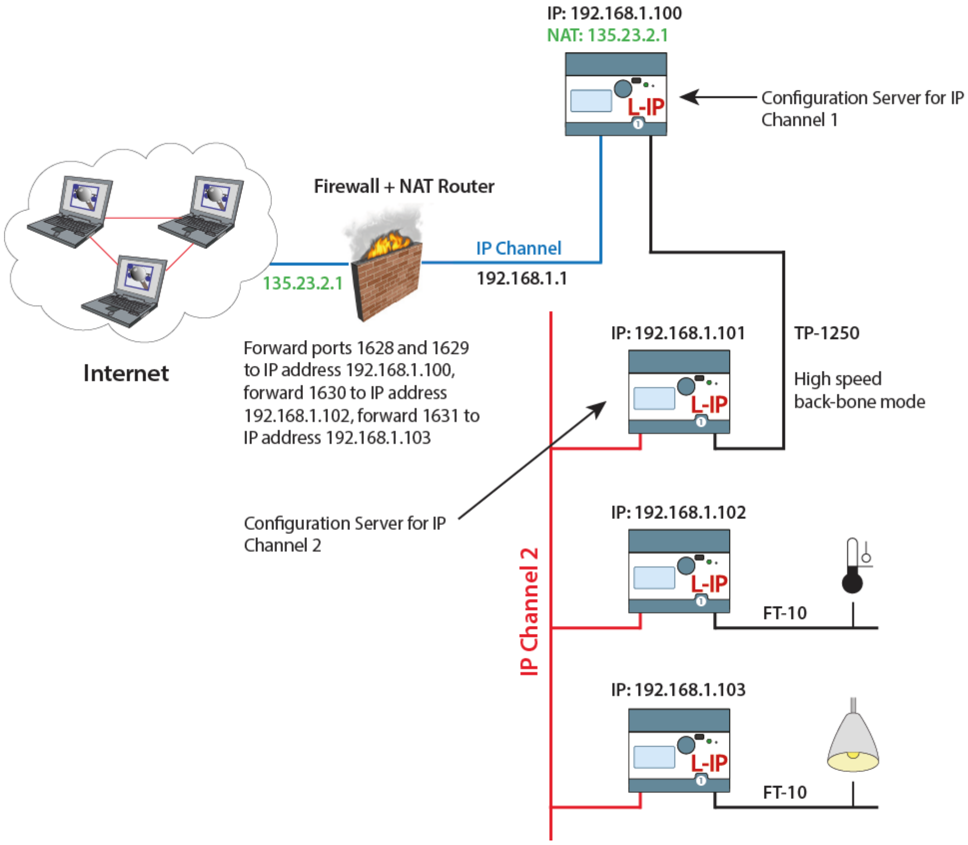

IP: 192.168.1.100
NAT: 135.23.2.1
L-IP
Configuration Server for IP Channel 1
Firewall + NAT Router
IP Channel
135.23.2.1
192.168.1.1
Internet
Forward ports 1628 and 1629 to IP address 192.168.1.100, forward 1630 to IP address 192.168.1.102, forward 1631 to IP address 192.168.1.103
IP: 192.168.1.101
TP-1250
High speed back-bone mode
Configuration Server for IP Channel 2
IP: 192.168.1.102
FT-10
IP Channel 2
IP: 192.168.1.103
FT-10

Figure 96: Application that uses multiple L-IP devices behind a NAT router firewall.

The L-IP with IP address 192.168.1.100 is member of IP Channel 1 and can be accessed through the Internet. The L-IP 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-IP devices on the different channels. In the example in Figure 96 the L-IP with address 192.168.1.100 acts as the configuration server for IP Channel 1 and the L-IP with IP address 192.168.1.101 acts as the configuration server for IP Channel 2.

8.4 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-IP supports both unicast and multi-cast delivery of CNIP data packets. Using multi-cast is recommended when using L-IPs in the Smart Switch Mode. For those L-IPs 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. All L-IPs 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 L-IP uses a hybrid scheme and sends unicast to those devices, which are not configured for multi-cast. Note, that the L-IP determines automatically, when to switch to the multi-cast mode depending 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 L-IP utilizes the multi-cast feature to send to other devices, contact the Extended CEA-852 device statistics in the statistics menu (Section 7.2). 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 7.2) counts the number of multicast packets transmitted to the group. If this item remains zero, no multi-cast is used by the L-IP.

8.5 Internet Timing Aspects

If the L-IP 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 6 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 6: 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 6.

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.

8.5.1 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 7.3.14 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.

8.5.2 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.

8.5.3 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.

If enabled or disabled, out-of-sequence packets are never sent to the CEA-709 channel. Please refer to Section 7.3.12 on how to enable or disable escrowing.

8.5.4 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 7.3.12 and Section 7.3.14 on how to enable the SNTP server.

8.6 Advanced Topics

8.6.1 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 7.3.12 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.

8.6.2 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 7.3.12 and 7.3.14 for details.

8.6.3 DHCP

When using DHCP the configuration server must always get the same IP address assigned. Client devices can get different IP addresses assigned as long as the “Roaming Member” function is activated on the configuration server. Do not use DHCP with dynamic IP addresses in applications with NAT routers.

8.6.4 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.

8.7 Network Buffers

The L-IP can handle packets from the network with a maximum length of 256 bytes. There is no explicit limit in the network buffer counts.

9 The L-IP in a Network

The L-IP is based on LOYTEC’s powerful L-Core™ and L-Chip™ technology. It is designed to be very robust and reliable in real-life applications. The L-IP either behaves completely transparent in a network or can be configured to behave like a configured CEA-709 router.

Before the L-IP can start routing CEA-709 packets over IP channels, the L-IP must be added to an IP-852 channel. Please refer to Section 8.2.2 on how to add the L-IP to an IP-852 channel.

9.1 L-IP Acts as a Standard CEA-709 Configured Router

Installing and operating the L-IP works like for a standard CEA-709 router, when used in the factory default state:

- Configured CEA-709 router,
- Bit-rate auto detection disabled and
- Backbone mode for TP-1250 ports disabled.

After adding the device to an IP-852 channel, a network management tool like LonMaker or NL-220 must be used to add and commission the L-IP as a configured router. We provide LonMaker shapes for the different operating modes of the L-IP. You can download those shapes from our website at http://www.loytec.com.

The multi-port L-IP contains multiple standard CEA-709 routers, one for each port, and an internal TP-1250 backbone. The internal TP-1250 is neither visible nor accessible from the outside and its sole task is to connect the individual routers. Figure 97 shows an example for the multi-port L-IP (LIP-33ECTB).

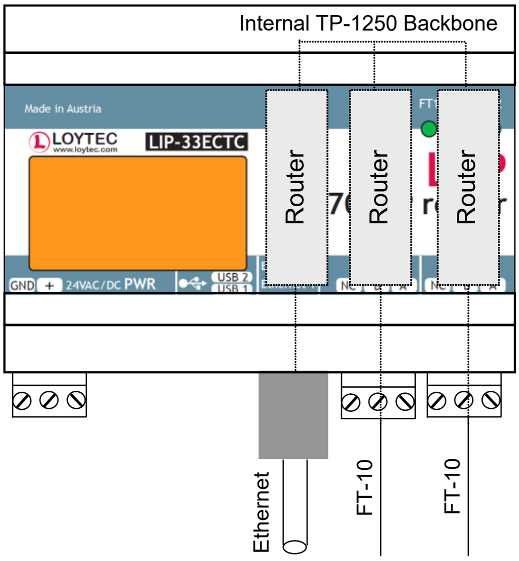


Figure 97: Internal structure of the multi-port L-IP in configured CEA-709 router mode.

Each router must be commissioned separately, reflecting the structure of the internal TP-1250 channel. The port LEDs of unconfigured routers are flashing green with a frequency of 1 Hz (once per second).

Pressing the status button longer than 2 seconds will allow you to cycle through the ports and select the port, which shall send out the “Service Pin Message” message: The port LED of the currently selected port will light up orange. After 2 seconds the next available port will be selected. When the status button is released the “Service Pin Message” is sent out on the currently selected port/router.

If an LNS-based installation tool (e.g. LonMaker) is used, the individual routers of the L-IP must be commissioned separately. Refer to application note AN003E “Using the L-IP with LNS-based Installation Tools” for more details.

9.2 L-IP Acts as a Smart Switch

Installation and operation is plug&play if used in the smart switch mode, which can be set with the DIP switches. Please refer to Section 8.1.2 to set the L-IP into smart switch mode. After connecting the network cables, the L-IP can be powered up and it will start its switching application. Before the L-IP starts routing packets it must be added to an IP-852 channel.

When using a standard binding tool (e.g. LonMaker), bindings between nodes connected to different ports can be done without considering the L-IP. Further, an L-IP can be added anywhere to an already configured network without reconfiguring the nodes in the network.

Due to the plug and play installation capability of the L-IP, it does not support any CEA-709 Router network management commands. However, it accepts all other standard network management commands (e.g. to set the channel parameters on every port).

9.3 L-IP Acts as an L-Switch

Existing installations using TP-1250 and/or FT-10 segments only can require routers between the network segments. In this case no IP-852 channel is required, nor are any IP settings required. The older LOYTEC L-Switch™ devices were used in such installations. Other manufacturers also provided LON routers (for example Echelon LonPoint™ routers).

The two-port L-IP can be configured as an L-Switch type device. In this mode, the IP-852 channel is disabled and the internal router acts as a Smart Switch™ or configured CEA-709 router between its TP-1250 and/or FT-10 ports. An example showing an LIP-33ECTC configured as an L-Switch type device is shown in Figure 98.

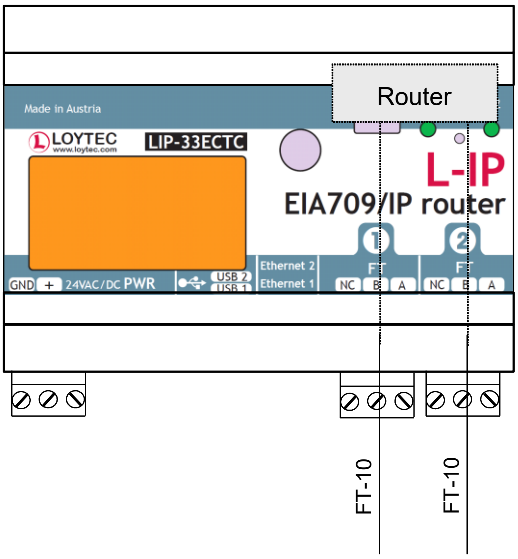


Figure 98: Internal structure of the two-port L-IP in configured as an L-Switch.

9.4 Using L-IP in LNS (LonMaker) Networks

We provide LonMaker shapes in order to add an L-IP to a LonMaker drawing. Please download the shapes from our homepage at http://www.loytec.com.

Detailed instructions on how to use the L-IP together with LNS based network management tools can be found in Section 15.

9.5 Using the L-IP as the Network Interface for LNS Applications

The L-IP can be used as a local or remote network interface for LNS based applications like LonMaker to access CEA-709 networks. Therefore the CEA-852 network interface must be enabled on the PC where the LNS application program is installed and the IP address of the PC must be added to the configuration server:

1. Add the IP address of the PC to the configuration server's list of devices (see Section 7.3.15).

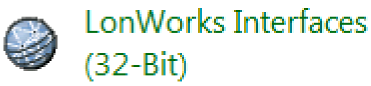


Figure 99: Icon for LonWorks Interfaces in Windows 7 Control Panel.

2. Select the LonWorks Interfaces utility program from your Control Panel and select the **IP-852** tab.

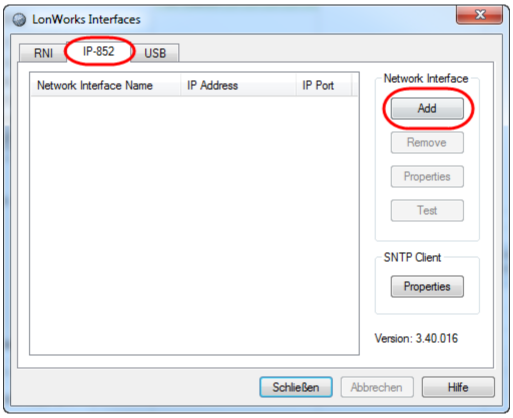
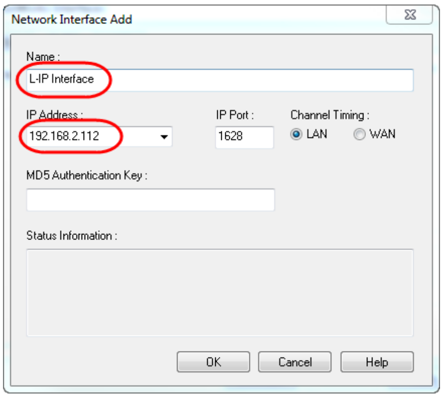


Figure 100: Add a new LNS IP interface to your PC.

3. Click on **Add**.



Name : L-IP Interface

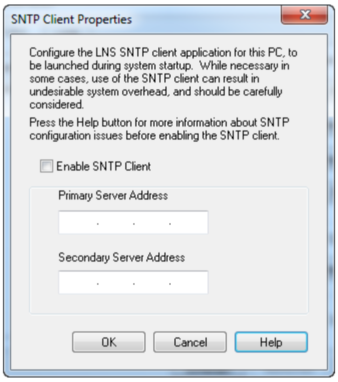
IP Address : 192.168.2.112

IP Port : 1628

Channel Timing : ● LAN ○ WAN

Figure 101: Give the new interface a name.

4. And specify a name for the interface in the Name field. The IP Address field shows the IP address of your PC. Leave the IP port at 1628. Leave the MD5 authentication key field empty. Click **OK**.



Configure the LNS SNTP client application for this PC, to be launched during system startup. While necessary in some cases, use of the SNTP client can result in undesirable system overhead, and should be carefully considered.

Press the Help button for more information about SNTP configuration issues before enabling the SNTP client.

☐ Enable SNTP Client

Figure 102: Disable the SNTP client if you have a local NTP client installed on your PC.

5. Click on **Properties** in the SNTP Client section. Do not enable the SNTP Client if the network interface is used in a local network like an Intranet. If the network interface is also accessed over a large network like the Internet one should specify an address for a Time Server and enable the SNTP Client. If you already have an NTP client installed on your PC, which synchronizes your PC clock to an NTP timer

server, you must not enable the SNTP Client otherwise it will compete with the NTP client already installed on your PC.

6. You can now start the LNS application and select the “L-IP Interface” as your interface to the CEA-709 network.

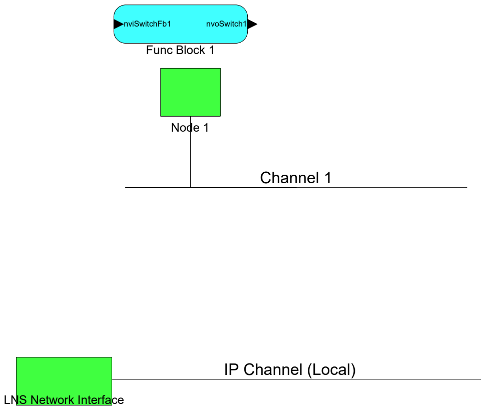


Figure 103: Move the LNS Network Interface to the newly created IP Channel.

7. If the L-IP is used as a CEA-709 configured router one should add the L-IP in the LonMaker drawing. Create a new Channel with channel type IP-10L in an Intranet or IP-10W in an Internet environment. Move the LNS Network Interface to this newly created IP channel as shown in Figure 103 by selecting the LNS Network Interface and choosing “Change Channel” from the context menu.

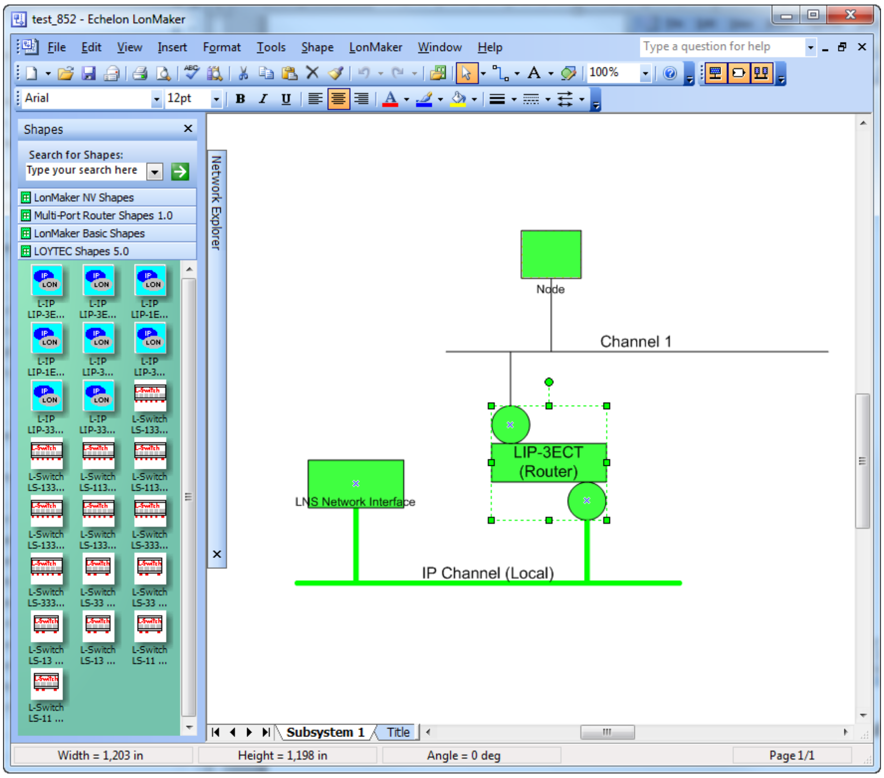


Figure 104: Drag the L-IP (Router) shape onto the drawing area and commission the device.

8. Now drag the L-IP (Router) shape from the “LoytecShapes” stencil onto the drawing area. Choose the existing channel “IP Channel” for the first router port and the existing channel “Channel 1” for the second port. Finally you must commission the

new L-IP router. LonMaker can now use the L-IP as a local or remote network interface that connects directly to the Ethernet network as shown in Figure 104.

9.6 Remote LPA Operation

The L-IP supports remote LPA access. This means that a CEA-709 protocol analyzer connected to the Ethernet network can connect to the L-IP and record all packets on the CEA-709 channel (FT-10). Our LPA-IP supports this sophisticated feature. The functionality is shown in Figure 105.

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-IP with IP address 192.168.1.210 and display all packets on the FT-10 channel connected to the L-IP 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.

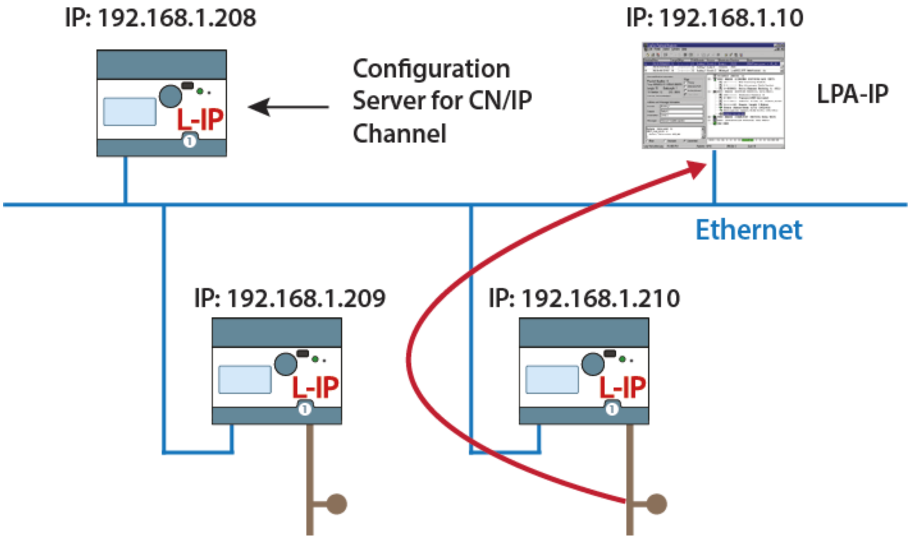


Figure 105: Remote LPA principle.

10 L-IP Redundant

10.1 Redundancy and Fault Detection in CEA-709.1 Networks

10.1.1 Reasons for Communication Failures

Figure 106 shows typical reasons for communication failures in CEA-709 networks:

1. **Broken connection on the backbone:** The router is not connected to the backbone anymore. Therefore the nodes are unable to communicate with nodes in other segments or the building management system (A).

2. **Router device failure:** The router device fails due to power failure or device failure. Again the nodes are unable to communicate with nodes in other segments or the building management system across the router (A,B).

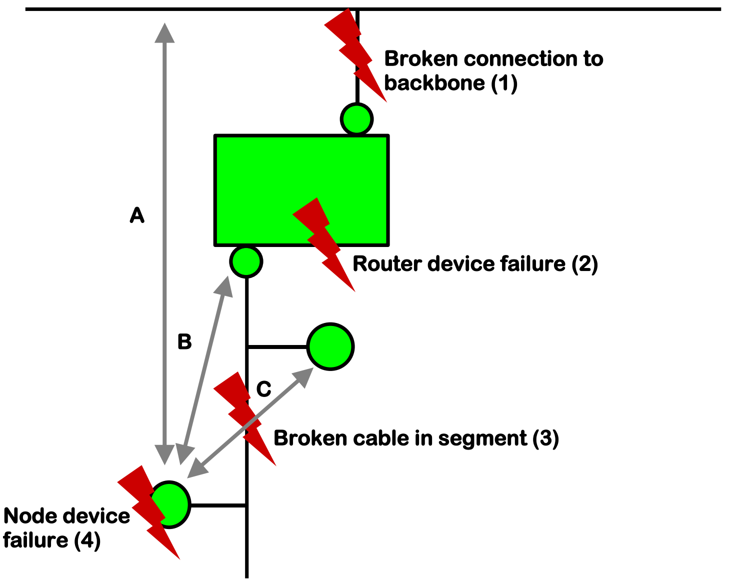

Broken connection to backbone (1)
A
Router device failure (2)
B
C
Broken cable in segment (3)
Node device failure (4)

Figure 106: Typical reasons communication failures in CEA-709 networks.

3. **Broken cable in the segment:** The nodes cannot communicate across the point of fracture. Thus, nodes behind the point of fracture cannot communicate with nodes before the point of fracture (C) and with the router (B) and therefore with nodes in other segments (A).

4. **Node device failure:** A node fails due to power failure or device failure. As a result the node cannot perform its function anymore and cannot be reached by its communication partners (A,B,C).

10.1.2 Conventional Strategies for Redundancy

Although CEA-709.1 allows introducing redundancy by allowing for a pair of conventional CEA-709.1 routers (twin routers) to be identically configured and connected between the same two channels, this configuration increases the traffic between those two channels two-fold. The built-in duplicate detection mechanism in CEA-709.1 discards the duplicate packets at each receiving node. However, the extra traffic could tax available network bandwidth significantly and create other problems. Further, this addresses only some of the above faults: “2. Router device failure” and to a limited extend “1. Broken connection on the backbone”[2].

Using CEA-709/IP Routers with a redundant IP infrastructure allows building a redundant backbone (“1. Broken connection on the backbone”). But still the connection to the router (switch, cable) remains a single point of failure.

10.2 L-IP Redundant Operating Modes

10.2.1 Bus Loop Monitoring

To achieve redundancy against “3. Broken cable in the segment” (see Section 10.1.1) the L-IP allows building a ring structure by connecting both ends of the bus cable to the L-IP Redundant (see Figure 107).

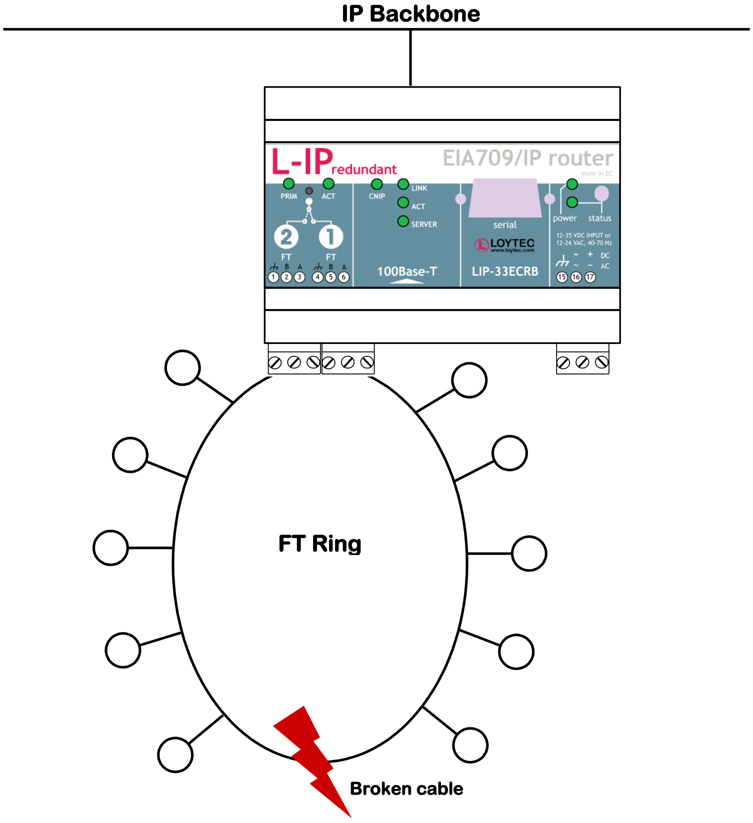


Figure 107: L-IP Redundant with Bus Loop Monitoring.

Now the L-IP Redundant is able to detect a cable fracture by permanently comparing the traffic on both sides of the bus: If the L-IP Redundant sees different traffic on its two terminals, the cable is deemed to be broken. In this case it starts to duplicate the traffic from

[2] Assuming a redundant backbone.

loop port 1 to loop port 2 and vice versa. Further an alarm is issued (see Sections 10.5.5 and 10.6.3). Once messages are received on both sides again the ring is considered closed and the cable fracture is deemed gone.

The L-IP Redundant is shipped with bus loop monitoring enabled. If bus loop monitoring is not desired it must be switched off to avoid a permanent “Ring open” alarm. Bus loop monitoring parameters can be configured using the L-IP Redundant plug-in (see Section 10.5.7) or the web interface (see Section 10.6.5).

The current bus loop monitoring state can be determined via network variables (see Section 10.7), in the L-IP Redundant plug-in (see Section 10.5.3), and in the web interface (see Section 10.6.1).

Important: ***To guarantee proper function of the bus loop monitoring algorithm it is required to keep average bandwidth utilization on the monitored segment below 50%! Bandwidth utilization can be monitored using the LOYTEC LPA or the built in diagnostic functions (see Sections 10.5.4 and 10.6.1).***

10.2.2 Router Redundancy

If IP network redundancy is available, full redundancy on the IP-Channel (Backbone) can be achieved with two devices installed in parallel (see Figure 108). In this case router redundancy is ensured as well by mutual monitoring of paired L-IP Redundant routers. Since two L-IP Redundant routers are used in this scenario, this use case is sometimes also referred to as “twin router mode”.

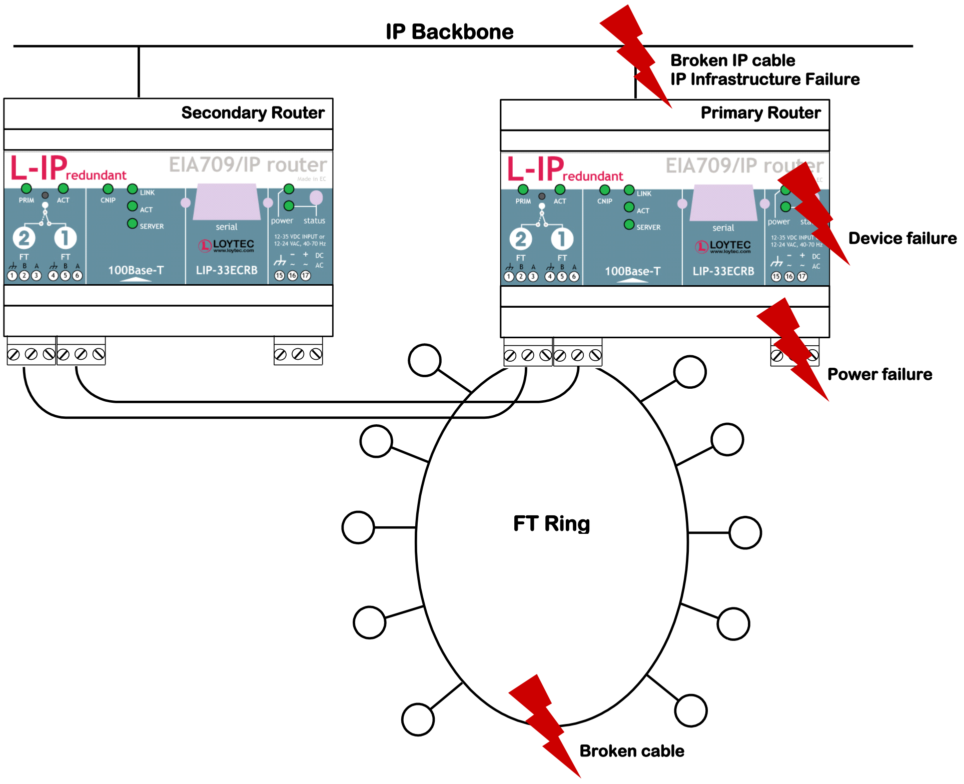


Figure 108: Router Redundancy with two paired L-IP Redundant routers

During power-up the two L-IP Redundant routers automatically negotiate, which one becomes the active router (primary router) and which one the inactive standby router (secondary router)[3]. The active router forwards packets, performs bus loop monitoring, and has node monitoring enabled, while the inactive devices has all these functions disabled. After this initial startup-phase the devices periodically monitor each other on the CEA-709 and on the CEA-852 (IP) side. If the secondary router no longer reaches the primary router on either side it becomes active and issues an alarm, if the primary router no longer reaches the secondary router just an alarm is issued.

Further, the secondary device, even though it is inactive and does not forward packets, it counts the number it *would* forward based on the packets it receives and on its routing tables. Now the two devices periodically compare these numbers and if these numbers significantly differ over multiple monitoring intervals an alarm is issued. This algorithm ensures that the routing tables of both devices are consistent and the secondary router is correctly configured and able to take over if the primary device fails. Further, if the primary device does not forward any packets in one direction, while the secondary would forward packets the secondary devices takes over and the primary device becomes inactive.

Router redundancy can be used with or without bus loop monitoring enabled (see Section 10.2.1).

To enable router redundancy both routers must be commissioned and added to the same IP-852 channel. Further, the two routers must be linked by binding certain network variables, which are used for communication between the two paired L-IP Redundant routers. Please see Section 10.4.3.2 on how to configure the L-IP Redundant for router redundancy.

Redundant router monitoring parameters can be configured using the L-IP Redundant plug-in (see Section 10.5.7) or the web interface (see Section 10.6.5).

The current router state can be determined via network variables (see Section 10.7), in the L-IP Redundant plug-in (see Section 10.5.3), and in the web interface (see Section 10.6.1).

10.2.3 Device and Network Monitoring

In addition to its redundancy functions the L-IP Redundant performs a couple of monitoring tasks. First a couple of channel quality parameters (e.g. bandwidth utilization, CRC error rate, etc.) are permanently monitored and their current values are provided as network variable (see Section 10.7), in the L-IP Redundant plug-in (see Section 10.5.4), and in the web interface (see Section 10.6.1).

Secondly the L-IP Redundant can be used to monitor other nodes in the network. For this purpose a list of nodes can be entered using the L-IP Redundant plug-in (see Section 10.5.6) or the web interface (see Section 10.6.4). If node monitoring is enabled, the L-IP Redundant periodically pings the nodes in this list using a Query Status network diagnostic request. If a node is not reachable or (soft) offline an alarm is issued. Further, the state of each node can be determined via a network variable (see Section 10.7), in the L-IP Redundant plug-in (see Section 10.5.3), and in the web interface (see Section 10.6.1). In addition the web interface shows detailed statistic information for each node (e.g. number of CRC errors).

If bus loop monitoring is enabled (see Section 10.2.1) the L-IP Redundant also determines from which loop port each node is reachable (both ports, loop port 1 only, or loop port 2 only). Thus, if the nodes were entered in the order they are connected to the bus this allows the L-IP Redundant to determine the exact location of a cable fracture by finding the last node reachable from port 1 and the last one reaching from port 2. This information is also provided to the user via network variables, in the L-IP Redundant plug-in, and in the web interface.

[3] The primary router is the device with the higher VID1.

10.3 The L-IP Redundant in a Network

As shown in Figure 109 the L-IP Redundant internally consists of a standard CEA-709 router and a diagnostic node. The router routes packets between the CEA-709 and the IP-852 channels, while the diagnostic node performs monitoring tasks (e.g. node monitoring) and offers network variables to show the results of these diagnostics.

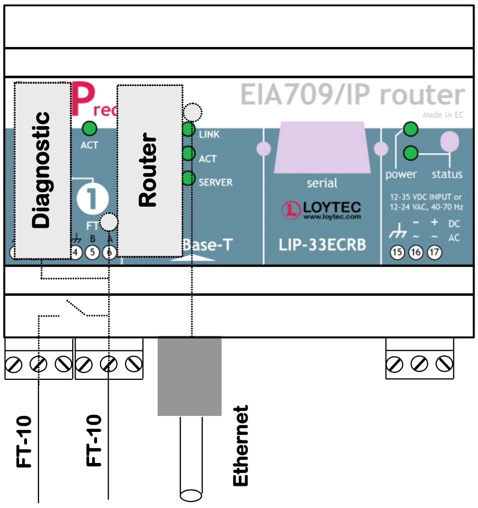


Figure 109: Internal structure of the L-IP Redundant

The router in the L-IP Redundant can only be used as Configured Router and thus requires to be commissioned with a network management tool (e.g. LonMaker) like any other router. Smart Switch Mode, Repeater Mode and Bridge Mode are not supported.

Since the diagnostic node resides on the CEA-709 side of the router, the router must be commissioned before the diagnostic node. To configure the diagnostic node with an LNS based network management tool, LOYTEC provides the "L-IP Redundant Plug-In" (see Section 10.5).

10.4 Installation

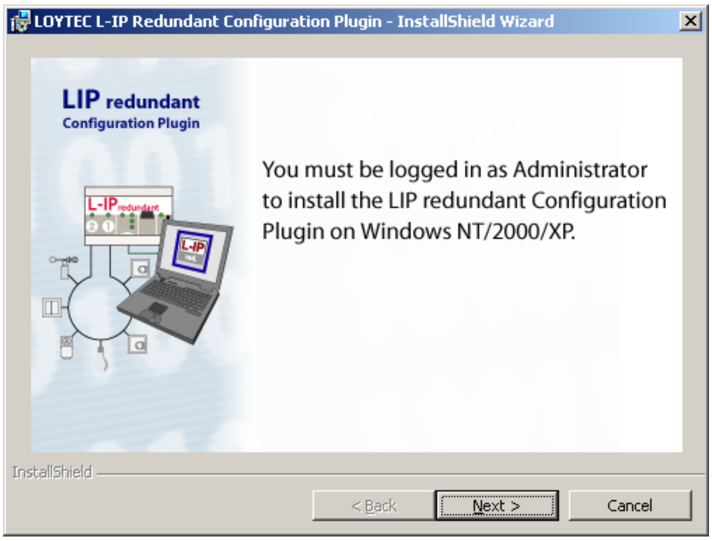
10.4.1 Installing the L-IP Redundant Plug-In

The L-IP Redundant Plug-In is used to configure the L-IP Redundant node monitoring (see Section 10.2.3), configure the various parameters influencing the behavior of the L-IP Redundant, download the L-IP Redundant Alarm Log, and view the current state of the L-IP Redundant. This configuration utility is installed as a plug-in tool for all LNS based network management tools.

System requirements:

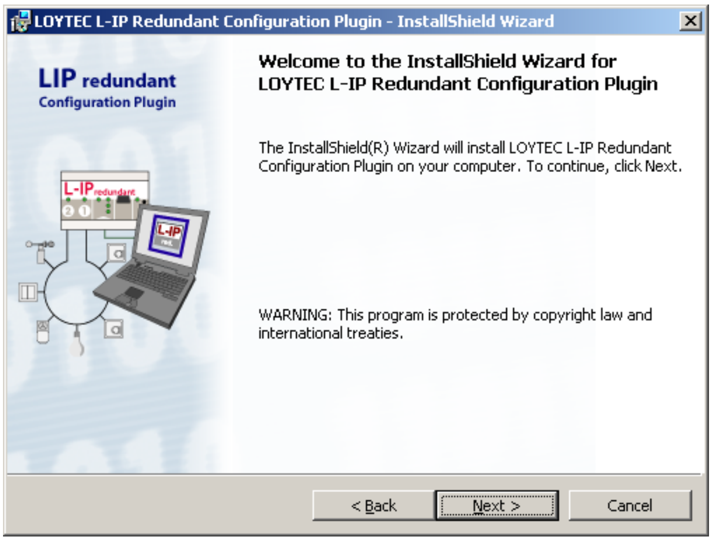
- LNS 3, Service Pack 7 or higher
- Windows XP, Windows Vista or Windows 7.

The L-IP Redundant Plug-In can be downloaded from the LOYTEC website http://www.loytec.com. To install the configuration utility double click on Setup and follow the installation steps.


LOYTEC L-IP Redundant Configuration Plugin - InstallShield Wizard

You must be logged in as Administrator to install the LIP redundant Configuration Plugin on Windows NT/2000/XP.

Figure 110: Be sure to be logged in as Administrator on Windows 2000/XP.

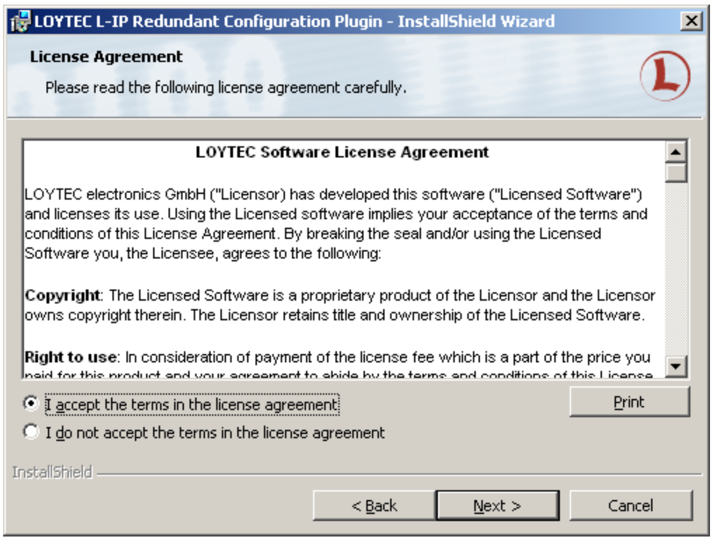

LOYTEC L-IP Redundant Configuration Plugin - InstallShield Wizard

Welcome to the InstallShield Wizard for LOYTEC L-IP Redundant Configuration Plugin

The InstallShield(R) Wizard will install LOYTEC L-IP Redundant Configuration Plugin on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Figure 111: L-IP Redundant Plug-In welcome screen.


LOYTEC L-IP Redundant Configuration Plugin - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

LOYTEC Software License Agreement

LOYTEC electronics GmbH ("Licensor) has developed this software ("Licensed Software") and licenses its use. Using the Licensed software implies your acceptance of the terms and conditions of this License Agreement. By breaking the seal and/or using the Licensed Software you, the Licensee, agrees to the following:

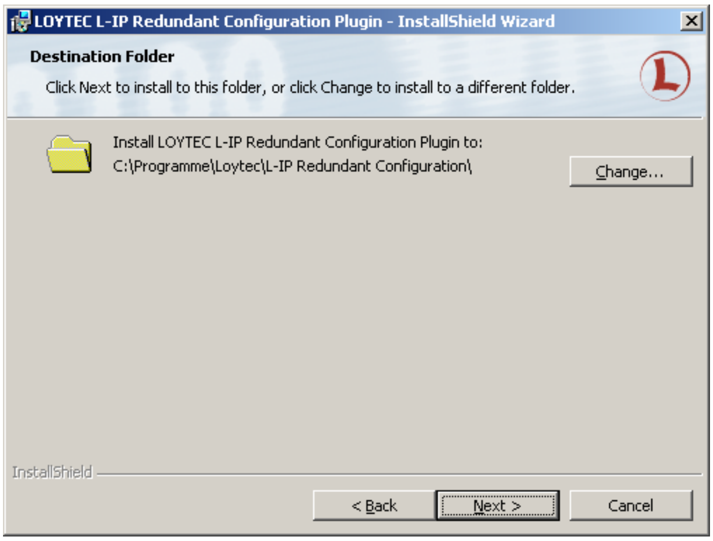
Copyright: The Licensed Software is a proprietary product of the Licensor and the Licensor owns copyright therein. The Licensor retains title and ownership of the Licensed Software.

Right to use: In consideration of payment of the license fee which is a part of the price you paid for this product and your agreement to abide by the terms and conditions of this License

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Figure 112: You have to agree to the Software License Agreement.



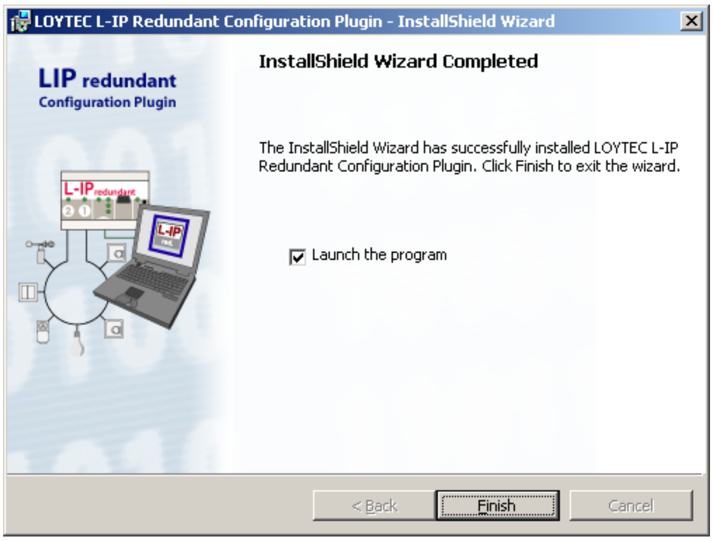
LOYTEC L-IP Redundant Configuration Plugin - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install LOYTEC L-IP Redundant Configuration Plugin to:
C:\Programme\Loytec\L-IP Redundant Configuration\

Figure 113: Choose the destination directory.



LOYTEC L-IP Redundant Configuration Plugin - InstallShield Wizard

InstallShield Wizard Completed

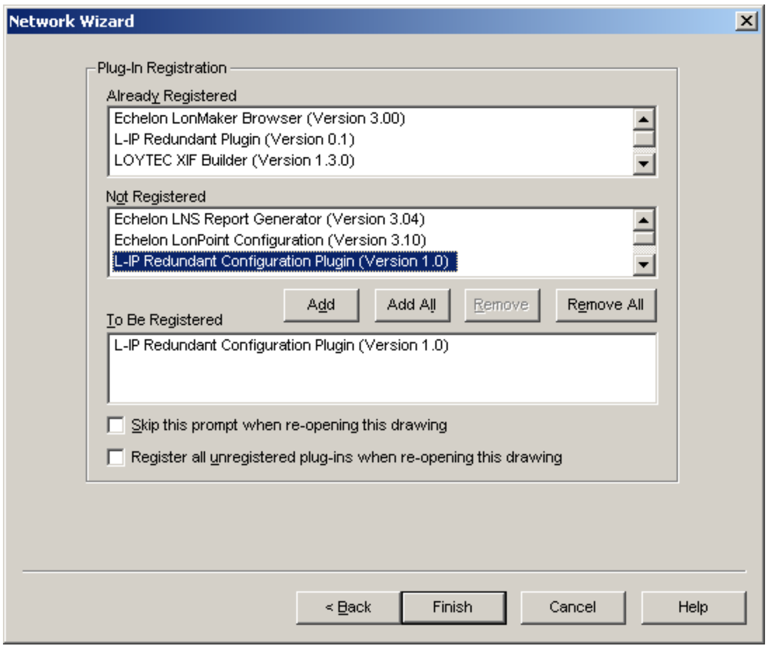
The InstallShield Wizard has successfully installed LOYTEC L-IP Redundant Configuration Plugin. Click Finish to exit the wizard.

☑ Launch the program

Figure 114: The Plug-In has been successfully installed.

10.4.2 Registering the L-IP Redundant Plug-In

After successfully installing the L-IP Redundant Plug-In the program must be registered as a plug-in in your LNS based network management tool. In the following section the process is described for LonMaker for Windows 3.1. Refer to the documentation of your network management tool on how to register a plug-in.


Network Wizard

Plug-In Registration

Already Registered
Echelon LonMaker Browser (Version 3.00)
L-IP Redundant Plugin (Version 0.1)
LOYTEC XIF Builder (Version 1.3.0)

Not Registered
Echelon LNS Report Generator (Version 3.04)
Echelon LonPoint Configuration (Version 3.10)
L-IP Redundant Configuration Plugin (Version 1.0)

To Be Registered
L-IP Redundant Configuration Plugin (Version 1.0)

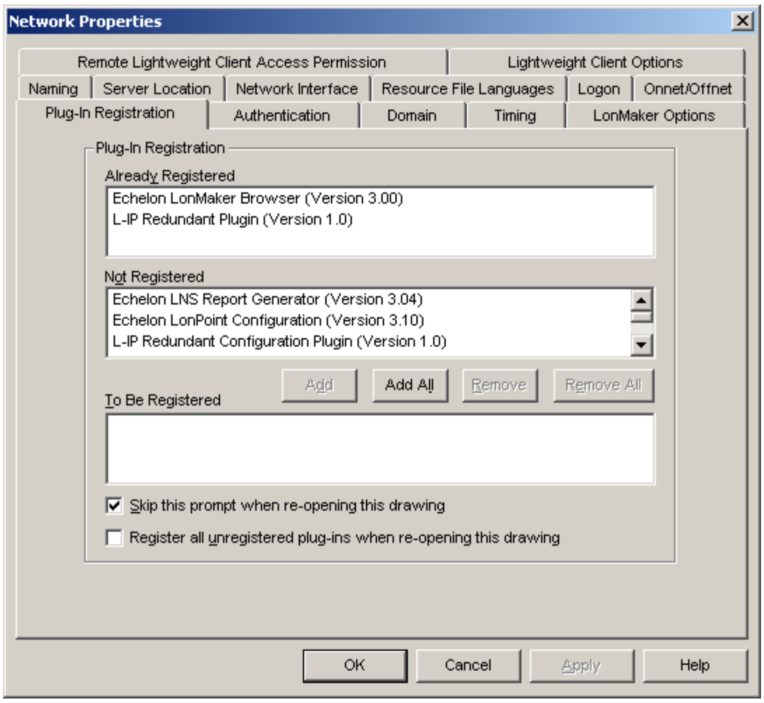
☐ Skip this prompt when re-opening this drawing
☐ Register all unregistered plug-ins when re-opening this drawing

Figure 115: Select the Plug-in to be registered and click **Add**.

Open LonMaker and create a new network. When the “Plug-in Registration” dialog window pops up select the **L-IP Redundant Configuration Plug-In** from the list of “Not Registered Plug-Ins” (see Figure 115). Click “Add” and “Finish” to register the plug-in. Device templates for the L-IP Redundant diagnostic node are added automatically and XIF files are copied into the LNS import directory.

Note: *If you are using multiple databases (projects) make sure you have registered the plug-in in each project.*

Under LonMaker => Network Properties => Plug-In Registration make sure that the **L-IP Redundant Configuration Plug-In** shows up under “Already Registered”.


Network Properties

Plug-In Registration

Already Registered
Echelon LonMaker Browser (Version 3.00)
L-IP Redundant Plugin (Version 1.0)

Not Registered
Echelon LNS Report Generator (Version 3.04)
Echelon LonPoint Configuration (Version 3.10)
L-IP Redundant Configuration Plugin (Version 1.0)

To Be Registered

☑ Skip this prompt when re-opening this drawing
☐ Register all unregistered plug-ins when re-opening this drawing

Figure 116: Double check that the L-IP Redundant Configuration Plug-In is properly registered

10.4.3 Adding the L-IP Redundant

The L-IP Redundant can be used standalone or with router redundancy. Depending on which operation scenario is selected, different steps have to be taken to add your L-IP Redundant router(s) to your network.

10.4.3.1 L-IP Redundant Standalone

For operating the L-IP Redundant in standalone mode (see Figure 107), the following steps have to be performed:

- Add a single router shape. Connect it to an IP-Channel on one side and to a FT-10 Channel on the other side of the router.

- Add one L-IP Redundant built-in diagnostic node "L-IP Redundant Diagnostic FT-10" device shapes on the FT-10 channel. The corresponding device template will be installed with the L-IP Redundant Plug-In (see Section 10.4.1).

- To get a service pin message for commissioning the diagnostic node, press the Status button on the L-IP Redundant (see Section 6.5) or use the **Send Service Pin Msg** button in the corresponding section of the Device Information Page in the Web interface (see Section 7.1).

If using LonMaker for Windows the resulting drawing should look like shown in Figure 117.

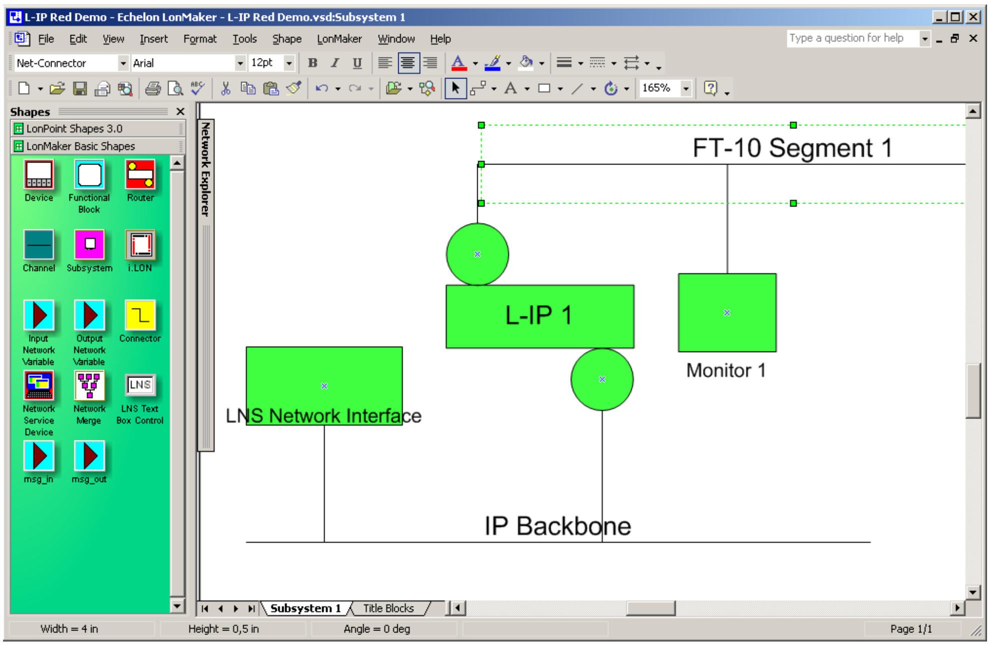


Figure 117: A single L-IP Redundant device configured for standalone operation.

Be sure to commission the router and the diagnostic node. Once they were successfully commissioned, the PRIM LED on the device should be green.

10.4.3.2 L-IP Redundant with Router Redundancy

For operating the L-IP Redundant in twin router mode (router redundancy, see Figure 108), the following steps have to be performed:

- Add two router shapes. Connect both to the same IP-Channel on one side and to the same FT-10 Channel on the other side of the router.

- Add two L-IP Redundant built-in diagnostic node “L-IP Redundant Diagnostic FT-10” device shapes on the FT-10 channel. The corresponding device template will be installed with the L-IP Redundant Plug-In (see Section 10.4.1).

- To get a service pin message for commissioning the diagnostic node, press the Status button on the L-IP Redundant (see Section 6.5) or use the **Send Service Pin Msg** button in the corresponding section of the Device Information Page in the Web interface (see Section 7.1).

- Add two “Twin Router” functional blocks, one for each L-IP Redundant diagnostic node.

- Connect nvoRedRtr of one L-IP Redundant with the nviRedRtr of its paired L-IP Redundant and vice versa.

If using LonMaker for Windows the resulting drawing should look like shown in Figure 118.

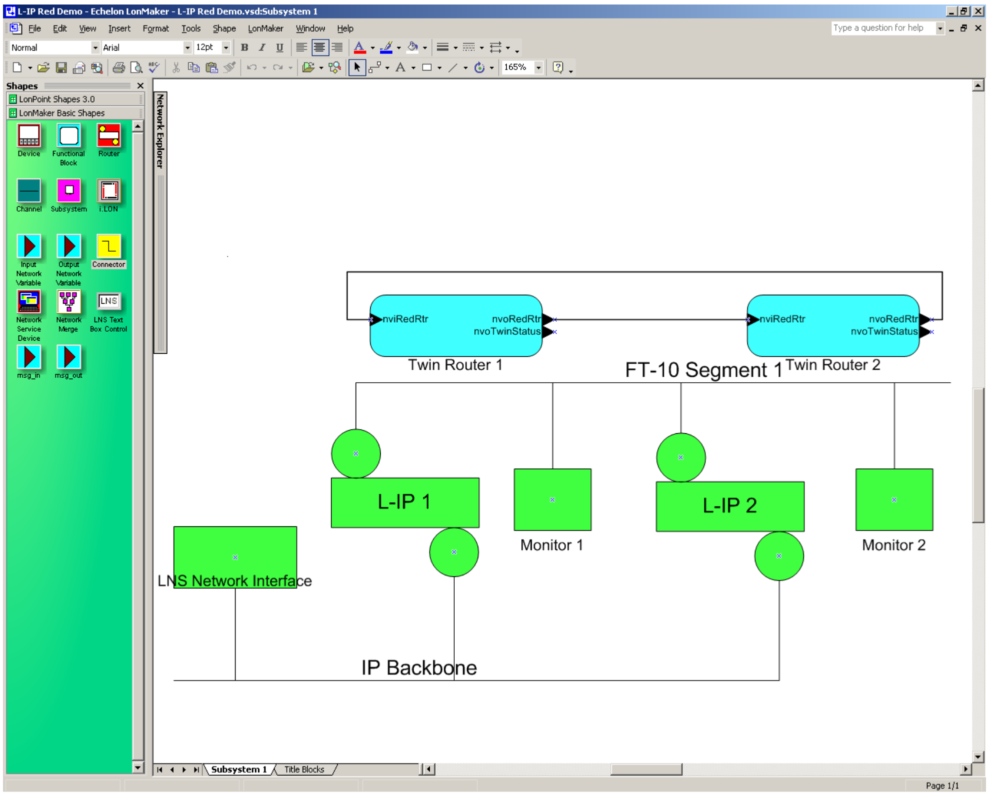


Figure 118: A pair of L-IP Redundant devices configured for twin router operation.

Be sure to commission both routers and both diagnostic nodes. Once both routers and both diagnostic nodes were successfully commissioned, the PRIM LED on one of the two L-IP Redundant devices should be green and should be off on the other one.

Important: ***If bus loop monitoring (see 10.2.1) is not used and thus the loop port 2 terminal of the L-IP Redundant routers is not connected be sure to first commission the router and the diagnostic node of one L-IP Redundant and switch off bus loop monitoring on this L-IP Redundant before connecting the second L-IP Redundant!***

After the router and the diagnostic node have been configured, use the L-IP Redundant Plug-In (see Section 10.5) or the web interface (see Section 10.6) to enter a node list for node monitoring or to change the parameters for bus loop monitoring and twin router monitoring.

10.5 L-IP Redundant Plug-In

10.5.1 Operation modes

The L-IP Redundant Configuration Plug-In can be used in on-line, off-line, and stand-alone mode. On-line and off-line mode refers to the two operating modes of your configuration tool.

10.5.1.1 On-line mode

This is the preferred method to use the configuration utility and allows using the full functionality of the plug-in. The network management tool is attached to the network and all network changes are directly propagated into the network. This mode must be used to commission the device, download and upload the node list, download and clear the alarm log, and get the current device state.

10.5.1.2 Off-line mode

The off-line mode can be used for all operations requiring LNS, that is, to add the device using the device templates, change the device properties, and create a node list including the automatic generation of a node list (LNS import). However, no communication with the device is possible (e.g. to download the node list).

10.5.1.3 Standalone mode

The L-IP Redundant Plug-In can also be executed as a standalone program. This operation mode offers least functionality. It allows creating and editing a node list or loading, altering and saving a configuration file.

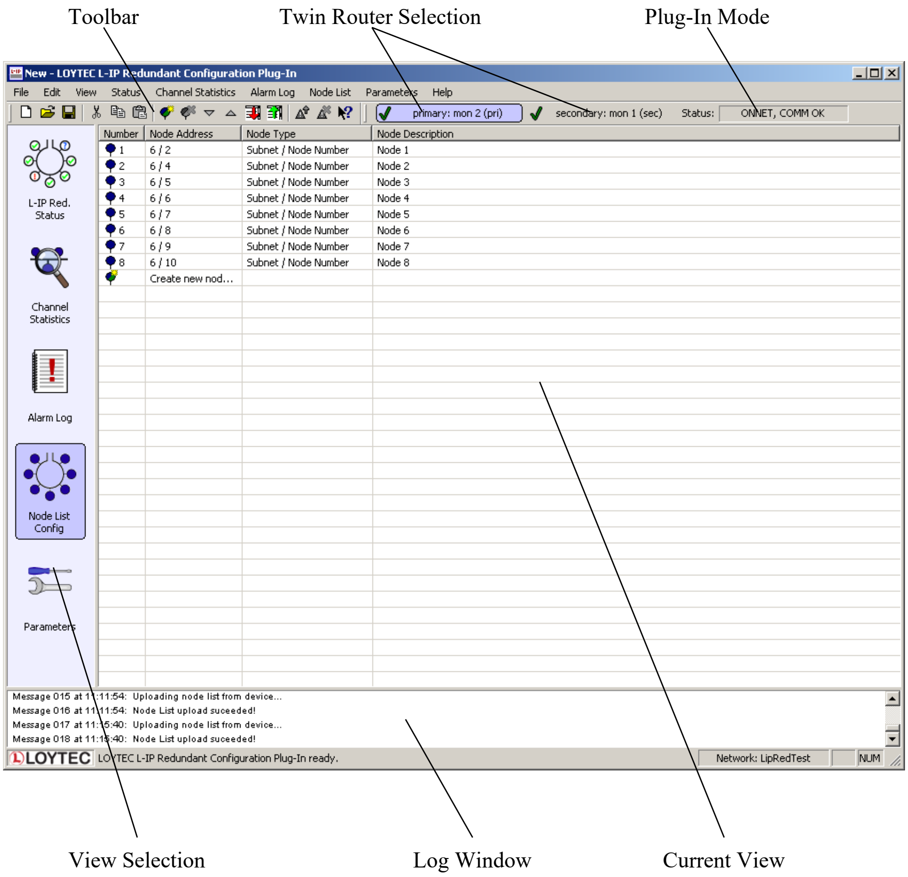
10.5.2 Overview

Figure 119 shows the L-IP Redundant Configuration Plug-In. The window is separated in three main areas:

- The view selection allows selecting different configuration and diagnostic pages.
- Depending on the selected view the current view area contains different information (e.g. the node list).
- The log window shows different all actions performed by the plug-in and any errors or warnings messages that occurred.

At the top of the window the toolbar allows selecting different actions depending on the currently selected view. The standard commands “load”, “save” and “new” are always possible. “Save” allows storing all configuration data (node list, properties) and the alarm log to a file, while “load” will restore all this information from a file. The information shown in the status and in the channel statistics view are not stored.

The “Twin Router Selection” shows the name of the primary and – if present – the secondary router. The one currently selected is marked. By clicking on the other one the selection can be changed on the fly.



Number	Node Address	Node Type	Node Description
1	6 / 2	Subnet / Node Number	Node 1
2	6 / 4	Subnet / Node Number	Node 2
3	6 / 5	Subnet / Node Number	Node 3
4	6 / 6	Subnet / Node Number	Node 4
5	6 / 7	Subnet / Node Number	Node 5
6	6 / 8	Subnet / Node Number	Node 6
7	6 / 9	Subnet / Node Number	Node 7
8	6 / 10	Subnet / Node Number	Node 8
	Create new nod...		

```
Message 015 at 11:11:54:  Uploading node list from device...
Message 016 at 11:11:54:  Node List upload suceeded!
Message 017 at 11:15:40:  Uploading node list from device...
Message 018 at 11:15:40:  Node List upload suceeded!
```

LOYTEC L-IP Redundant Configuration Plug-In ready.   Network: LipRedTest   NUM

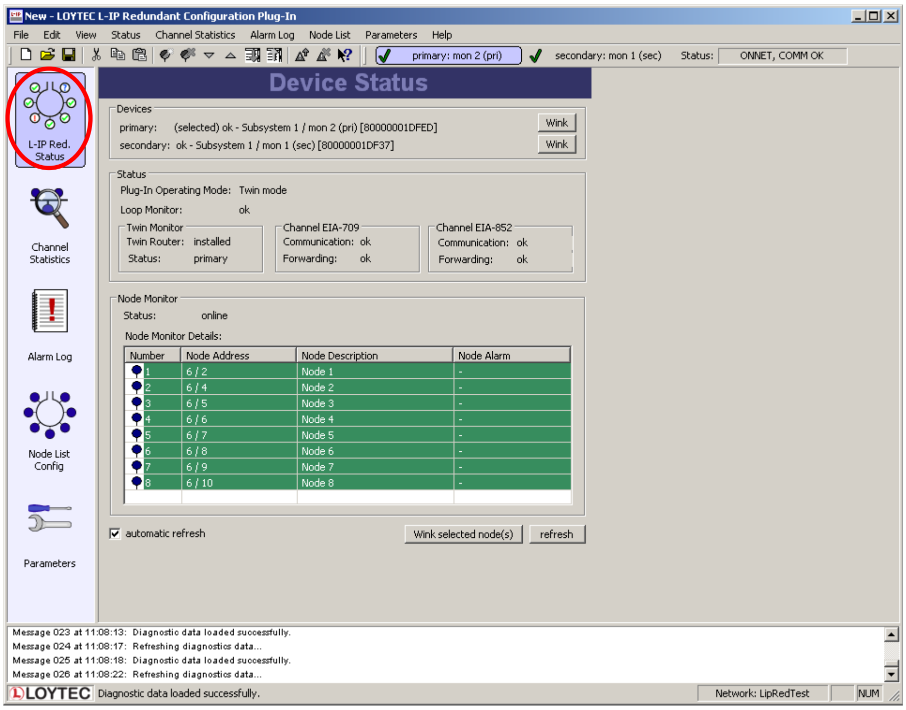
Figure 119: The L-IP Redundant Configuration Plug-In.

The “Plug-In Mode” shows the operation mode of the plug-in (see 10.5.1) and whether the device is accessible over the network.

10.5.3 Device Status

The device status view is used to view the current state of the L-IP Redundant. To access the device status view click on the “L-IP Red. Status” icon on the left side of the L-IP Redundant Plug-In window (see Figure 120).

Note: *Most of the diagnostic information is only available if the plug-in is running in online mode and the device is accessible over the network.*



Device Status

Devices
primary: (selected) ok - Subsystem 1 / mon 2 (pri) [80000001DFED]
secondary: ok - Subsystem 1 / mon 1 (sec) [80000001DF37]

Status
Plug-In Operating Mode: Twin mode
Loop Monitor: ok

Twin Monitor
Twin Router: installed
Status: primary

Channel EIA-709
Communication: ok
Forwarding: ok

Channel EIA-852
Communication: ok
Forwarding: ok

Node Monitor
Status: online
Node Monitor Details:

Number	Node Address	Node Description	Node Alarm
1	6 / 2	Node 1	-
2	6 / 4	Node 2	-
3	6 / 5	Node 3	-
4	6 / 6	Node 4	-
5	6 / 7	Node 5	-
6	6 / 8	Node 6	-
7	6 / 9	Node 7	-
8	6 / 10	Node 8	-

☑ automatic refresh

```
Message 023 at 11:08:13:  Diagnostic data loaded successfully.
Message 024 at 11:08:17:  Refreshing diagnostics data...
Message 025 at 11:08:18:  Diagnostic data loaded successfully.
Message 026 at 11:08:22:  Refreshing diagnostics data...
```

LOYTEC Diagnostic data loaded successfully.

Figure 120: The Device Status View.

The device status view has the following elements:

Devices

Shows the name and the subsystem of the primary and – if present – the secondary device. By clicking on the “Wink” button the corresponding L-IP Redundant can be winked (see 6.4.9). Further the device currently selected by the plug-in is shown (“selected”) and if the plug-in can communicate with the device (“ok”/”fail”). Finally the unique node ID of the monitoring node on the routers is given.

Loop Monitor

Shows whether the loop is open, closed or bus loop monitoring disabled.

Twin Monitor

Shows the twin router status of the device. This includes:

- Twin Router: Shows whether the device has a twin router installed.

- Status: Shows whether the device is primary, secondary, still negotiating or the secondary has temporary taken over since the primary failed.

- CEA-709/CEA-852 Communication: Shows whether its twin router is reachable via the CEA-709 and CEA-852 segment respectively.

- CEA-709/CEA-852 Forwarding: Shows whether the device forwards significantly lower amount of packets to its CEA-709 and CEA-852 side respectively (warning) or does not forward any packets anymore at all (error).

Node Monitoring Status List

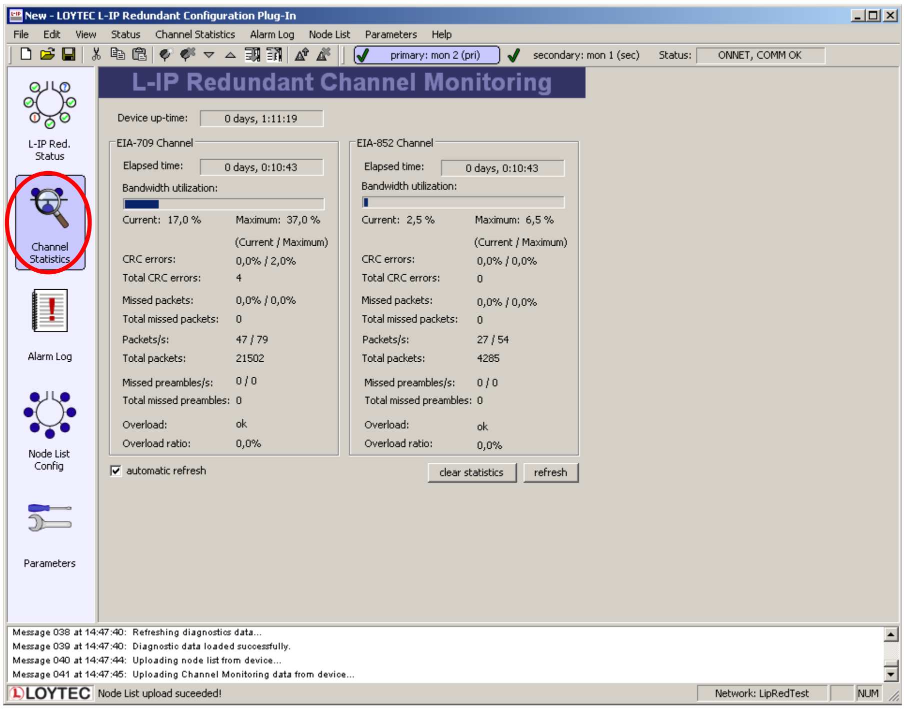
This list shows all the nodes in the node list of the device with the current status. If a node is not reachable/offline or the ring is open and the node is only reachable via one loop port the corresponding alarm is shown in the column “Node Alarm”. By selecting one or multiple nodes in the list and clicking on the “Wink selected node(s)” button the corresponding nodes can be winked using the CEA-709 wink network management command.

If the checkbox “automatically refresh data” is checked data in the device status view is refreshed every 15 seconds. The page can be refreshed manually by pressing the “refresh” button.

10.5.4 Channel Statistics

The channel statistics view is used to view statistic data accumulated by the L-IP Redundant for the two channels connected to the L-IP Redundant. To access the channel statistics view click on the “Channel Statistics” icon on the left side of the L-IP Redundant Plug-In window (see Figure 121).

Note: *Most of the diagnostic information is only available if the plug-in runs in online mode and the device is accessible over the network.*


New - LOYTEC L-IP Redundant Configuration Plug-In
File Edit View Status Channel Statistics Alarm Log Node List Parameters Help
L-IP Red. Status
Channel Statistics
Alarm Log
Node List Config
Parameters
L-IP Redundant Channel Monitoring
clear statistics
refresh
LOYTEC
NUM

primary: mon 2 (pri) secondary: mon 1 (sec) Status: ONNET, COMM OK

Device up-time: 0 days, 1:11:19

EIA-709 Channel

Elapsed time: 0 days, 0:10:43
Bandwidth utilization:
Current: 17,0 % Maximum: 37,0 %
(Current / Maximum)
CRC errors: 0,0% / 2,0%
Total CRC errors: 4
Missed packets: 0,0% / 0,0%
Total missed packets: 0
Packets/s: 47 / 79
Total packets: 21502
Missed preambles/s: 0 / 0
Total missed preambles: 0
Overload: ok
Overload ratio: 0,0%

EIA-852 Channel

Elapsed time: 0 days, 0:10:43
Bandwidth utilization:
Current: 2,5 % Maximum: 6,5 %
(Current / Maximum)
CRC errors: 0,0% / 0,0%
Total CRC errors: 0
Missed packets: 0,0% / 0,0%
Total missed packets: 0
Packets/s: 27 / 54
Total packets: 4285
Missed preambles/s: 0 / 0
Total missed preambles: 0
Overload: ok
Overload ratio: 0,0%

☑ automatic refresh

```
Message 038 at 14:47:40:  Refreshing diagnostics data...
Message 039 at 14:47:40:  Diagnostic data loaded successfully.
Message 040 at 14:47:44:  Uploading node list from device...
Message 041 at 14:47:45:  Uploading Channel Monitoring data from device...
```

Node List upload suceeded! Network: LipRedTest

Figure 121: The Channel Statistics View.

The channel statistics view has the following elements:

Device up-time

Shows the time elapsed since the L-IP was (re-)booted.

The following data is shown for each channel the L-IP Redundant is attached to (CEA-709/CEA-852):

Elapsed time

Shows the time since L-IP Redundant powered up or since the statistics for this port where reset.

Bandwidth utilization

Shows the current and the maximum value of the bandwidth utilization of the corresponding channel. The bar shows the current bandwidth utilization.

CRC errors

Shows the current and the maximum percentage as well as the total number of packets with CRC errors observed on the corresponding channel.

Missed Packets

Shows the current and the maximum percentage as well as the total number of packets, which could not be processed or received on the corresponding channel.

Packets

Shows the current and the maximum number of packets per second as well as the total number of packets on the corresponding channel.

Missed Preambles

Shows the current and the maximum number of missed preambles per second as well as the total number of missed preambles observed on the corresponding channel. A missed preamble is detected, whenever the link layer receives a preamble, which is shorter than the defined preamble length. A large number in this counter is usually due to noise on the channel.

Overload

Signals an overload 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 exceeded the limit defined by the parameter “Bandwidth Utilization Limit” (default 70%) OR

- The CRC Error Rate during the last statistic interval exceeded the limit defined by the parameter “CRC Error Limit” (default 5%) OR

- The Missed Packets Rate during the last statistic interval was not zero OR

- The Missed Preamble Rate during the last statistic interval exceeded the limit defined by the parameter “Missed Preamble Limit” (default switched off).

Overload Ratio

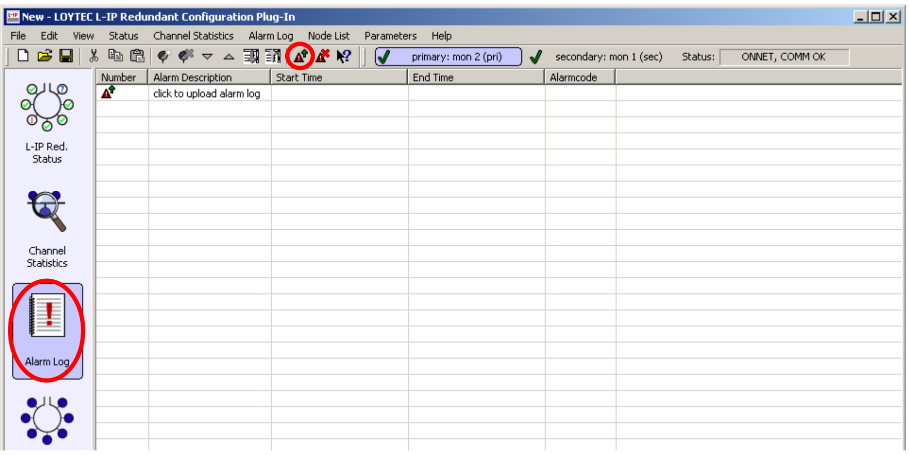
Ratio between statistic intervals during which the channel was in overload condition and intervals during which the channel was not in overload condition.

If the checkbox “automatically refresh data” is checked data in the channel statistics view is refreshed every 15 seconds. The page can be refreshed manually by pressing the “refresh” button. Finally all statistic data can be cleared by pressing the “clear statistics” button.

10.5.5 Alarm Log

Whenever an alarm occurs (e.g. “Ring open”) on the L-IP Redundant it is logged in the internal alarm log. The alarm log can hold up to 256 alarms.

The alarm log view is used to access the alarms logged in the L-IP Redundant. To access the alarm log click on the “Alarm Log” icon on the left side of the L-IP Redundant Plug-In window (see Figure 122).



primary: mon 2 (pri)

secondary: mon 1 (sec)

Status: ONNET, COMM OK

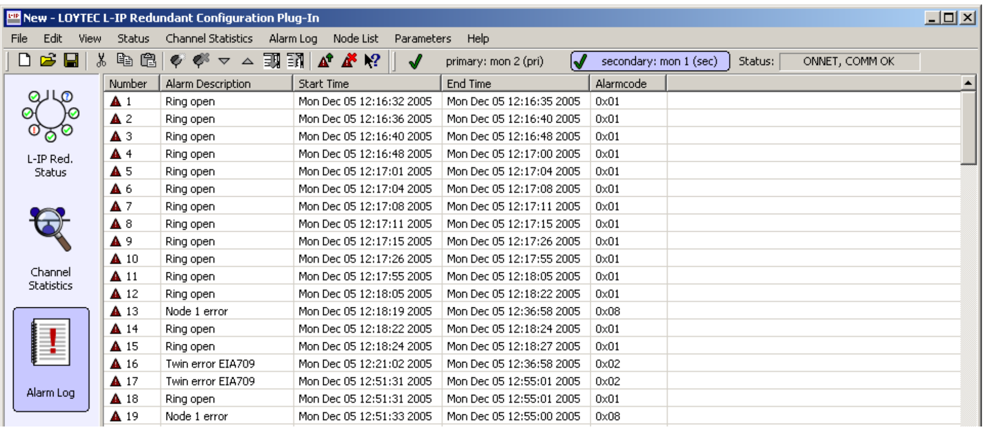
Number	Alarm Description	Start Time	End Time	Alarmcode
	click to upload alarm log			

Figure 122: The Alarm Log View.

If the plug-in is running in online mode you can download the alarm log from the L-IP Redundant either by double-clicking on the “click to upload alarm log” entry in the list, via “Upload Alarm Log” in the “Alarm Log” menu, or by clicking on the corresponding icon in the tool bar (see Figure 122). Similar the alarm log can be cleared.

Figure 123 shows a typical alarm log. For each alarm an description, a start time an end time and an alarm code is logged. All alarm times refer to the time set on the L-IP Redundant. Currently the following alarms are possible:

- "Ring open": Bus loop monitoring has detected an open loop (see Section 10.2.1).
- "Twin error CEA-709": Twin router is not reachable any more via the CEA-709 side (see Section 10.2.2).
- "Twin error IP": Twin router is not reachable any more via the CEA-852 side (see Section 10.2.2).
- "Fwd warning CEA-709": Packets forwarded from the CEA-709 to the CEA-852 side on the selected device is significantly lower than on the remote twin router (see Section 10.2.2).
- "Fwd warning IP": Packets forwarded from the CEA-852 to the CEA-709 side on the selected device is significantly lower than on the remote twin router (see Section 10.2.2).
- "Fwd error CEA-709": The selected device does not forward any packets from the CEA-709 to the CEA-852 side, while the remote twin router does.
- "Fwd error IP": The selected device does not forward any packets from the CEA-852 to the CEA-709 side, while the remote twin router does.
- “Side 1 disconnect”/”Side 2 disconnect”: The selected device does not reach its twin router via its port 1 or port 2 respectively. This error can only occur on the secondary (inactive) twin router.
- “Dev No <no> error” or “<desc> error”: Node with number <no> or description <desc> is either not reachable or not configured online.



Number	Alarm Description	Start Time	End Time	Alarmcode
▲ 1	Ring open	Mon Dec 05 12:16:32 2005	Mon Dec 05 12:16:35 2005	0x01
▲ 2	Ring open	Mon Dec 05 12:16:36 2005	Mon Dec 05 12:16:40 2005	0x01
▲ 3	Ring open	Mon Dec 05 12:16:40 2005	Mon Dec 05 12:16:48 2005	0x01
▲ 4	Ring open	Mon Dec 05 12:16:48 2005	Mon Dec 05 12:17:00 2005	0x01
▲ 5	Ring open	Mon Dec 05 12:17:01 2005	Mon Dec 05 12:17:04 2005	0x01
▲ 6	Ring open	Mon Dec 05 12:17:04 2005	Mon Dec 05 12:17:08 2005	0x01
▲ 7	Ring open	Mon Dec 05 12:17:08 2005	Mon Dec 05 12:17:11 2005	0x01
▲ 8	Ring open	Mon Dec 05 12:17:11 2005	Mon Dec 05 12:17:15 2005	0x01
▲ 9	Ring open	Mon Dec 05 12:17:15 2005	Mon Dec 05 12:17:26 2005	0x01
▲ 10	Ring open	Mon Dec 05 12:17:26 2005	Mon Dec 05 12:17:55 2005	0x01
▲ 11	Ring open	Mon Dec 05 12:17:55 2005	Mon Dec 05 12:18:05 2005	0x01
▲ 12	Ring open	Mon Dec 05 12:18:05 2005	Mon Dec 05 12:18:22 2005	0x01
▲ 13	Node 1 error	Mon Dec 05 12:18:19 2005	Mon Dec 05 12:36:58 2005	0x08
▲ 14	Ring open	Mon Dec 05 12:18:22 2005	Mon Dec 05 12:18:24 2005	0x01
▲ 15	Ring open	Mon Dec 05 12:18:24 2005	Mon Dec 05 12:18:27 2005	0x01
▲ 16	Twin error EIA709	Mon Dec 05 12:21:02 2005	Mon Dec 05 12:36:58 2005	0x02
▲ 17	Twin error EIA709	Mon Dec 05 12:51:31 2005	Mon Dec 05 12:55:01 2005	0x02
▲ 18	Ring open	Mon Dec 05 12:51:31 2005	Mon Dec 05 12:55:01 2005	0x01
▲ 19	Node 1 error	Mon Dec 05 12:51:33 2005	Mon Dec 05 12:55:00 2005	0x08

Figure 123: An alarm log.

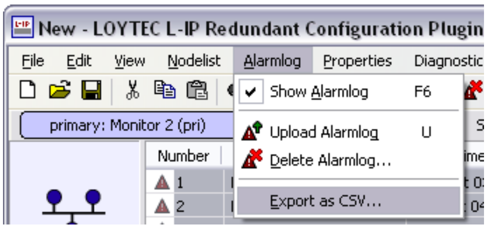
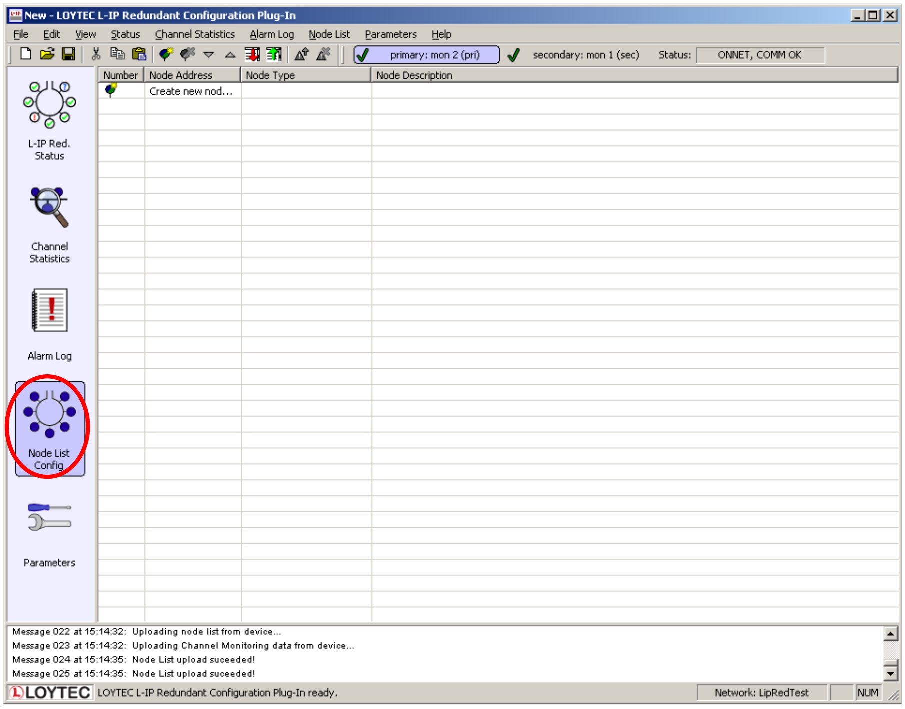


Figure 124: Exporting an alarm log to a CSV-file.

The alarm log can by transferred to another application using Copy & Paste or by export to a CSV-file (see Figure 124).

10.5.6 Node List Config

The node list is used for node monitoring (see Section 10.2.3). It must contain all the nodes, which should be monitored by the L-IP Redundant. If bus loop monitoring is used the order of the nodes in the list should represent the order of the nodes along the bus to be able to detect the point of fracture in case of a cable break: The node with index 1 must be the node closest to loop port 1 while the last node in the list must be the node closest to loop port 2.



Number	Node Address	Node Type	Node Description
	Create new nod...		

```
Message 022 at 15:14:32:  Uploading node list from device...
Message 023 at 15:14:32:  Uploading Channel Monitoring data from device...
Message 024 at 15:14:35:  Node List upload suceeded!
Message 025 at 15:14:35:  Node List upload suceeded!
```

LOYTEC L-IP Redundant Configuration Plug-In ready.   Network: LipRedTest   NUM

Figure 125: The Node List Config View.

To create a new node list or edit an existing node list, go to the node list view by clicking on the “Node List Config” icon on the left side of the L-IP Redundant Plug-In window (see Figure 125).

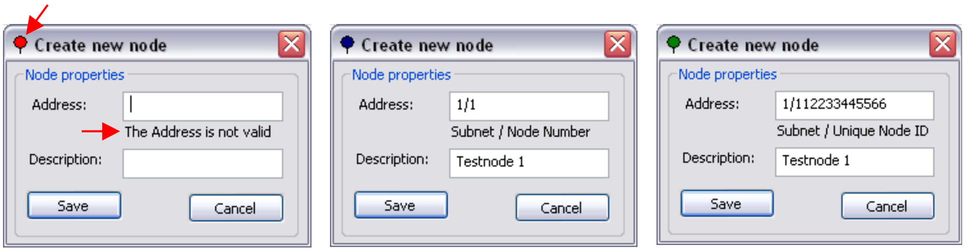
Nodes can be added to the node list in different ways:

- Nodes can be added or edited manually
- Node can be imported from the LNS database
- Nodes can be imported from a CSV-file

Further, the order of the nodes in the node lists can be changed and a node list can be exported. Finally the node list can be downloaded to the device and an existing node list can be uploaded from the device.

10.5.6.1 Manually add and edit nodes

You can double click on “Create new node…” to open the new node dialog box (see Figure 126).



Address: |
The Address is not valid
Description:

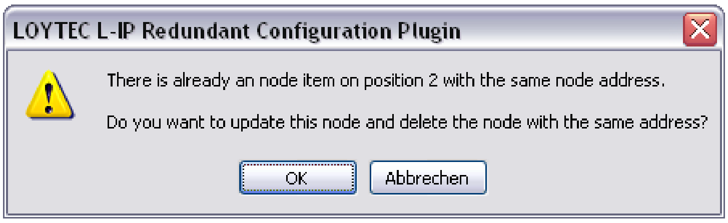
Address: 1/1
Subnet / Node Number
Description: Testnode 1

Address: 1/112233445566
Subnet / Unique Node ID
Description: Testnode 1

Figure 126: Adding a new node.

As you type the node address, it will be checked and the result of the syntax check is indicated by the dialog icon and the text field. Press the “Save” – Button to save the node address into the node list.

Existing nodes can be edited by double clicking on the row containing the node in the list.



LOYTEC L-IP Redundant Configuration Plugin

There is already an node item on position 2 with the same node address.

Do you want to update this node and delete the node with the same address?

Figure 127: Tried to save entry which is identical to an already existing one.

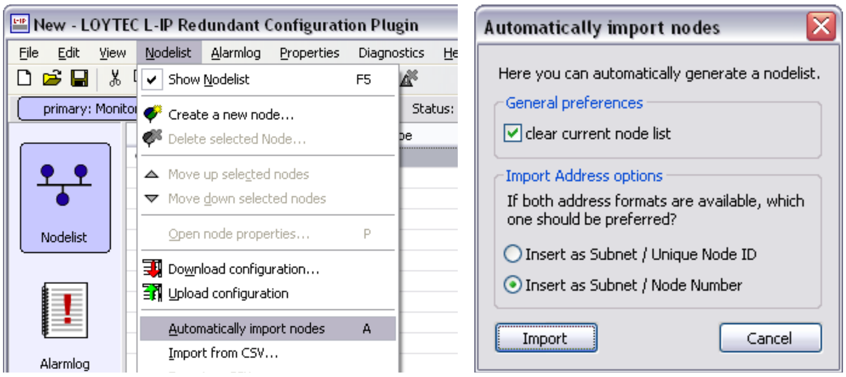
Note that the address is checked against double entries while saving and an error message will appear if you try to add a new entry or change the address of an existing entry into an address which already exists (see Figure 127). If you press OK here, entry number 2 will be deleted and entry number 1 updated.

10.5.6.2 Import node list from LNS database

Press ‘A’ on the keyboard or choose the entry in the “Node List” menu to open the “Automatically import nodes” – Dialog (see Figure 128).

You can choose to delete the current node list prior to import. If this option is not selected only nodes not present in the current node list are added. Further the address format used to contact the node can be selected. You can choose between the Subnet/Node address format and the Unique Node ID (“Neuron ID”) address format.

LNS import is only available in on-line and off-line operation mode, but not in standalone operation mode.



Automatically import nodes

Here you can automatically generate a nodelist.

General preferences

☑ clear current node list

Import Address options

If both address formats are available, which one should be preferred?

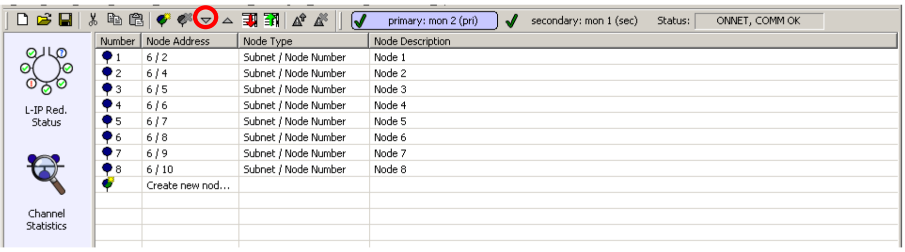
○ Insert as Subnet / Unique Node ID

● Insert as Subnet / Node Number

Figure 128: Import node list from LNS database.

10.5.6.3 Change order of node list

To change the order of the node list select the entries and move them up and down with the arrows in the toolbar (see Figure 129). To select multiple items press the CTRL-key while selecting.



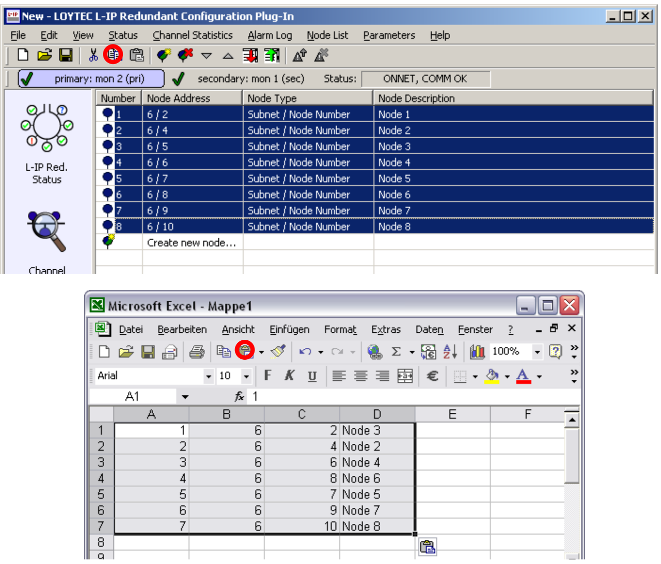
Number	Node Address	Node Type	Node Description
1	6 / 2	Subnet / Node Number	Node 1
2	6 / 4	Subnet / Node Number	Node 2
3	6 / 5	Subnet / Node Number	Node 3
4	6 / 6	Subnet / Node Number	Node 4
5	6 / 7	Subnet / Node Number	Node 5
6	6 / 8	Subnet / Node Number	Node 6
7	6 / 9	Subnet / Node Number	Node 7
8	6 / 10	Subnet / Node Number	Node 8
	Create new nod…		

Figure 129: Moving multiple entries in the node list.

10.5.6.4 Import/Export Node List

Entries in the node list can be selected and transferred to other applications using Copy & Paste (e.g. a spreadsheet application like Microsoft Excel). The fields copied are number, subnet address, node address OR unique node ID address, and description (see Figure 130).

Further, the node list can be exported and imported to/from a CSV-file. This allows using a spreadsheet application (e.g. Microsoft Excel) to create and edit the node list (see Figure 131).


New - LOYTEC L-IP Redundant Configuration Plug-In
File Edit View Status Channel Statistics Alarm Log Node List Parameters Help
primary: mon 2 (pri)
secondary: mon 1 (sec)
Status:
ONNET, COMM OK
L-IP Red. Status
Channel
Microsoft Excel - Mappe1
Datei Bearbeiten Ansicht Einfügen Format Extras Daten Fenster ?
Arial
10
100%
A1
1

Number	Node Address	Node Type	Node Description
1	6 / 2	Subnet / Node Number	Node 1
2	6 / 4	Subnet / Node Number	Node 2
3	6 / 5	Subnet / Node Number	Node 3
4	6 / 6	Subnet / Node Number	Node 4
5	6 / 7	Subnet / Node Number	Node 5
6	6 / 8	Subnet / Node Number	Node 6
7	6 / 9	Subnet / Node Number	Node 7
8	6 / 10	Subnet / Node Number	Node 8
	Create new node…		

	A	B	C	D	E	F
1	1	6	2	Node 3		
2	2	6	4	Node 2		
3	3	6	6	Node 4		
4	4	6	8	Node 6		
5	5	6	7	Node 5		
6	6	6	9	Node 7		
7	7	6	10	Node 8		
8						

Figure 130: Transfer the node list between applications with Copy & Paste.

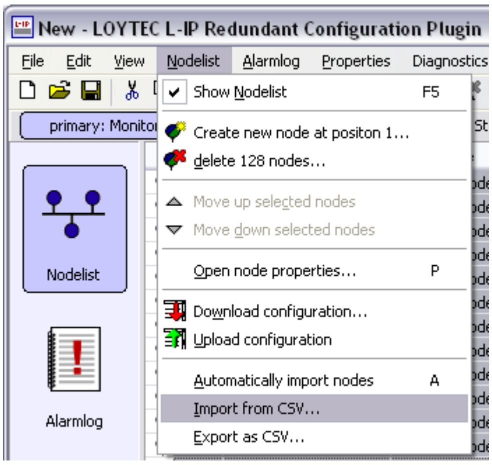


Figure 131: Importing a CSV-file.

10.5.6.5 Downloading and Uploading the Node List

If the L-IP Redundant Plug-In is running in Online-Mode the node list can be uploaded from the device and downloaded to the device (see Figure 132).

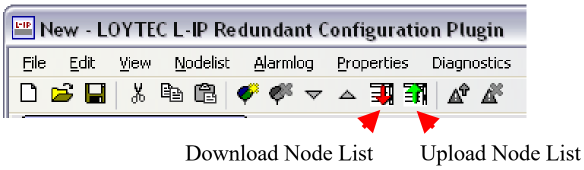
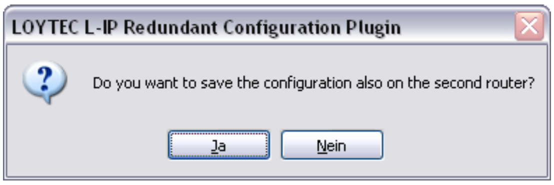


Figure 132: Up- and Downloading the Node List.

If the router redundancy is used, a dialog will ask whether to copy the same node list to the twin router (see Figure 133) after the download to the selected device has finished. It is strongly recommended to answer this dialog with "Yes".


LOYTEC L-IP Redundant Configuration Plugin

Do you want to save the configuration also on the second router?

Figure 133: Download the Node List to both routers?

10.5.7 Parameters

The properties view is used to access the configuration properties used to define the behaviour of the L-IP Redundant. To access the properties view click on the "Parameters" icon on the left side of the L-IP Redundant Plug-In window (see Figure 134).

The following properties can be changed:

Max Status Send Time

This parameter influences the heart beat functionality in the node object of the diagnostic node (see Section 10.7.1). If set to 0 the heart beat functionality is disabled, any other value will enable heart beat functionality and *nvoStatus*, *nvoAlarm* and *nvoAlarm_2* will be sent out with the interval defined by this value.

Enable Loop Monitor

Deselecting this check box will disable bus loop monitoring (see Section 10.2.1).

Max Send Time

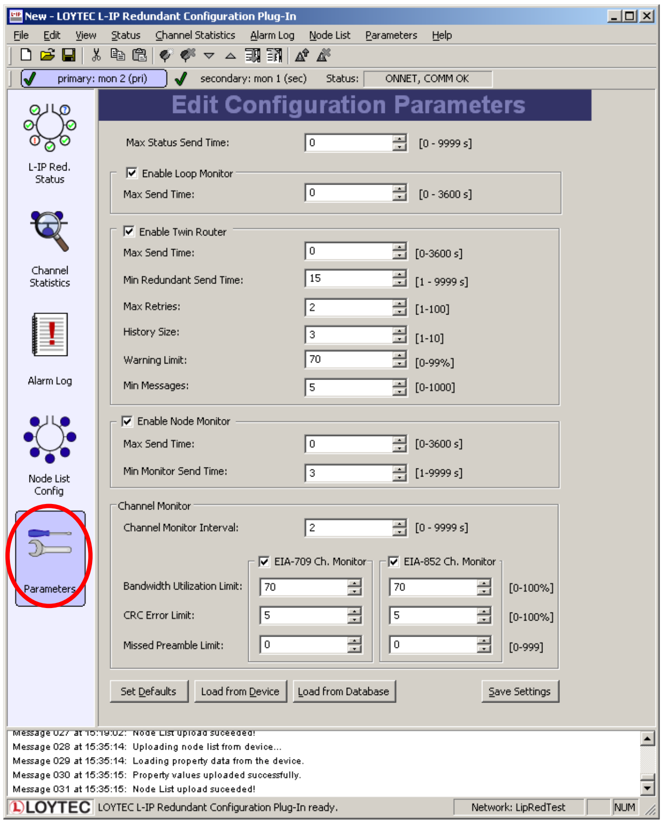
This parameter influences the heart beat functionality in the bus loop monitor object of the diagnostic node. If set to 0 the heart beat functionality is disabled, any other value will enable heart beat functionality and *nvoLoopOK* and *nvoLoopStatus* will be sent out with the interval defined by this value.

Enable Twin Router

Deselecting this check box will disable twin router monitoring (see Section 10.2.2). Note: If no twin router is present it is not required to turn off twin router monitoring.

Max Send Time

This parameter influences the heart beat functionality in the twin router object of the diagnostic node. If set to 0 the heart beat functionality is disabled, any other value will enable heart beat functionality and *nvoTwinStatus* will be sent out with the interval defined by this value.



✓ primary: mon 2 (pri) ✓ secondary: mon 1 (sec) Status: ONNET, COMM OK

Edit Configuration Parameters

Max Status Send Time: 0 [0 - 9999 s]

☑ Enable Loop Monitor

Max Send Time: 0 [0 - 3600 s]

☑ Enable Twin Router

Max Send Time: 0 [0-3600 s]

Min Redundant Send Time: 15 [1 - 9999 s]

Max Retries: 2 [1-100]

History Size: 3 [1-10]

Warning Limit: 70 [0-99%]

Min Messages: 5 [0-1000]

☑ Enable Node Monitor

Max Send Time: 0 [0-3600 s]

Min Monitor Send Time: 3 [1-9999 s]

Channel Monitor

Channel Monitor Interval: 2 [0 - 9999 s]

	☑ EIA-709 Ch. Monitor	☑ EIA-852 Ch. Monitor	
Bandwidth Utilization Limit:	70	70	[0-100%]
CRC Error Limit:	5	5	[0-100%]
Missed Preamble Limit:	0	0	[0-999]

```
Message 027 at 15:19:02:  Node List upload suceeded!
Message 028 at 15:35:14:  Uploading node list from device...
Message 029 at 15:35:14:  Loading property data from the device.
Message 030 at 15:35:15:  Property values uploaded successfully.
Message 031 at 15:35:15:  Node List upload suceeded!
```

LOYTEC L-IP Redundant Configuration Plug-In ready. Network: LipRedTest NUM

Figure 134: The Parameters View.

Min Redundant Send Time

This value defines the twin router monitoring interval. It must be identical on both twin routers.

Max Retries

This value defines the number of retries used by the twin router monitoring algorithm if the twin router does not respond. Thus, the maximum time it takes until a twin router failure will be detected calculates to:

$$TwinRouterFailureDetectionTime \leq Min\,\mathrm{Re}\,dundantSendTime \times (Max\,\mathrm{Re}\,tries + 1)$$

History Size

This value defines the number of monitoring intervals used to compare the number of packets forwarded by both twin routers. It must be identical on both twin routers.

Warning Limit

This value defines the limit for issuing the “Forwarding Warnings” (see *nvoTwinStatus*, Section 10.7.4 or alarm log, Section 10.6.3): If the number of packets forwarded by the local router is less then <*Warning Limit*> % of the number of packets forwarded by the twin router an warning is triggered.

Min Messages

This value defines minimum number of packets to be forwarded on the twin router to issue a “Forwarding Error” (see *nvoTwinStatus*, Section 10.7.4 or alarm log, Section 10.6.3): If the number of packets forwarded by the local router is zero but the number of packets forwarded by the twin router is at least < *Min Messages* > the alarm is issued. Further, if the device is the primary router the secondary router will take over (standby mode).

Enable Node Monitor

Deselecting this check box will disable node monitoring (see 10.2.3).

Max Send Time

This parameter influences the heart beat functionality in the device monitor object of the diagnostic node. If set to 0 the heart beat functionality is disabled, any other value will enable heart beat functionality and *nvoNodeMonAlarm, nvoNodeMonStatus, nvoRingALastNode, nvoRingBLastNode, nvoRingAReceived* and *nvoRingAReceived* will be sent out with the interval defined by this value.

Min Monitor Send Time

This value defines the interval used to send query status messages to the nodes in the node list. Thus, the maximum delay until a node failure is detected and the duration of a complete scan pass calculates to:

$$MaxDetectionDelay \leq TotalScanTime = MinMonitorSendTime \times NodesInNodeList$$

Channel Monitor Interval

This value defines the interval which is used by the channel monitor objects to accumulate statistic data and to calculate the resulting average values.

CEA-709 Ch. Monitor/CEA-852 Ch. Monitor

Deselecting these check boxes will disable the corresponding channel monitor object (see Section 10.2.3).

Bandwidth Utilization Limit

This value defines the upper bandwidth utilization limit for the calculation of the overload condition. If the current bandwidth utilization exceeds this limit the corresponding channel is considered to be in overload state. Set this value to 0 to exclude the bandwidth utilization from the calculation of the overload state.

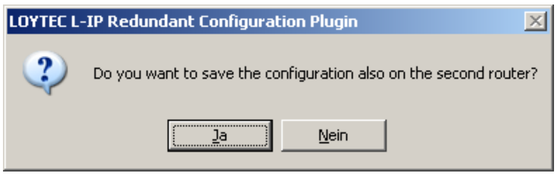
CRC Error Limit

This value defines the upper CRC error rate limit for the calculation of the overload condition. If the current CRC error rate exceeds this limit the corresponding channel is considered to be in overload state. Set this value to 0 to exclude the CRC error rate from the calculation of the overload state.

Missed Preamble Limit

This value defines the upper missed preamble rate limit for the calculation of the overload condition. If the current missed preamble rate exceeds this limit the corresponding channel is considered to be in overload state. Set this value to 0 to exclude the missed preamble rate from the calculation of the overload state.

If the plug-in runs in online mode the changes can be saved in the LNS database and downloaded to the device by pressing the “Save Settings” button, if the plug-in is in offline mode changes are only saved in the LNS database and will be downloaded to the device the next time the network management tool is in online mode.


LOYTEC L-IP Redundant Configuration Plugin

Do you want to save the configuration also on the second router?

Figure 135: Download configuration to second router?

If router redundancy is used and a twin router is assigned the configuration can also be synchronized with the twin router. Simply click “Yes” in the dialog shown after the configuration was stored for the selected router (see Figure 135). It is strongly recommended to always keep the configuration properties in both routers identical to guarantee smooth operation.

Default settings can be restored by pressing the “Set Defaults” button. To copy the values currently used by the device to the LNS database press the button “Load from Device”.

10.6 Web Interface

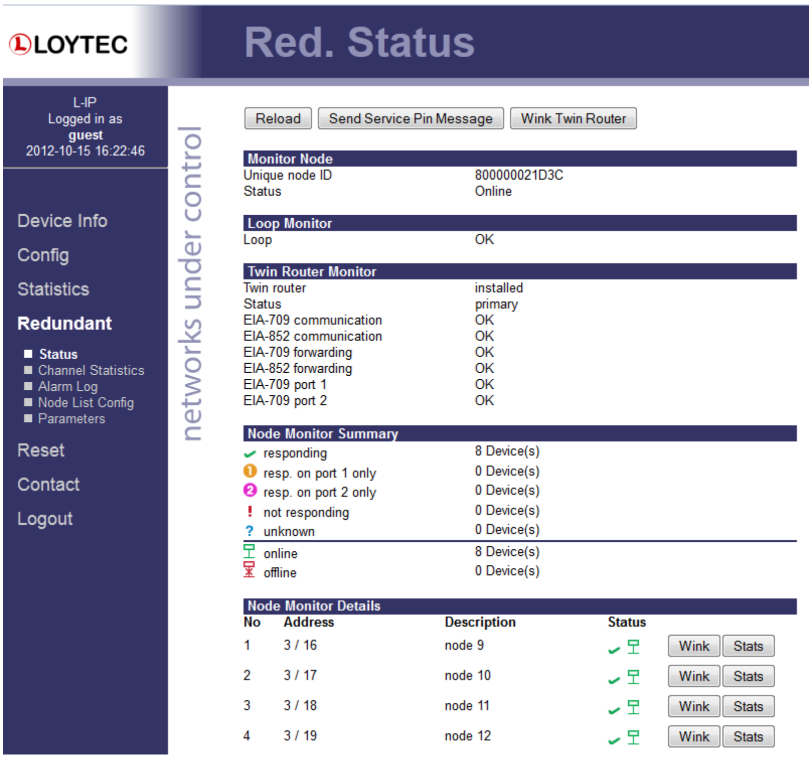
On the L-IP Redundant an additional item “Redundant” is found in the main menu of the web interface (see Figure 136). This menu item offers the following submenus:

10.6.1 Status

Figure 136 shows the status page. This page offers similar information as the status view of the L-IP Redundant Plug-In (see Section 10.5.3).

Major differences compared to the plug-in interface are:

- When clicking on the “Send Service Pin Message” button a service pin message is sent by the L-IP Redundant Diagnostic node.



Monitor Node	
Unique node ID	800000021D3C
Status	Online

Loop Monitor	
Loop	OK

Twin Router Monitor	
Twin router	installed
Status	primary
EIA-709 communication	OK
EIA-852 communication	OK
EIA-709 forwarding	OK
EIA-852 forwarding	OK
EIA-709 port 1	OK
EIA-709 port 2	OK

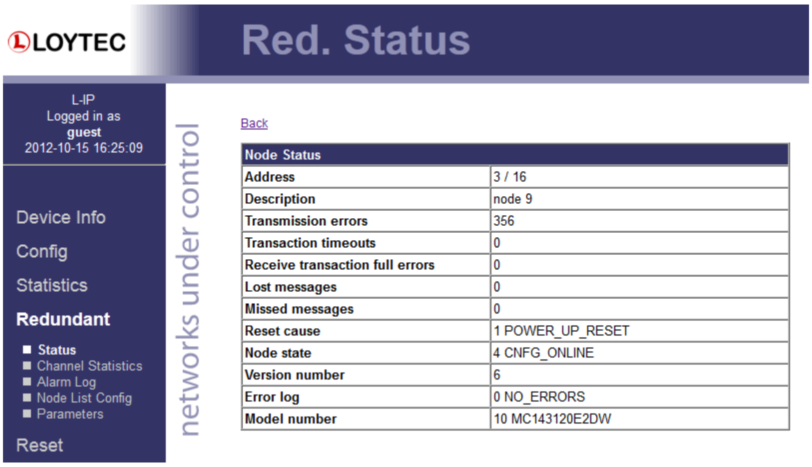
Node Monitor Summary	
✓ responding	8 Device(s)
❶ resp. on port 1 only	0 Device(s)
❷ resp. on port 2 only	0 Device(s)
! not responding	0 Device(s)
? unknown	0 Device(s)
online	8 Device(s)
offline	0 Device(s)

Node Monitor Details

No	Address	Description	Status	
1	3 / 16	node 9	✓	Wink Stats
2	3 / 17	node 10	✓	Wink Stats
3	3 / 18	node 11	✓	Wink Stats
4	3 / 19	node 12	✓	Wink Stats

Figure 136: The L-IP Redundant Web Interface – Status Page.

For each node in the “Node Monitor Details” table, which is responding over the network, a “Stats” button is present. This button allows viewing the node statistics of the remote node (see Figure 137).

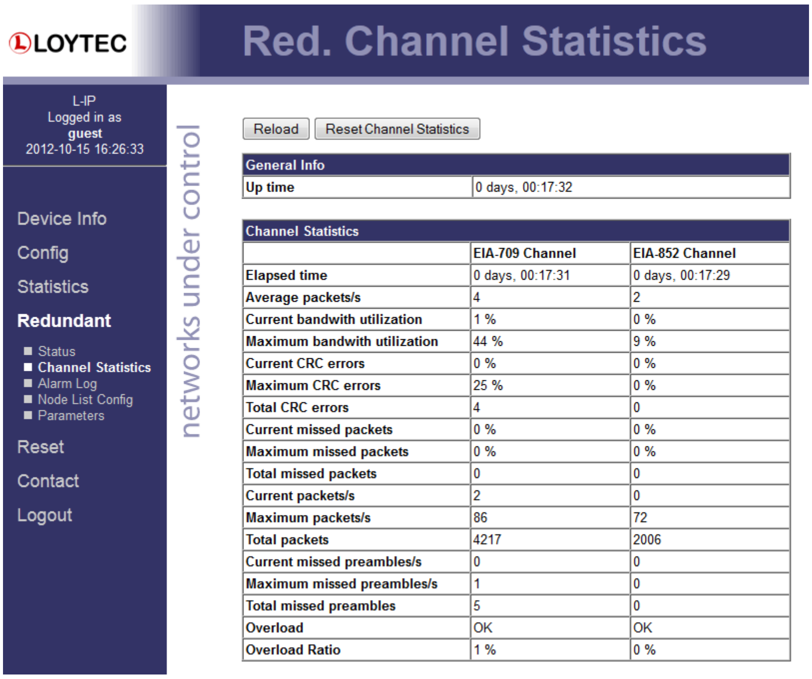


Node Status	
Address	3 / 16
Description	node 9
Transmission errors	356
Transaction timeouts	0
Receive transaction full errors	0
Lost messages	0
Missed messages	0
Reset cause	1 POWER_UP_RESET
Node state	4 CNFG_ONLINE
Version number	6
Error log	0 NO_ERRORS
Model number	10 MC143120E2DW

Figure 137: The L-IP Redundant Web Interface – Device Statistics Page.

10.6.2 Channel Statistics

Figure 138 shows the channel statistics page. This page offers similar information as the channel statistics view of the L-IP Redundant Plug-In (see Section 10.5.4).



General Info	
Up time	0 days, 00:17:32

Channel Statistics		
	EIA-709 Channel	EIA-852 Channel
Elapsed time	0 days, 00:17:31	0 days, 00:17:29
Average packets/s	4	2
Current bandwith utilization	1 %	0 %
Maximum bandwith utilization	44 %	9 %
Current CRC errors	0 %	0 %
Maximum CRC errors	25 %	0 %
Total CRC errors	4	0
Current missed packets	0 %	0 %
Maximum missed packets	0 %	0 %
Total missed packets	0	0
Current packets/s	2	0
Maximum packets/s	86	72
Total packets	4217	2006
Current missed preambles/s	0	0
Maximum missed preambles/s	1	0
Total missed preambles	5	0
Overload	OK	OK
Overload Ratio	1 %	0 %

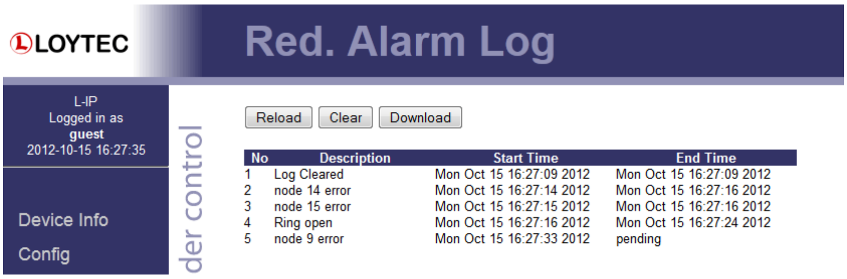
Figure 138: The L-IP Redundant Web Interface – Channel Statistics Page

10.6.3 Alarm Log

Figure 139 shows the alarm log page. This page offers similar information as the alarm log view of the L-IP Redundant Plug-In (see Section 10.5.5).

Major differences compared to the plug-in interface are:

A “Download” button allows downloading the alarm log as CSV-file.

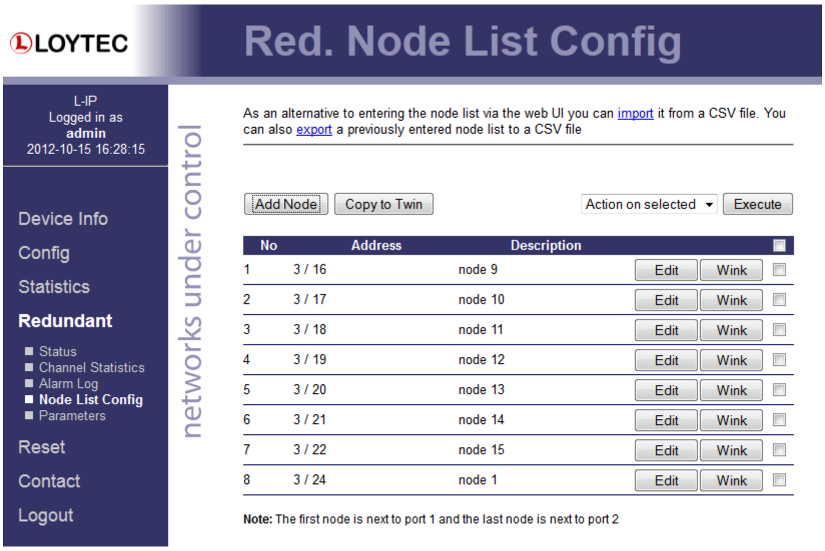


No	Description	Start Time	End Time
1	Log Cleared	Mon Oct 15 16:27:09 2012	Mon Oct 15 16:27:09 2012
2	node 14 error	Mon Oct 15 16:27:14 2012	Mon Oct 15 16:27:16 2012
3	node 15 error	Mon Oct 15 16:27:15 2012	Mon Oct 15 16:27:16 2012
4	Ring open	Mon Oct 15 16:27:16 2012	Mon Oct 15 16:27:24 2012
5	node 9 error	Mon Oct 15 16:27:33 2012	pending

Figure 139: The L-IP Redundant Web Interface – Alarm Log Page

10.6.4 Node List Configuration

Figure 140 shows the node list configuration page. This page offers similar information as the node list view of the L-IP Redundant Plug-In (see Section 10.5.6).



As an alternative to entering the node list via the web UI you can import it from a CSV file. You can also export a previously entered node list to a CSV file

No	Address	Description			□
1	3 / 16	node 9	Edit	Wink	□
2	3 / 17	node 10	Edit	Wink	□
3	3 / 18	node 11	Edit	Wink	□
4	3 / 19	node 12	Edit	Wink	□
5	3 / 20	node 13	Edit	Wink	□
6	3 / 21	node 14	Edit	Wink	□
7	3 / 22	node 15	Edit	Wink	□
8	3 / 24	node 1	Edit	Wink	□

Note: The first node is next to port 1 and the last node is next to port 2

Figure 140: The L-IP Redundant Web Interface – Node List Config Page

Major differences compared to the plug-in interface are:

Clicking on the link “import” allows importing/uploading a node list from a CSV-file

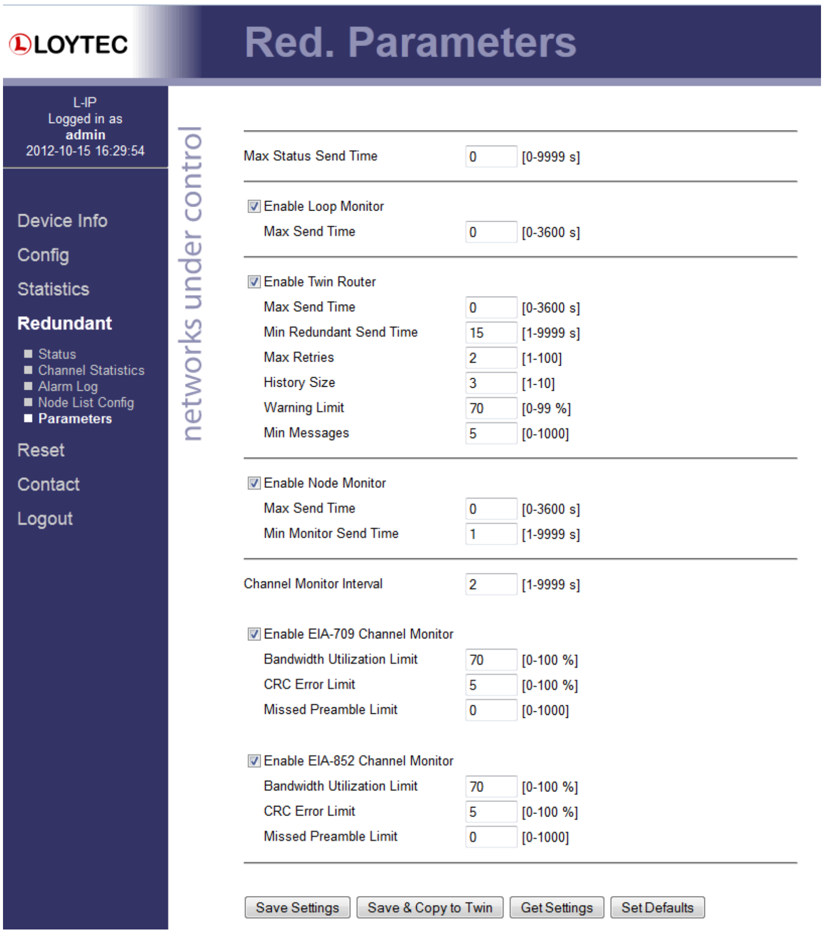
Multiple nodes can be selected by checking the check box at the end of each column. The drop down box “Action on Selected” allows choosing an action (Move up, Move down, Delete). Clicking on the “Execute” button executes the chosen action on the selected nodes list entries.

If router redundancy is used the node list can be copied to the twin router by clicking on the “Copy to Twin” button. It is strongly recommended to always copy the node list to the twin router if a node list has been created or edited.

Note that the node list is included in the backup and restore operation offered by the web interface (see Section 7.6.1).

10.6.5 Parameters

Figure 141 shows the parameters page. This page offers similar information as the parameters view of the L-IP Redundant Plug-In (see Section 10.5.7).



Max Status Send Time	0	[0-9999 s]
☑ Enable Loop Monitor		
Max Send Time	0	[0-3600 s]
☑ Enable Twin Router		
Max Send Time	0	[0-3600 s]
Min Redundant Send Time	15	[1-9999 s]
Max Retries	2	[1-100]
History Size	3	[1-10]
Warning Limit	70	[0-99 %]
Min Messages	5	[0-1000]
☑ Enable Node Monitor		
Max Send Time	0	[0-3600 s]
Min Monitor Send Time	1	[1-9999 s]
Channel Monitor Interval	2	[1-9999 s]
☑ Enable EIA-709 Channel Monitor		
Bandwidth Utilization Limit	70	[0-100 %]
CRC Error Limit	5	[0-100 %]
Missed Preamble Limit	0	[0-1000]
☑ Enable EIA-852 Channel Monitor		
Bandwidth Utilization Limit	70	[0-100 %]
CRC Error Limit	5	[0-100 %]
Missed Preamble Limit	0	[0-1000]

Figure 141: The L-IP Redundant Web Interface – Parameters Page

Major differences compared to the plug-in interface are:

If router redundancy is used, the button “Save & Copy to Twin” allows saving changes in the configuration to the local device and its twin router. It is strongly recommended to always copy the parameters to the twin router to guarantee smooth operation.

10.7 Network Interface

The following network variable interface is available for visualization, alarming and configuration. It follows the guidelines defined by the LonMark organization.

10.7.1 Node Object

The Node Object functional block is shown in Figure 142. In addition to the mandatory functions defined in the LonMark Node Object functional profile the following optional and user defined functions are implemented:

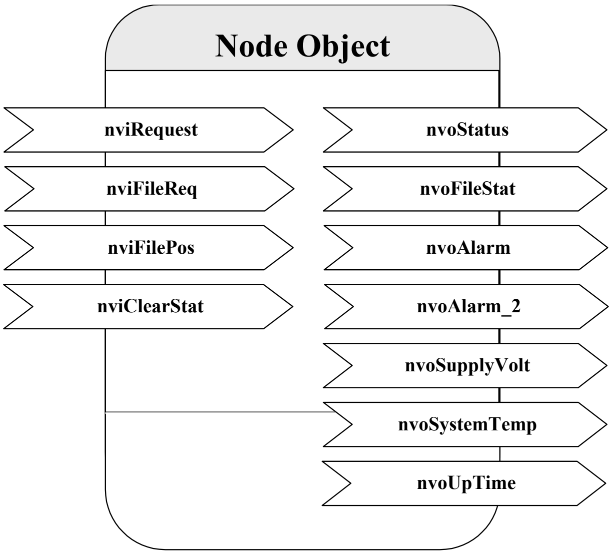


Figure 142: Node Object.

- 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

- LonMark alarming is supported via *nvoAlarm* (SNVT_alarm) and *nvoAlarm_2* (SNVT_alarm_2). This allows devices supporting the LonMark alarm notifier profile (e.g. i.LON 100) to receive alarms generated by the L-IP Redundant 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.

- The network variable *nvoSupplyVolt* (SNVT_volt) holds the current supply voltage of the L-IP Redundant, while *nvoSystemTemp* (SNVT_temp) contains the current internal temperature. With these two network variables a simple health monitoring can be performed.

- The statistic counters of all Channel Monitor objects (see Section 10.7.5) can be reset by setting the network variable *nviClearStat* (SNVT_switch) to {100, ON} and back to {0, OFF}.

- The network variable *nvoUpTime* (SNVT_elapsed_tm) gives the time elapsed since the L-IP was (re-)booted.

10.7.2 Bus Loop Monitor Object

Figure 143 shows the Bus Loop Monitor Object functional block. This functional block is responsible for the bus loop monitoring (see Section 10.2.1). It has the following network variables:

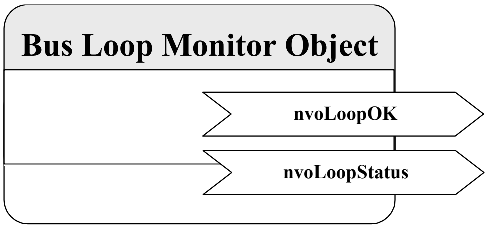


Figure 143: Bus Loop Monitor Object.

SNVT_switch nvoLoopOK

This network variable represents the loop state. It can have the following values:

- {100, ON}: The loop is closed.
- {0, OFF}: The loop is open.
- {0, INVAL}: Bus loop monitoring is disabled.

SNVT_state_64 nvoLoopStatus

This network variable represents the current state of the loop object. Currently the following bits are used:

- *bit0*: 0 if bus loop monitoring is enabled, 1 if bus loop monitoring is disabled. Bus loop monitoring can be disabled either manually (e.g. by disabling the object) or because the L-IP is in twin router mode and the device is in standby mode and thus inactive.
- *bit1*: 0 if the loop is closed, 1 if the loop is open.

10.7.3 Device Monitor Object

Figure 144 shows the Device Monitor Object functional block. This functional block is responsible for the device monitoring (see Section 10.2.3). It has the following network variables:

SNVT_state_64 nvoNodeMonStatus

This network variable represents the current state of the device monitor object. Currently the following bits are used:

- *bit0*: 0 if device monitoring is enabled, 1 if device monitoring is disabled. Device monitoring can be disabled either manually (e.g. by disabling the object) or because the L-IP is in twin router mode and the device is in standby mode and thus inactive.
- *bit1*: 0 if all monitored nodes node is reachable and online or was not yet queried, 1 otherwise.

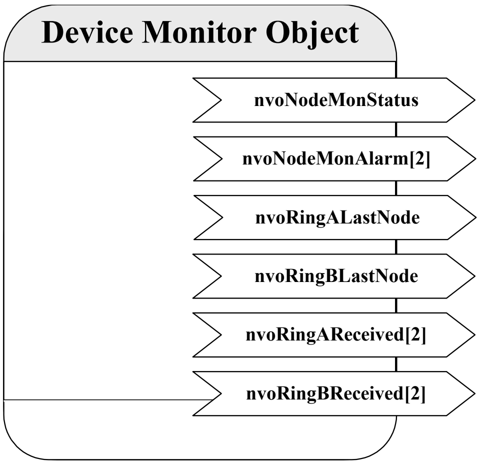


Figure 144: Device Monitor Object.

SNVT_state_64 nvoNodeMonAlarm[2]

Shows the state of the monitored nodes. Each bit corresponds to one node in the node list (e.g. bit0 -> index 1, bit1 -> index 2, etc.). Array element *nvoNodeMonAlarm[0]* represents nodes with index 1- 64, while array element *nvoNodeMonAlarm[1]* represents nodes with index 65-128. If the bit is 0 the corresponding node is reachable and online or was not yet queried, if the bit is 1 the corresponding node is not reachable or not in configured online state.

SNVT_count nvoRingALastNode

SNVT_count nvoRingBLastNode

These two network variables allow detecting the point of fracture if the loop is interrupted by showing the two nodes closest to the fracture. *nvoRingALastNode* contains the index of the last node reachable from loop port 1, while *nvoRingBLastNode* contains the index of the last node reachable from loop port 2. The value is encoded as follows:

0:	All nodes are reachable from this port (loop closed).
1-128:	Loop interrupted. Value corresponds to index of last node reachable from this port.
0xFFFF:	Loop interrupted directly at loop port 1 (*nvoRingALastNode*) or loop port 2 (*nvoRingBLastNode*) respectively.

Note: *Only valid if bus loop monitoring is enabled and the node list order corresponds to the order of the nodes within the loop (node closest to loop port 1 has index 1, node closest to loop port 2 has highest index). Otherwise the network variable is set to 0.*

SNVT_state_64 nvoRingAReceived[2]

SNVT_state_64 nvoRingBReceived[2]

Shows on which port(s) the monitored nodes were responding to the last query status request sent by the device monitor object. Each bit corresponds to one node in the node list (e.g. bit0 -> index 1, bit1 -> index 2, etc.). Array element *nvoRingXReceived[0]* represents nodes with index 1- 64, while array element *nvoRingXReceived[1]* represents nodes with index 65-128. If the corresponding bit in *nvoRingAReceived[X]* is set to 1 the node was responding on loop port 1, if it is set in *nvoRingBReceived[X]* the node was responding on loop port 2. This allows the combinations shown in Table 7.

RingAReceived	RingBReceived	Significance
0	0	No response received Node is responding from other subnet (i.e. across the router) Bus loop monitoring disabled
1	0	Node responds on port 1 only Loop is open
0	1	Node responds on port 2 only Loop is open
1	1	Node responds on both ports Loop is closed

Table 7: Significance of nvoRingXReceived bit combinations.

10.7.4 Twin Router Object

Figure 145 shows the Twin Router Object functional block. This functional block is responsible for the router redundancy (see Section 10.2.2). It has the following network variables:

UNVT_red_rtr nviRedRtr

UNVT_red_rtr nvoRedRtr

As already mentioned in Section 10.4.3.2 these two network variables are used to establish the connection between paired L-IP Redundant devices.

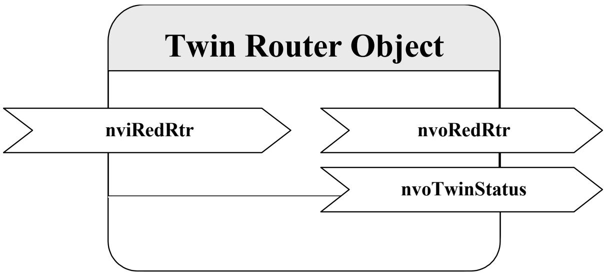


Figure 145: Twin Router Object.

SNVT_state_64 nvoTwinStatus

This network variable represents the current state of the twin router object. Currently the following bits are used:

- *bit0*: 0 if twin router monitoring is enabled, 1 if twin router monitoring is disabled. Twin router monitoring can be disabled only manually (e.g. by disabling the object).

- *bit1*: 0 if the device is the secondary router, 1 if the device is the primary router.

- *bit2*: 0 if the device is in normal operation mode (primary -> active, secondary -> inactive), 1 if the secondary router has taken over (primary -> inactive, secondary -> active).

- *bit3*: 0 if the device is in normal operation, 1 if the device is currently negotiating with its twin router to determine which one is primary and which secondary router.

- *bit4*: 0 if the twin router address is not known yet, 1 if the twin router address is known. If the twin router address is not yet known CEA-852 monitoring (bit9) and the forwarding warnings and errors (bit10-bit13) are not applicable.

- *bit8*: 1 if the twin router is not reachable via the CEA-709 segment (local segment), 0 otherwise.

- *bit9*: 1 if the twin router is not reachable via the IP-852 channel (IP backbone), 0 otherwise.

- *bit10*: 1 if the packets forwarded from the CEA-709 to the CEA-852 side on the local device is significantly lower than on the remote twin router. 0 if the router is working properly.

- *bit11*: 1 if the packets forwarded from the CEA-852 to the CEA-709 side on the local device is significantly lower than on the remote twin router. 0 if the router is working properly.

- *bit12*: 1 if the local device does not forward any packets from the CEA-709 to the CEA-852 side, while the remote twin router does. 0 if the router is working properly.

- *bit13*: 1 if the local device does not forward any packets from the CEA-852 to the CEA-709 side, while the remote twin router does. 0 if the router is working properly.

10.7.5 Channel Monitor Objects

Figure 146 shows the Channel Monitor Object functional block. This functional block is responsible for network monitoring (see Section 10.2.3). There is one object for each channel the L-IP Redundant is attached to: The channel monitor object with index 0 corresponds to the CEA-709 side of the L-IP Redundant, while the object with index 1 corresponds to the CEA-852/IP side of the L-IP Redundant. Each object has the following network variables:

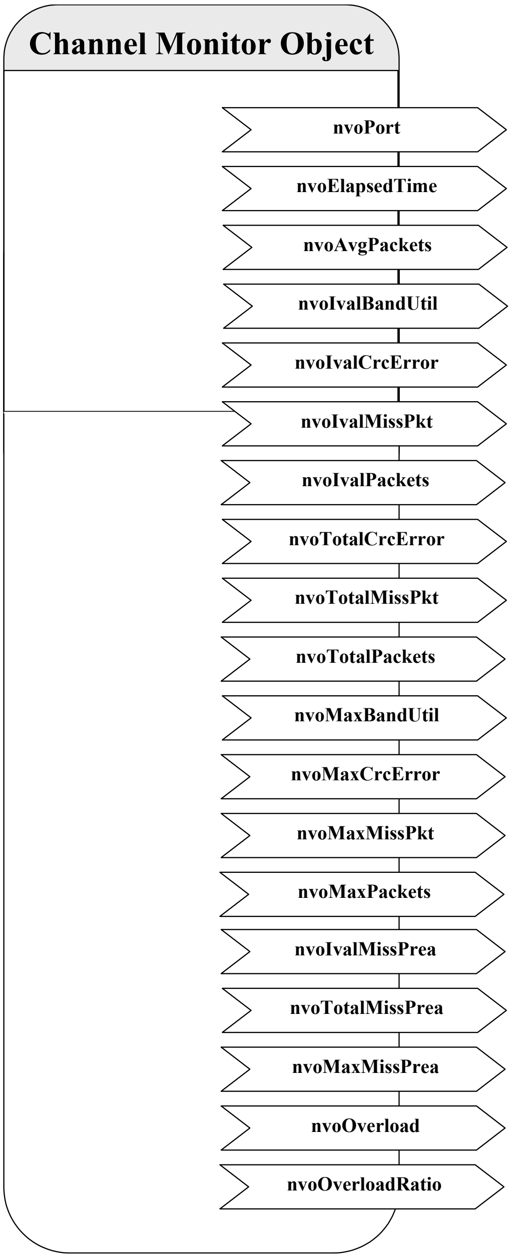


Figure 146: Channel Monitor Object.

SNVT_count nvoPort

Index of port associated with this Channel Monitor Object instance. Port 1 corresponds to the CEA-709 side of the L-IP Redundant, while port 2 corresponds to the CEA-852/IP side of the L-IP Redundant. Polled only.

SNVT_elapsed_tm nvoElapsedTime

Time since L-IP Redundant powered up or since the statistics for this port where reset. The statistics can be reset using the web interface (see Section 10.6), the network variable *nvoClearStat* (see Section 10.7.1) or if the node is reset with a network management command (e.g. while the device is commissioned). Polled only.

SNVT_count_32 nvoAvgPackets

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.

SNVT_lev_cont nvoIvalBandUtil

Bandwidth utilization of associated channel during the last interval. For a smooth operation of the CEA-709 segment the bandwidth utilization must remain below 50%.

SNVT_lev_cont nvoIvalCrcError

Percentage of packets with CRC error received on the associated channel during the last interval.

SNVT_lev_cont nvoIvalMissPkt

Percentage of packets from the associated channel which could not be processed during the last interval.

SNVT_count_32 nvoIvalPackets

Number of packets received or transmitted via the associated channel during the last interval.

SNVT_count_32 nvoTotalCrcError

Total number of packets with CRC error received via the associated channel since power-up or since the statistics for this port where reset.

SNVT_count_32 nvoTotalMissPkt

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.

SNVT_count_32 nvoTotalPackets

Total number of packets received or transmitted via the associated channel since power-up or since the statistics for this port where reset.

SNVT_lev_cont nvoMaxBandUtil

Maximum value of *nvoIvalBandUtil* since power-up or since the statistics for this port where reset. For a smooth operation of the CEA-709 segment the bandwidth utilization must remain below 50%.

SNVT_lev_cont nvoMaxCrcError

Maximum value of *nvoIvalCrcError* since power-up or since the statistics for this port where reset.

SNVT_lev_cont nvoMaxMissPkt

Maximum value of *nvoIvalMissPkt* since power-up or since the statistics for this port where reset.

SNVT_count_32 nvoMaxPackets

Maximum value of *nvoIvalPackets* since power-up or since the statistics for this port where reset.

SNVT_count_32 nvoIvalMissPrea

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.

SNVT_count_32 nvoTotalMissPrea

Total number of missed preambles per second on the associated channel measured since power-up or since the statistics for this port where reset.

SNVT_count_32 nvoMaxMissPrea

Maximum value of *nvoIvalMissPrea* since power-up or since the statistics for this port where reset.

SNVT_switch nvoOverload

Signals an overload 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 (*nvoIvalBandUtil*) exceeded the limit defined by the CP *nciBandUtilLim* (default 70%) OR

- The CRC Error Rate during the last statistic interval (*nvoIvalCrcError*) exceeded the limit defined by the CP *nciCrcErrorLim* (default 5%) OR

- The Missed Packets Rate during the last statistic interval (*nvoIvalMissPkt*) was not zero OR

- The Missed Preamble Rate during the last statistic interval (*nvoIvalMissPrea*) exceeded the limit defined by the CP *nciMissPreaLim* (default switched off).

If an overload is detected the network variable is set to {100, ON}, while if no error occurred it is set to {0, OFF}.

SNVT_lev_cont nvoOverloadRatio

Ratio between statistic intervals during which the channel was in overload condition and intervals during which the channel was not in overload condition since power-up or since the statistics for this port where reset.

11 Operating Interfaces

11.1 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.

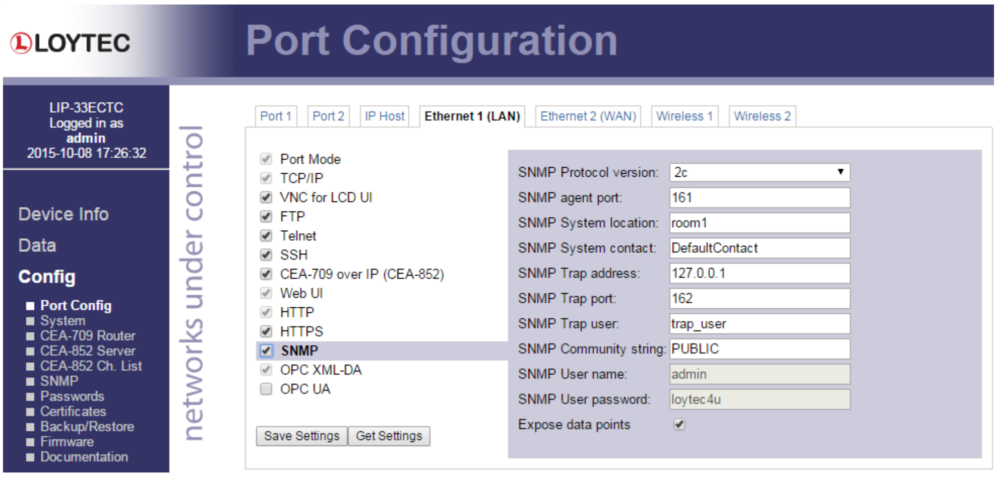
11.1.1 SNMP Features

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.

11.1.2 Configuration

The SNMP agent can be configured in the Web UI and in the configuration software. Figure 147 shows the Web interface. The settings in the configuration software are similar.



☑ Port Mode
☑ TCP/IP
☑ VNC for LCD UI
☑ FTP
☑ Telnet
☑ SSH
☑ CEA-709 over IP (CEA-852)
☑ Web UI
☑ HTTP
☑ HTTPS
☑ SNMP
☑ OPC XML-DA
□ OPC UA

SNMP Protocol version:	2c
SNMP agent port:	161
SNMP System location:	room1
SNMP System contact:	DefaultContact
SNMP Trap address:	127.0.0.1
SNMP Trap port:	162
SNMP Trap user:	trap_user
SNMP Community string:	PUBLIC
SNMP User name:	admin
SNMP User password:	loytec4u
Expose data points	☑

Figure 147: 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:** This 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.

11.1.3 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.

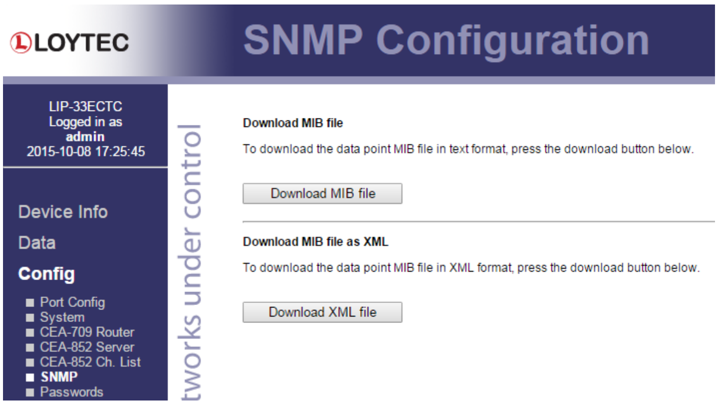
As SNMP has several restrictions on what can be represented, the following mappings are made:

- **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.



Download MIB file

To download the data point MIB file in text format, press the download button below.

Download MIB file as XML

To download the data point MIB file in XML format, press the download button below.

Figure 148: Downloading device-specific MIB files

Figure 148 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.

11.1.4 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.

12 Network Media

12.1 TP-1250

The TP-1250 uses transformers for galvanic isolation. The topology of a TP-1250 network is a bus. Thus, both ends of the bus cable need to be terminated. LOYTEC recommends using its L-TERM network terminators (LT-13) for network termination (see Figure 149).

If the collision-less backbone mode (recommended, default behavior) is disabled, the L-IP TP-1250 ports are fully compatible to the parameters specified by LONMARK for this channel (TP/XF-1250). If the collision-less backbone mode is enabled, proprietary channel parameters are used. In this case no Neuron Chip based nodes or other nodes with standard TP-1250 communication parameters are permitted on the same channel.

12.2 FT-10

The L-IP FT-10 ports are fully compatible to the parameters specified by LONMARK for this channel. FT-10 ports can also be used on Link Power (LP-10) channels. However, the L-IP does not provide the power supply for Link Power channels.

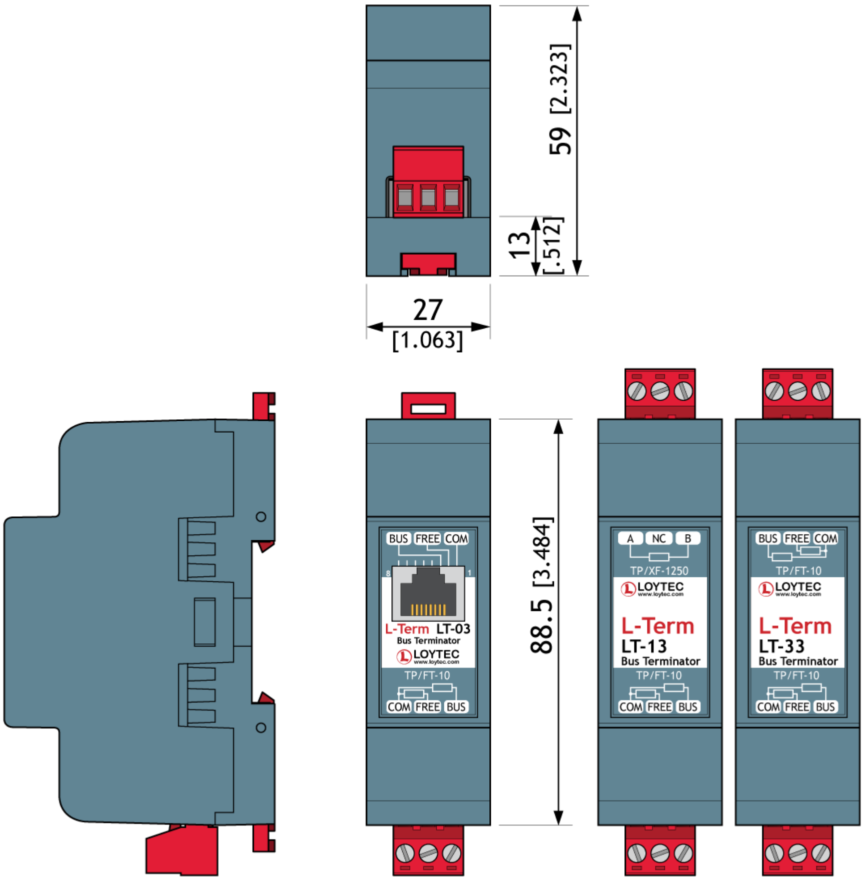


Figure 149: FT-10 Network Termination.

When using the Free Topology Segment feature of the FT-10, only one termination is required and can be placed anywhere on the free topology segment. In a double terminated bus topology, two terminations are required. These terminations need to be placed at each end of the bus.

LOYTEC recommends using its L-TERM network terminators (LT-13, LT-33 or LT-03) for network termination (see Figure 149).

12.3 RS-485

The L-IP RS-485 ports are fully compatible with the parameters specified by TIA/EIA RS-485 for this channel. A maximum of 32 L-IP RS-485 ports can be connected to one channel.

The RS-485 ports support bit-rates between 300 kbps and 2.5 Mbps. When using bit-rate auto-detection the L-IP checks for the following bit-rates: 0.61 kbps, 1.221 kbps, 2.441 kbps, 4.883 kbps, 9.766 kbps, 19.531 kbps, 39.0625 kbps, 78.125 kbps, 156.25 kbps, 312.5 kbps, 625 kbps, 1,250 kbps and 2,500 kbps. Standard Neuron Chip compatible channel parameters with a channel priority of 4, but no node priority are used with these bit-rates. If bit-rate auto-detection is switched off, the channel parameters for the LONMARK TP-RS485-39 channel (39 kbps) are used.

RS-485 can only be used in a bus configuration and must be terminated on both ends. The maximum stub length between the main bus and a single node is 0.3 m.

LOYTEC recommends using its L-TERM network terminators (LT-04 or LT-B4) for network termination (see Figure 150).

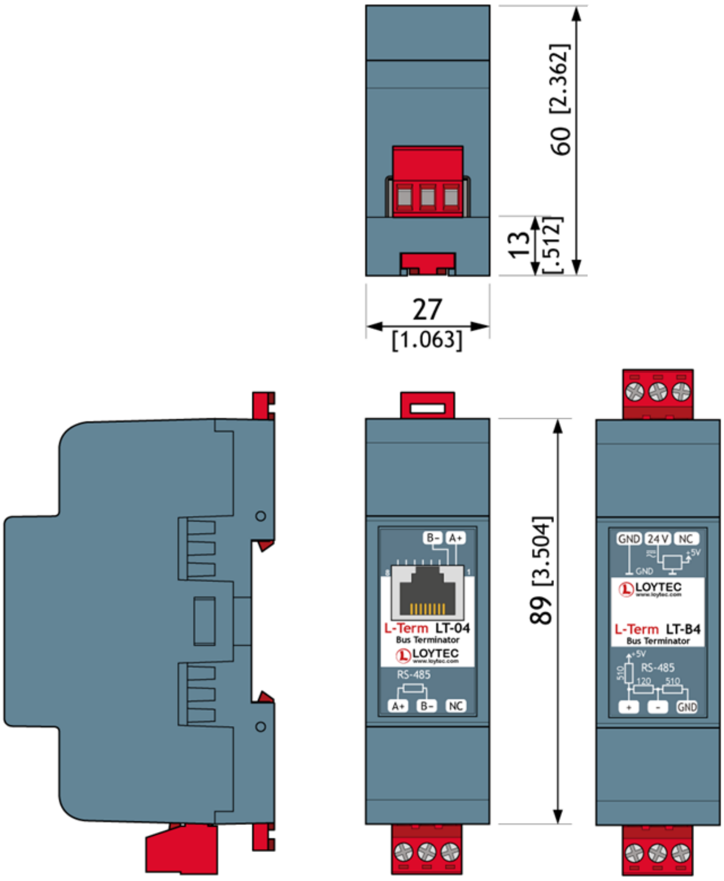


Figure 150: RS-485 Network Termination.

The L-IP supports bit-rate auto-detection on RS-485 channels. The factory default DIP-switch setting enables bit-rate auto-detection on all RS-485 ports. Figure 151 shows the DIP-switch settings to disable bit-rate auto-detection, assuming all other DIP switches remain in the factory default position.

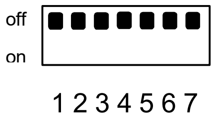


Figure 151: DIP-switch 3 disables bit-rate auto-detection

Alternatively the bit-rate auto-detection can be enabled/disabled via the console menu. Further the console menu allows restarting the bit-rate auto-detection on selected ports. While the port is auto-detecting the activity LED is flashing orange.

12.4 Redundant Ethernet

12.4.1 Ethernet Cabling Options

The L-IP series “C” 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-IP, 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-IP 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.

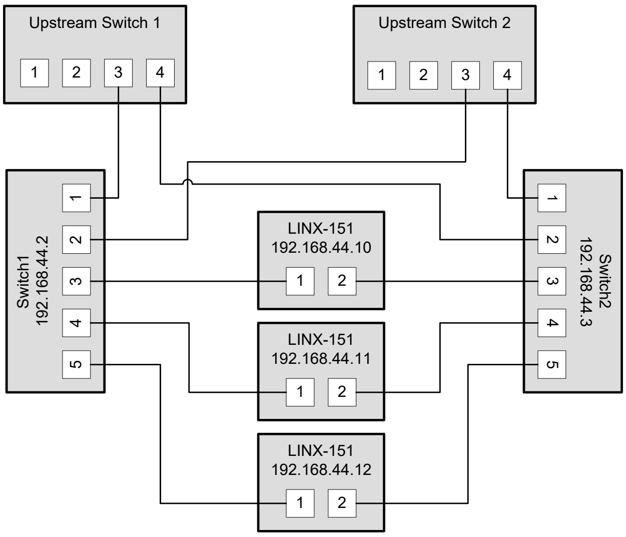


Figure 152: Fully redundant Ethernet topology

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 152, the L-IP 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 153, the L-IP 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.

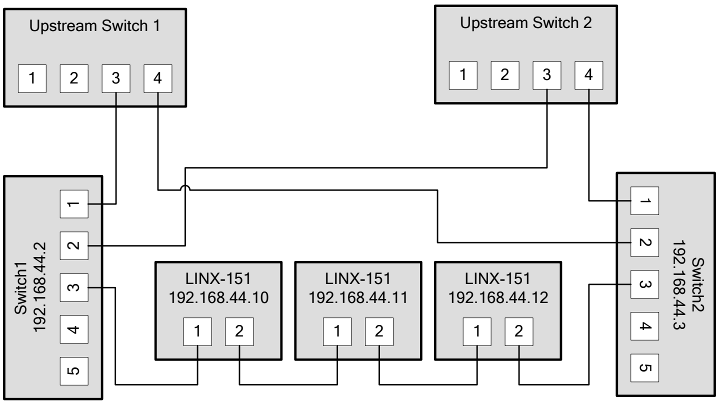


Figure 153: Ring Ethernet topology

12.4.2 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-IP 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 154.

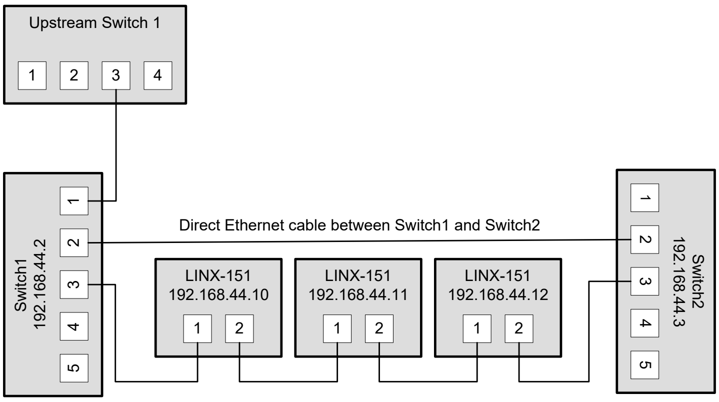


Figure 154: Single upstream connection.

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-IP 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 152.

12.4.3 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.

12.4.4 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.

12.4.5 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-IP 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-IP directly connected to Switch1.
    - The connection between Switch2 and the L-IP directly connected to Switch2.
    - A connection in the L-IP chain which is not connected directly to either Switch1 or Switch2.

12.4.6 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 152.

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
```

12.5 WLAN

12.5.1 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.

12.5.2 802.11s 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.

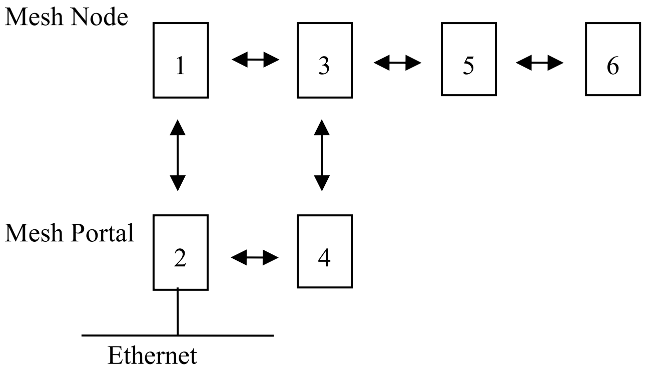


Figure 155: Mesh Networking

Figure 155 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.

12.5.3 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.

13 L-IP Firmware Update

The L-IP firmware supports remote upgrade over the network and the serial console.

To guarantee that the L-IP cannot be destroyed due to a failed firmware update the L-IP firmware consists of two images:

- Fall-back image
- L-IP application image

The fall-back image is write protected in flash memory and provides everything needed to talk to the L-IP platform over the network. The L-IP application image is designed to be updated over the network whenever there is a need to do so.

The fall-back image makes sure that the L-IP comes up in a status where the maintenance software can at least talk to the L-IP platform and can download a new L-IP application image.

When the L-IP boots up with the fall-back image, all port LEDs are flashing red. In this state it does not forward any messages.

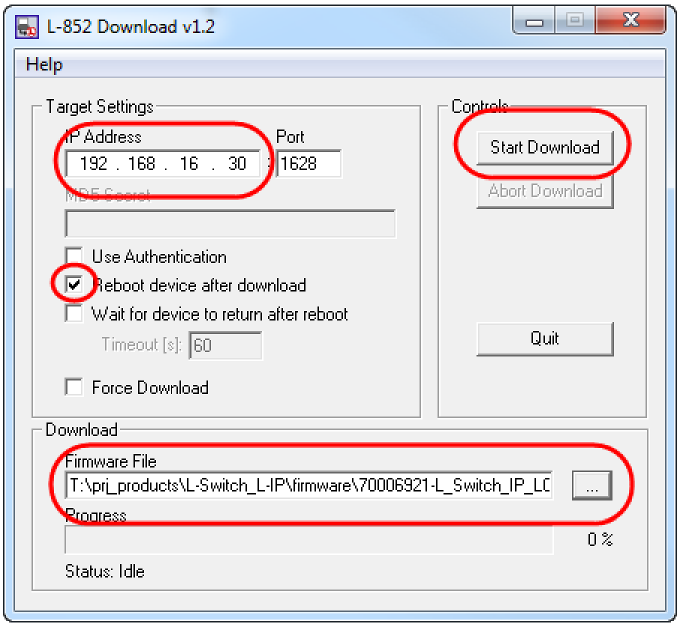
13.1 Firmware Update via the Web Interface

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 see Section 7.6.2. This is the preferred method for L-IP series “C” models.

13.2 Firmware Update via the IP Network

To download the firmware via the IP network the L-IP must have a valid IP configuration (see Section 5.2). You will need the LOYTEC L-852 Download Tool, which can be downloaded from our homepage at www.loytec.com.

When running the software the window shown in Figure 156 appears. Enter the **IP Address** of the L-IP you want to update, choose the firmware *.dl in the field **Firmware File**, optionally check the check-box **Reboot device after download** and press the button **Start Download**.



IP Address: 192 . 168 . 16 . 30
Port: 1628

□ Use Authentication
☑ Reboot device after download
□ Wait for device to return after reboot
Timeout [s]: 60
□ Force Download

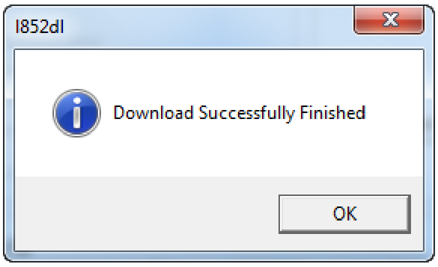
Firmware File: T:\prj_products\L-Switch_L-IP\firmware\70006921-L_Switch_IP_LC

Progress: 0 %

Status: Idle

Figure 156: The L-852 Download Tool

If the upgrade is successful the following window appears (Figure 157).



Download Successfully Finished

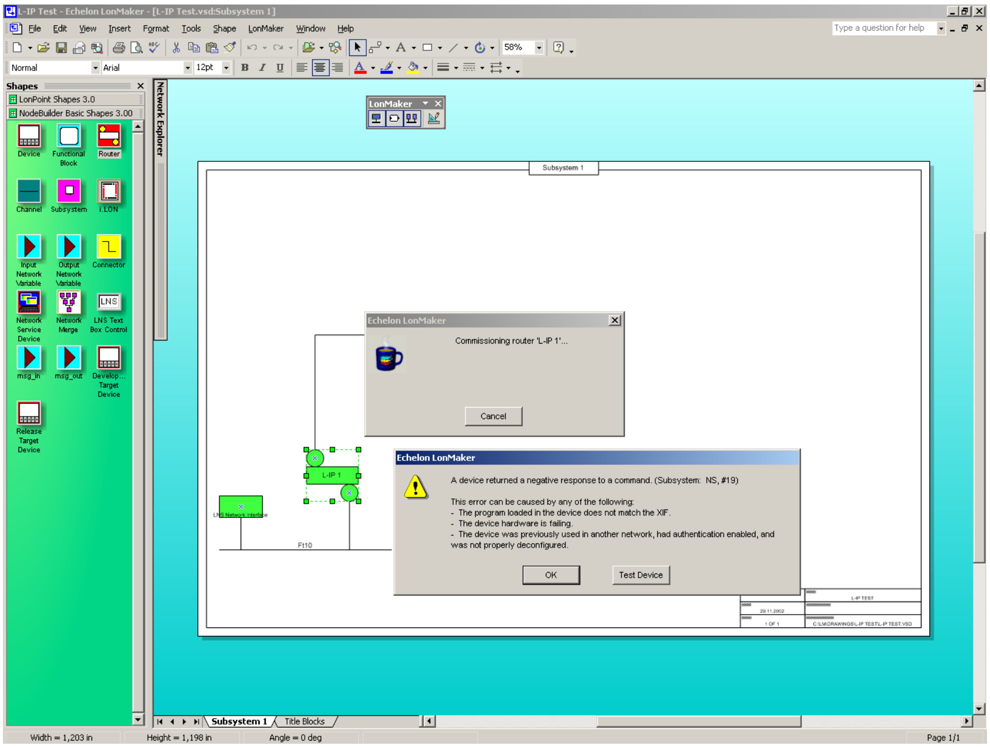
Figure 157: Successful firmware upgrade.

14 Troubleshooting

14.1 When commissioning the L-IP LonMaker responds with an error

Problem

LonMaker reports an error when commissioning the L-IP as shown in Figure 158.



Echelon LonMaker

Commissioning router 'L-IP 1'...

Cancel

Echelon LonMaker

A device returned a negative response to a command. (Subsystem: NS, #19)

This error can be caused by any of the following:
- The program loaded in the device does not match the XIF.
- The device hardware is failing.
- The device was previously used in another network, had authentication enabled, and was not properly deconfigured.

OK Test Device

Figure 158: LonMaker fails to commission the L-IP router.

Explanation

The L-IP is not configured as a CEA-709 configured router.

Solution

Please make sure to set the DIP-switches according to Figure 87 as CEA-709 configured router and reboot the L-IP. If the L-IP is used in smart switch mode simply do not commission the L-IP.

If the problem still persists please contact LOYTEC support (see Section 14.8).

14.2 L-IP packet routing fails if Channel Timeout is activated

Problem

The L-IP stops routing packets if a Channel Timeout >0ms is specified.

Explanation

Most likely the local clocks are not synchronized and the stale packet detection might drop all packets received from other L-IPs.

Solution

Make sure that a proper Channel Timeout according Table 6 and that at least one SNTP server is specified for the IP-852 channel. If the L-IP is operated behind a firewall make sure that the firewall doesn’t block SNTP requests at port 123.

14.3 Default Gateway Address is wrong

Problem

The L-IP reports the error “Can’t set default route:” during the boot process.

```
LOYTEC electronics GmbH
www.loytec.com

Testing Board ID (0E)                                      Passed
Testing RAM                                                Passed
Testing boot loader                                        Passed
Testing fallback image                                     Passed
Testing primary image                                      Passed
Testing Flash                                              Passed

Loading primary image                                      Passed

Starting application                                       Passed

Port 1 detected (FT-10)                                    Passed

Can’t set default route: Network is unreachable
Starting TCP/IP networking (Timeout)                       Failed
```

Explanation

The default gateway address is set to a wrong address or to an address that doesn’t exist.

Solution

In the configuration menu “[5] IP configuration” select item “[4] IP Gateway” and enter a valid gateway address. Even if you don’t use a gateway enter the gateway address for this subnet e.g. IP address: 192.168.1.34 => Gateway Address: 192.168.1.1.

14.4 TP-1250 port does not work

Problem

Messages are not forwarded to or from the TP-1250 port(s). All other ports work properly.

Explanation

This problem might be due to mixing backbone mode and non-backbone mode devices on one channel.

Solution

If the TP-1250 channel is used in backbone mode make sure all devices on the network have backbone mode enabled, only L-IP or L-Switch devices are connected to this backbone and every L-IP/L-Switch has a unique station ID set.

If the TP-1250 channel is not used in backbone mode make sure that all L-IP and L-Switch devices on that channel have the backbone mode disabled.

14.5 CEA-709 Activity LED is flashing red

Problem

The CEA-709 activity LED is flashing red whenever there is traffic on the channel (instead of green).

Explanation

The L-IP has a built-in network analysis functionality (see Section 6.4.10): Whenever it detects a potential problem on one port, the activity LED will change its color to red.

Solution

Most likely this behavior is due to a wiring problem. Check the wiring and termination of the network connected to the affected port. If this does not solve your problem use a protocol analyzer (e.g. LOYTEC’s LPA) and/or a network diagnostics tool (e.g. LOYTEC’s LSD Tool or Echelon’s Nodeutil) to find the source of the problem.

14.6 The CEA-709 activity LED and the status LED are flashing red

Problem

The CEA-709 activity LED and the status LED are flashing red at a rate of approx. once per second and the L-IP does not forward any messages.

Explanation

Somehow the primary image was destroyed and the fall-back image was booted (see Section 7). This image does not support forwarding of messages. It only allows downloading a new firmware.

Solution

If this problem occurs because a firmware update was attempted (and failed somehow), simply retry downloading the new firmware image.

If no firmware update was attempted, please contact LOYTEC support (see Section 14.8).

14.7 IP-852 traffic may flood the entire switched IP network

Problem

In a setup where CNIP routers are used to send data in one direction only (unacknowledged services), the receiving CNIP router never sends out any data, therefore its position in the network becomes unknown after a while (due to the aging mechanism of Ethernet switches) and the traffic is then flooded to the entire network.

Explanation

Ethernet switches use an aging mechanism to store and manage Ethernet MAC addresses. After some time the switch forgets the MAC address and forwards the Ethernet packets with the forgotten MAC address to all ports.

Solution

Please activate the keep alive function on the configuration server to establish two-way communication with the CNIP router.

14.8 Technical Support

LOYTEC offers free telephone and e-mail support for our L-IP 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

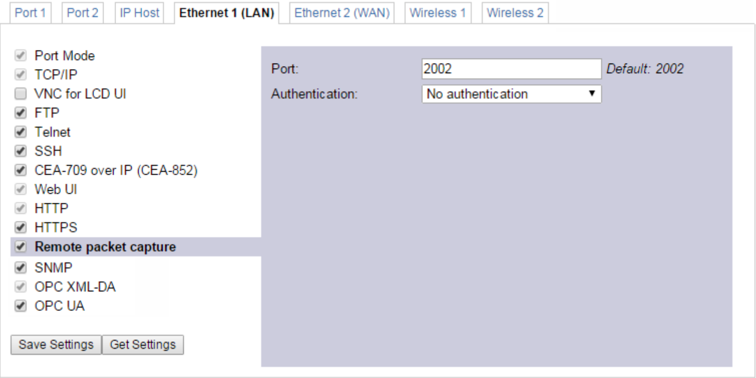
LOYTEC Americas Inc.
N27 W23957 Paul Road
Suite 103
Pewaukee, WI 53072
USA

e-mail:	***support@loytec-americas.com***
Web:	***http://www.loytec-americas.com***
tel:	***+1 (512) 402 5319***
fax:	***+1 (262) 408 5238***

14.9 Packet Capture

14.9.1 Configure Remote Packet Capture

Remote packet capture is able to capture packets on the Ethernet port. To enable the remote packet capture feature, go to the **Ethernet** port configuration and enable **Remote packet capture** as shown in Figure 159.


Port 1 | Port 2 | IP Host | **Ethernet 1 (LAN)** | Ethernet 2 (WAN) | Wireless 1 | Wireless 2

- ☑ Port Mode
- ☑ TCP/IP
- □ VNC for LCD UI
- ☑ FTP
- ☑ Telnet
- ☑ SSH
- ☑ CEA-709 over IP (CEA-852)
- ☑ Web UI
- ☑ HTTP
- ☑ HTTPS
- ☑ **Remote packet capture**
- ☑ SNMP
- ☑ OPC XML-DA
- ☑ OPC UA

Port:	2002	*Default: 2002*
Authentication:	No authentication ▾	

Save Settings | Get Settings

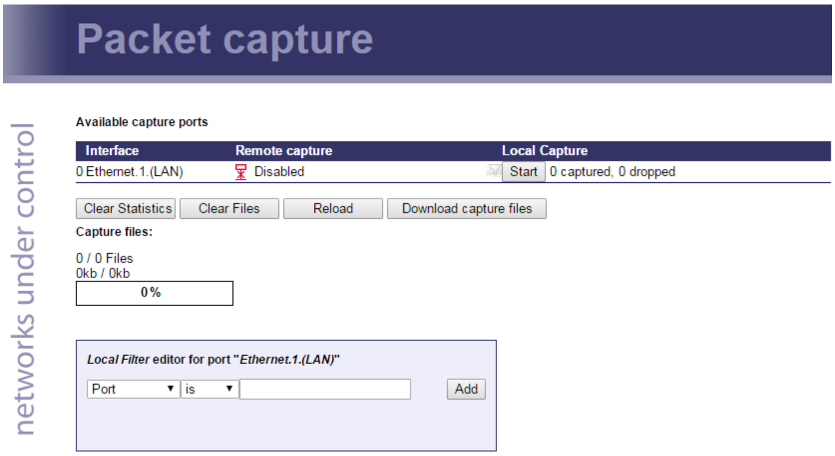
Figure 159: Remote packet capture port configuration.

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.

14.9.2 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 160**.**



Packet capture

Available capture ports

Interface	Remote capture	Local Capture
0 Ethernet.1.(LAN)	Disabled	Start 0 captured, 0 dropped

Clear Statistics | Clear Files | Reload | Download capture files

Capture files:

0 / 0 Files
0kb / 0kb
0%

Local Filter editor for port "*Ethernet.1.(LAN)*"

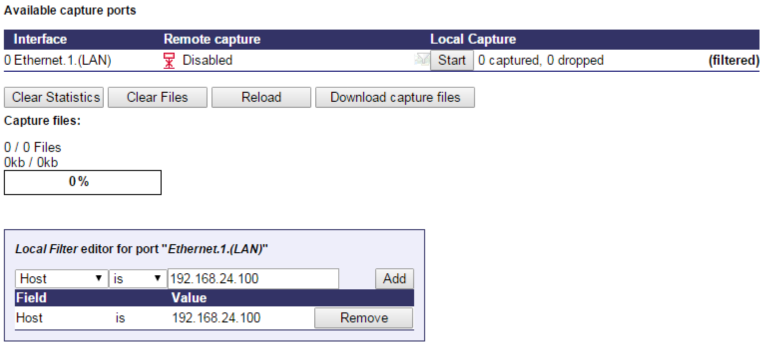
Port ▾ | is ▾ | | Add

Figure 160: Packet capture statistics.

Verify that the Ethernet ports are listed in the **Available capture ports** table and that the **Remote capture** status for these ports reads **Disconnected**.

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. Finally click on **Save Filters** to store and activate the local capture filters. Figure 161 shows an example filter for packets with IP address 192.168.24.100.



Available capture ports

Interface	Remote capture	Local Capture	
0 Ethernet.1.(LAN)	Disabled	Start 0 captured, 0 dropped	(filtered)

Capture files:

0 / 0 Files
0kb / 0kb
0%

Local Filter editor for port "*Ethernet.1.(LAN)*"

Host ▾ is ▾ 192.168.24.100 Add

Field		Value	
Host	is	192.168.24.100	Remove

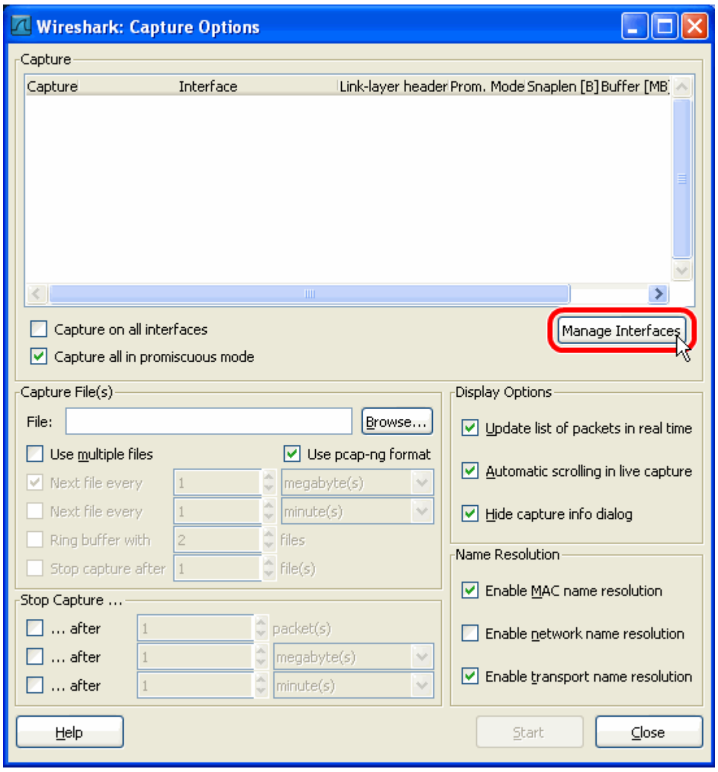
Figure 161: Adding local Ethernet capture filters.

14.9.3 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 162.



☐ Capture on all interfaces
☑ Capture all in promiscuous mode

☐ Use multiple files
☑ Use pcap-ng format
☑ Next file every 1 megabyte(s)
☐ Next file every 1 minute(s)
☐ Ring buffer with 2 files
☐ Stop capture after 1 file(s)

☐ ... after 1 packet(s)
☐ ... after 1 megabyte(s)
☐ ... after 1 minute(s)

☑ Update list of packets in real time
☑ Automatic scrolling in live capture
☑ Hide capture info dialog

☑ Enable MAC name resolution
☐ Enable network name resolution
☑ Enable transport name resolution

Figure 162: 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 163.

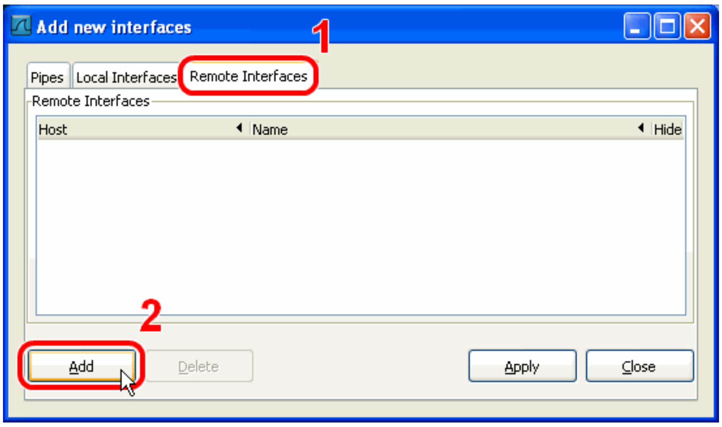
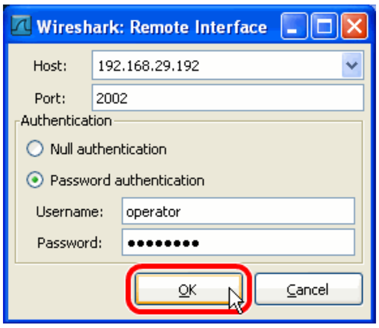


Figure 163: Wireshark Add New Interfaces Dialog.

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 164.

5. Note that only the users **admin** and **operator** are allowed to connect.



Wireshark: Remote Interface

Host: 192.168.29.192

Port: 2002

Authentication

○ Null authentication

● Password authentication

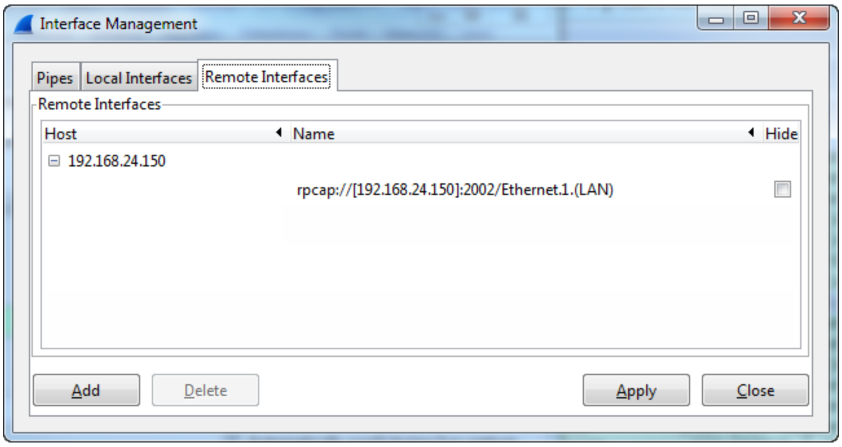
Username: operator

Password: ••••••••

Figure 164: 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 165.



Interface Management

Remote Interfaces

Host	Name	Hide
⊟ 192.168.24.150		
	rpcap://[192.168.24.150]:2002/Ethernet.1.(LAN)	□

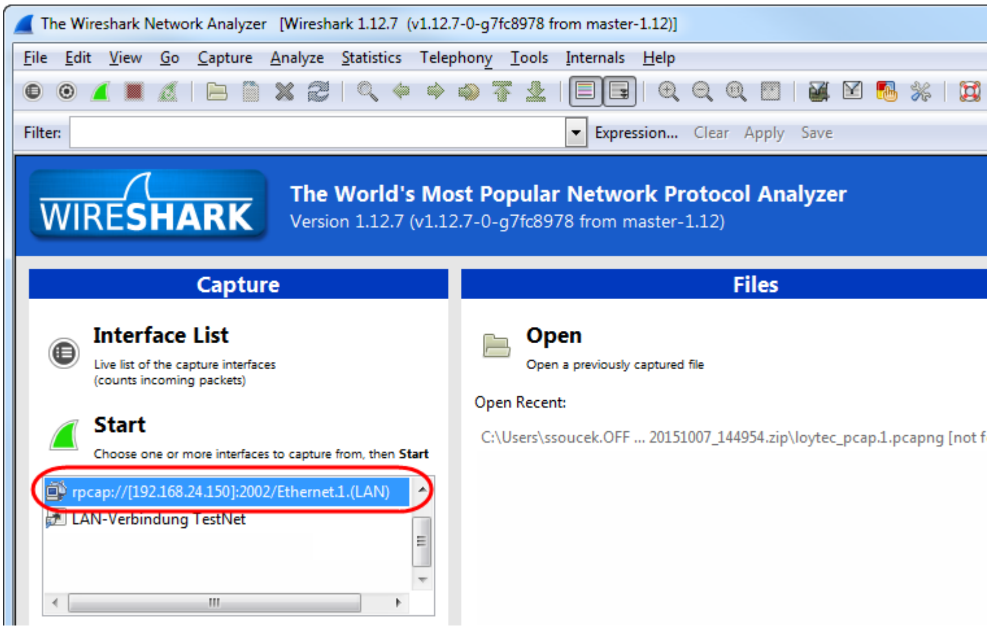
Figure 165: Added new interface to Wireshark.

8. **Close** the window 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 capture.

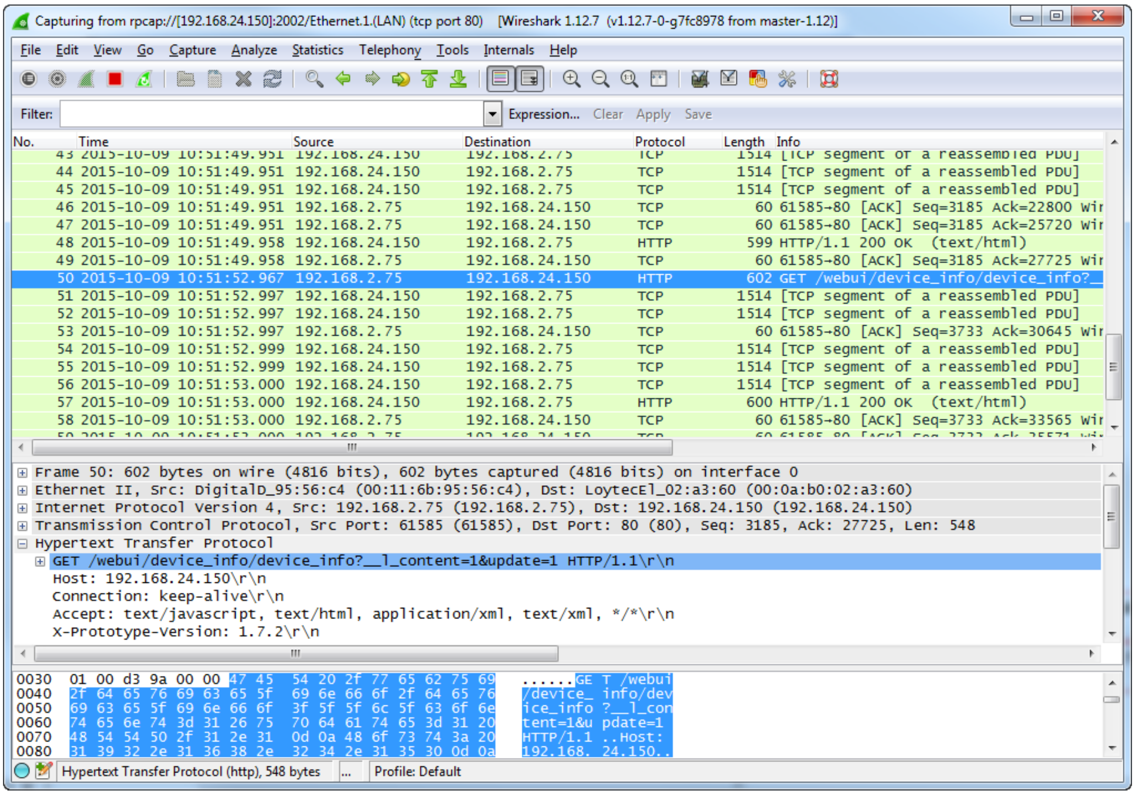
2. Click the **Start** button as shown in Figure 166.



The Wireshark Network Analyzer [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
rpcap://[192.168.24.150]:2002/Ethernet.1.(LAN)
LAN-Verbindung TestNet
Files
Open
Open a previously captured file
Open Recent:
C:\Users\ssoucek.OFF ... 20151007_144954.zip\loytec_pcap.1.pcapng [not f

Figure 166: 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 167.



Capturing from rpcap://[192.168.24.150]:2002/Ethernet.1.(LAN) (tcp port 80) [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time                     Source          Destination     Protocol  Length Info
  43 2015-10-09 10:51:49.951 192.168.24.150  192.168.2.75    TCP       1514 [TCP segment of a reassembled PDU]
  44 2015-10-09 10:51:49.951 192.168.24.150  192.168.2.75    TCP       1514 [TCP segment of a reassembled PDU]
  45 2015-10-09 10:51:49.951 192.168.24.150  192.168.2.75    TCP       1514 [TCP segment of a reassembled PDU]
  46 2015-10-09 10:51:49.951 192.168.2.75    192.168.24.150  TCP         60 61585→80 [ACK] Seq=3185 Ack=22800 Wir
  47 2015-10-09 10:51:49.951 192.168.2.75    192.168.24.150  TCP         60 61585→80 [ACK] Seq=3185 Ack=25720 Wir
  48 2015-10-09 10:51:49.958 192.168.24.150  192.168.2.75    HTTP       599 HTTP/1.1 200 OK  (text/html)
  49 2015-10-09 10:51:49.958 192.168.2.75    192.168.24.150  TCP         60 61585→80 [ACK] Seq=3185 Ack=27725 Wir
  50 2015-10-09 10:51:52.967 192.168.2.75    192.168.24.150  HTTP       602 GET /webui/device_info/device_info?_
  51 2015-10-09 10:51:52.997 192.168.24.150  192.168.2.75    TCP       1514 [TCP segment of a reassembled PDU]
  52 2015-10-09 10:51:52.997 192.168.24.150  192.168.2.75    TCP       1514 [TCP segment of a reassembled PDU]
  53 2015-10-09 10:51:52.997 192.168.2.75    192.168.24.150  TCP         60 61585→80 [ACK] Seq=3733 Ack=30645 Wir
  54 2015-10-09 10:51:52.999 192.168.24.150  192.168.2.75    TCP       1514 [TCP segment of a reassembled PDU]
  55 2015-10-09 10:51:52.999 192.168.24.150  192.168.2.75    TCP       1514 [TCP segment of a reassembled PDU]
  56 2015-10-09 10:51:53.000 192.168.24.150  192.168.2.75    TCP       1514 [TCP segment of a reassembled PDU]
  57 2015-10-09 10:51:53.000 192.168.24.150  192.168.2.75    HTTP       600 HTTP/1.1 200 OK  (text/html)
  58 2015-10-09 10:51:53.000 192.168.2.75    192.168.24.150  TCP         60 61585→80 [ACK] Seq=3733 Ack=33565 Wir
```

```
⊞ Frame 50: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface 0
⊞ Ethernet II, Src: DigitalD_95:56:c4 (00:11:6b:95:56:c4), Dst: LoytecEl_02:a3:60 (00:0a:b0:02:a3:60)
⊞ Internet Protocol Version 4, Src: 192.168.2.75 (192.168.2.75), Dst: 192.168.24.150 (192.168.24.150)
⊞ Transmission Control Protocol, Src Port: 61585 (61585), Dst Port: 80 (80), Seq: 3185, Ack: 27725, Len: 548
⊟ Hypertext Transfer Protocol
  ⊞ GET /webui/device_info/device_info?__l_content=1&update=1 HTTP/1.1\r\n
    Host: 192.168.24.150\r\n
    Connection: keep-alive\r\n
    Accept: text/javascript, text/html, application/xml, text/xml, */*\r\n
    X-Prototype-Version: 1.7.2\r\n
```

```
0030  01 00 d3 9a 00 00 47 45  54 20 2f 77 65 62 75 69   ......GE T /webui
0040  2f 64 65 76 69 63 65 5f  69 6e 66 6f 2f 64 65 76   /device_ info/dev
0050  69 63 65 5f 69 6e 66 6f  3f 5f 5f 6c 5f 63 6f 6e   ice_info ?__l_con
0060  74 65 6e 74 3d 31 26 75  70 64 61 74 65 3d 31 20   tent=1&u pdate=1 
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ..Host: 
0080  31 39 32 2e 31 36 38 2e  32 34 2e 31 35 30 0d 0a   192.168. 24.150..
```

Figure 167: Example Ethernet remote capture in progress.

15 Application Notes

Please refer to the application notes listed in Table 8 for further information on using the L-IP in different application scenarios.

Application Note	Topic
AN002E LSD Tool	How to use the enhanced statistic features of the L-IP with the LOYTEC system diagnostics tool (LSD tool)
AN003E L-IP and LNS	How to use the L-IP with LonMaker and other network management tools
AN005E L-Switch XP with L-IP Backbone	This document shows how to combine L-Switches with an L-IP (Ethernet) backbone.
AN007E Network Infrastructure	This application note provides information on how to use LOYTEC network infrastructure products (L-Switch, L-IP, L-Proxy, and NIC) together with LOYTEC network interfaces in different example use cases. It also explains how the different operating modes of the devices work and which operating mode should be chosen for specific applications.

Table 8: L-IP related application notes.

16 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.

16.1 Installation Instructions

Install the device over the Web interface:

- Set up the basic device functions and protocol settings as described in Section 5.2 and 7.3. When connecting over the Web UI use https:// in the URL.
- Change the default admin password to a secure password as described in Section 7.1. As of firmware 8.4.0 strong passwords are enforced.
- Disable the HTTP service in the IP port configuration as described in Section 7.3.3.
- Create a new HTTPS server certificate as described in Section 7.4.2.
- Set a password for the “guest” user or disable the guest user to protect information of the device info page from unwanted disclosure.

16.2 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 13. 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.

There exists exactly one firmware image for all L-IP models. The firmware has built-in auto-detection of the fieldbus ports the device is equipped with. It adds virtual routers to an internal channel. For the function of the device on the IP side this makes absolutely no difference, as the IP connection is also tapped on to this internal channel.

16.3 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:

- 1628 udp/tcp: This is the data exchange port for CEA-852 (LON over 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.

- 1629 udp/tcp: This is the configuration server port of CEA-852. Exactly one device in the system needs this port open. Other devices register with the configuration server to form the IP-852 channel list. 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 16.1:

- 21 tcp: This port is opened by the FTP server. This port is disabled by default.
- 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. This port is disabled by default .
- 80 tcp: This port is opened by the Web server. It can be disabled.
- 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.
- 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.

16.4 Services

Required services:

- CEA-852 (LON over IP): Primary function of the device. This service is in accordance with the standard ANSI/CEA-852-B.

Optional services not necessary for the primary product function. They can be disabled as described in the installation instructions in Section 16.1:

- 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 and Telnet: The FTP and Telnet server is used for connection to the device for remote configuration (L-WEB), firmware upgrade, and access to the log file. The service is disabled by default.
- SSH: SSH server. It provides secure access to the device console menu over the network, firmware upgrade, and access to the log file.
- HTTPS: Secure Web server. It provides a Web-based configuration UI using HTTPS. It is also used for connection to the device for remote configuration (L-WEB), firmware upgrade, and access to the log file.
- 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.

16.5 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 Section 7.4.2 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 Section 7.3.16 on how to upgrade your RSA key to 2048 bits.

16.6 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 LOYTEC 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.
- Commission of the CEA-709 node/router.
- Static errors in the device and its configuration.
- System overload situations as one-time log messages since last power-on.
- Crucial communication errors as they occur.
- Logins and login failures.
- Failed firmware upgrade attempts.

16.7 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.

16.8 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.

16.9 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.

16.10Information Policy

LOYTEC follows a policy for reporting, documenting an 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.
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.

17 Specifications

17.1 Physical Specifications

17.1.1 LIP-xxECRB

Operating Voltage	12-35 VDC or 12-24 VAC ±10%
Power Consumption	typ. 3 W
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	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

17.1.2 LIP-3ECTC, LIP-33ECTC, LIP-13ECTC

Operating Voltage	12-35 VDC or 12-24 VAC ±10%
Power Consumption	typ. 3 W
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

17.1.3 LIP-3333ECTC

Operating Voltage	12-35 VDC or 12-24 VAC ±10%
Power Consumption	typ. 3 W
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

17.2 FCC Warning

This device has been tested and found to comply with limits for a Class B digital device, pursuant to Part 2 and 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates and radiates radio frequency energy and, if not installed and used in accordance with the user’s manual, it may cause interference in which case users will be required to correct interference at their own expenses.

17.3 CE Warning

This is a Class B product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

18 Revision History

Date	Version	Author	Description
2002-07-11	1.0	DL	Initial revision V1.0
2003-01-17	1.1	DL	Added menu item 9 (device statistics) in Section 4.10 Improved behavior of cnip LED in Section 3.4.7 Added automatic IP connection keep-alive in Section 4.6.8
2003-05-09	2.0	DL	Add Section 2.3 IP Configuration for Client Device via Web-Interface Add Section 4.4.3 Option 8 – Webserver Add Section 4.4.4 Option 9 - Change Web server Password Changed menu in Section 4.5 EIA 709 Configuration Menu Rewrite Section 4.5.1 and Section 4.5.2. Add Section 4.7.10 Option 9 - Location string Add Section 4.8.7 Option 7 - Auto members support Add Section 4.8.8 Option 8 - Roaming members support Add Section 4.8.15 Option s - Show device statistics Add Section 4.8.17 Option r - Recontact devices & list channel members Add new device states to Table 14 Add flags to Figure 35: List all CN/IP channel members. Add Chapter 5 Web Interface Add Section 4.4.2.3 Option 3 - Set router configuration according to DIP switch Add Section 7.9 Remote LPA Operation Rewrite Section 7.11.3 DHCP
2003-09-15	2.1	DL	Added note about PC NTP client to Section 7.10.1 Add Section 11.7 IP-852 traffic may flood the entire switched IP network Corrected information on controlling RS-485 bit-rate auto-detection with DIP switch, see Section 3.6 Add route command starting with firmware version 2.1 in Section 2.3 and Section 5.1. Add Section 4.10.6 Option 6 - Enhanced Communications Test Add Enhanced Communications Test to Section 5.4
2004-04-15	2.2	JB	Updated for L IP 2.2
2004-09-21	3.0	STS	Added extended NAT, multi-cast, Auto-NAT, new enhanced communications test, new channel list in Web, i.LON 600. Corrected terminals 25, 26.
2005-04-19	4.3	STS	Updated manual for multi-port L-IP.
2005-09-22	4.4	JB	Updated manual for L-IP Redundant.
2006-06-27	4.5	JB	Updated manual for LIP-xxxxECTB.
2012-09-28	6.0	JB	Updated for firmware version 6.0. Remove information on legacy L-IP products. Updated images to show new enclosures. Updated to new manual design. Added Chapter “Security Hardening Guide”. Minor corrections.
2015-10-09	6.1	STS	Updated for firmware version 6.1. Added Section 1.2 L-IP Models. Added Chapter 2 What's in in L-IP. Chapter 4 refers to installation sheets, removed terminal layout, enclosure, product labels, DIP switches. Added Section 3.2.3 Configuration via the LCD display. Added Section 4.6 LCD display and jog dial. Added Section 6.2.5 Using Multiple IP Ports. Added Section 6.2.6 IP Host Configuration. Added Section 6.2.7 WLAN Configuration. Added Section 6.2.8 VNC Configuration. Added Section 6.2.14 Certificate Management. Added Section 6.2.15 Firmware. Added Section 6.2.16 SNMP. Added Section 6.2.17 Documentation. Updated 6.3.1 System Log. Added Section 6.4 Documentation. Added Section 10.1 SNMP Interface. Added Section 11.4 Redundant Ethernet. Added Section 11.5 WLAN. Added Section 12.1 Firmware Update via the Web Interface. Added Section 13.9 Packet Capture. Updated Chapter 15 Security Hardening Guide. Removed Chapter Firmware Versions.
2018-08-08	6.4	STS	Updated for firmware version 6.4. Section 6.2.1 language selection. Added Section 6.2.14 SSH Server Configuration. Updated Section 6.2.15 Certificate Management. Section 6.2.16 Documented backup before firmware download. Added Section 6.5.1 Safe Reboot. Updated Chapter 15 Security Hardening Guide.

2019-09-25	7.0	STS	Updated for firmware version 6.4. Added Section 6.2.19 VPN configuration. Updated Chapter 15 Security Hardening Guide.
2021-04-26	7.4	STS	Updated for firmware version 7.4. Removed Chapter Console interface. Chapter 7: Reorganized to match new menu structure. Section 7.1.1: Updated device setup and password enforcement. Section 7.3.5: Added 802.1X port authentication. Added Section 7.3.7 dynamic DNS. Section 7.3.18: Added description of the VPN tab. Section 7.3.19: Added LTE configuration. Updated Chapter 16 Security Hardening Guide.
2023-03-30	8.0	STS	Updated for firmware version 8.0. Section 7.3.8 + 7.3.9: WLAN tab updates (Client, AP, Mesh). Section 7.3.16 Added EC keys to SSH server. Section 7.4.2 Added EC key option to certificate management. Updated Chapter 16 Security Hardening Guide.
2024-01-05	8.2	STS	Updated for firmware version 8.2.
2024-06-15	8.2.8	STS	Updated for firmware version 8.2.8. Added model LIP-13ECTC. Added Section 5.4 Configure as LON Router drop-in replacement. Added Section 6.6.4 Router Mode LCD menu. Added Section 9.3 L-IP Acts as an L-Switch.
2025-06-16	8.4.0	STS	Updated for firmware version 8.4.0. Added 'loytec.local' method to Section 5.2.1. Updated Chapter 16 Security Hardening Guide.