

L-IPTM

EIA709/IP Router



User's Manual

LOYTEC

This page is intentionally left blank!

Contact

LOYTEC
Stolzenthalgasse 24/3
A-1080 Vienna
AUSTRIA/EUROPE
support@loytec.com
<http://www.loytec.com>

Version 4.5

Document No. 88065909

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.

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

L-Chip™, LC7093™ and L-IP™ are trademarks of LOYTEC electronics GmbH.

LonTalk®, LonWorks® and Neuron®, LonMaker, and LNS are trademarks of Echelon Corporation registered in the United States and other countries.

Contents

1	Introduction.....	13
1.1	Overview	13
1.1.1	L-IP	13
1.1.2	L-IP Redundant.....	15
1.2	Scope	16
2	Quick-Start Guide	17
2.1	Hardware installation	17
2.1.1	L-IP	17
2.1.2	L-IP Redundant.....	18
2.2	IP Configuration for Client Device via Console	20
2.3	IP Configuration for Client Device via Web-Interface	21
2.4	Configuration Server Settings	23
2.5	L-IP Redundant Configuration.....	24
3	Hardware Installation.....	26
3.1	Enclosure	26
3.1.1	L-IP	26
3.1.2	L-IP Redundant.....	28
3.2	Product Label	28
3.3	Mounting	29
3.4	LED signals	29
3.4.1	Power LED	29
3.4.2	Status LED.....	29
3.4.3	EIA-709 Activity LED	29
3.4.4	Twin Router Status LED (L-IP Redundant only).....	30
3.4.5	Ethernet Link LED	30
3.4.6	Ethernet Activity LED.....	30
3.4.7	EIA-852 Status LED (CNIP LED)	30
3.4.8	Configuration Server LED.....	31
3.4.9	Wink Action.....	31
3.4.10	Network Diagnostics	31
3.5	Status Button	32
3.5.1	Resetting Forwarding Tables.....	32

3.6	DIP Switch Settings.....	33
3.6.1	L-IP	33
3.6.2	L-IP Redundant.....	33
3.7	Power Supply.....	33
3.8	Terminal Layout	35
3.8.1	LIP-3ECT (FT-10).....	35
3.8.2	LIP-1ECT (TP-1250).....	35
3.8.3	LIP-33ECTB (2 x FT-10)	36
3.8.4	LIP-33ECRB (L-IP Redundant with FT-10)	36
3.8.5	LIP-3333ECTB (4 x FT-10)	37
3.9	Wiring.....	37
3.9.1	L-IP	37
3.9.2	L-IP Redundant.....	38
4	Console Interface	40
4.1	Console Connection.....	40
4.2	Self Test.....	40
4.3	L-IP Configuration Menu (Main Menu)	41
4.3.1	Option 1 - Show device information.....	42
4.3.2	Option 2 - Serial firmware upgrade	42
4.3.3	Option 3 - System configuration.....	42
4.3.4	Option 4 - EIA-709 configuration	42
4.3.5	Option 5 - IP configuration.....	42
4.3.6	Option 6 - EIA-852 client configuration	42
4.3.7	Option 7 - EIA-852 server configuration.....	43
4.3.8	Option 8 - Reset configuration (factory defaults).....	43
4.3.9	Option 9 - Device statistics.....	43
4.4	System Configuration Menu.....	43
4.4.1	Option 1 - Set date/time	43
4.4.2	Option 2 - Router mode	43
4.4.2.1	Option 1 - Enable Configured Router Mode (Default)	44
4.4.2.2	Option 2 - Enable Smart Switch Mode	44
4.4.2.3	Option 3 - Set router configuration according to DIP switch	45
4.4.3	Option 8 - Webserver.....	45
4.4.4	Option 9 - Change Web server Password	45
4.4.5	Option 0 - Web Server Port	46
4.5	EIA-709 Configuration Menu	46

4.5.1	Option 1 - Change transceiver configuration for Port 1	46
4.6	IP Configuration Menu.....	46
4.6.1	Option 1 - DHCP/BOOTP	47
4.6.2	Option 2 - IP Address, 3 - IP Netmask, 4 - IP Gateway	48
4.6.3	Option 5 - Hostname, 6 - Domainname	48
4.6.4	Option 7 - DNS Servers	48
4.6.5	Option 8 - NAT Address.....	48
4.6.6	Option 9 - MAC Address.....	49
4.6.7	Option 0 - Multicast Address.....	49
4.6.8	Option a - Connection Keep Alive	49
4.6.9	Option b - Link Speed & Duplex.....	50
4.7	EIA-852 Device Configuration Menu.....	50
4.7.1	Option1 - Config server address, 2 - Config server port	51
4.7.2	Option 3 - Config client port	51
4.7.3	Option 4 - Device name	51
4.7.4	Channel Mode.....	51
4.7.5	SNTP server, channel timeout	51
4.7.6	Option 5 - Escrow timeout.....	51
4.7.7	Option 6 - Aggregation Timeout	51
4.7.8	Option 7 - MD5 authentication.....	51
4.7.9	Option 8 - MD5 secret	52
4.7.10	Option 9 - Location string	52
4.8	EIA-852 Server Configuration Menu.....	52
4.8.1	Option 1 - Config server status.....	53
4.8.2	Option 2 - Config server port.....	53
4.8.3	Option 3 - Channel name	53
4.8.4	Item Channel Mode	53
4.8.5	Option 4 - Primary SNTP server, 5 - Secondary SNTP server.....	53
4.8.6	Option 6 - Channel Timeout	54
4.8.7	Option 7 - Auto members support	54
4.8.8	Option 8 - Roaming members support.....	54
4.8.9	Option 9 - MD5 authentication.....	54
4.8.10	Option 0 - MD5 secret.....	55
4.8.11	Option a - Add device	55
4.8.12	Option e - Edit device.....	55

4.8.13	Option d - Delete device.....	56
4.8.14	Option n - Enable/Disable device.....	56
4.8.15	Option s - Show device statistics.....	56
4.8.16	Option l - List channel members	56
4.8.17	Option r - Recontact devices & list channel members	57
4.9	Reset configuration (load factory defaults).....	57
4.9.1	Option 1 - Reset everything to factory defaults.....	58
4.9.2	Option 2 - Reset switch configuration to factory defaults.....	58
4.10	Device Statistics Menu.....	58
4.10.1	Option 1 - EIA852 device statistics.....	58
4.10.2	Option 2 - Extended EIA852 device statistics.....	59
4.10.3	Option 3 - Clear all EIA852 device statistics	59
4.10.4	Option 4 - IP statistics	60
4.10.5	Option 5 - Monitor Connection Keep Alive.....	61
4.10.6	Option 6 - Enhanced Communications Test.....	61
5	Web Interface.....	63
5.1	Start Screen and Account Management	63
5.2	Device Information.....	65
5.3	Device Configuration	66
5.3.1	EIA-852 Channel List.....	66
5.3.2	Backup/Restore the L-IP Configuration	67
5.4	Device Statistics	68
5.5	Reset, Contact, Logout	69
6	Operating Modes.....	70
6.1	EIA-709 Router - Operating Modes	70
6.1.1	Configured Router Mode	70
6.1.2	Smart Switch Mode	71
6.1.3	Repeater Mode.....	72
6.1.4	Smart Switch Mode with No Subnet Broadcast Flooding.....	73
6.2	EIA-852 Operating Modes	73
6.2.1	CN/IP Device	74
6.2.2	CN/IP Configuration Server	74
6.3	Firewall and NAT Router Configuration	75
6.3.1	Automatic NAT Configuration.....	75
6.3.2	Multiple L-IPs behind a NAT: Extended NAT Mode	76

6.3.3	Multiple L-IPs behind a NAT: Classic Method.....	78
6.4	Network Buffers	79
6.5	Multi-Cast Configuration	79
7	The L-IP in a Network	80
7.1	L-IP Acts as a Standard EIA-709 Configured Router	80
7.2	L-IP Acts as a Smart Switch.....	81
7.3	Creating and Managing a CN/IP Channel.....	81
7.4	Setting up an L-IP Device	82
7.4.1	Configuration Server Contacts L-IP Device.....	82
7.4.2	L-IP Device Contacts Configuration Server.....	83
7.5	Using the Built-In Configuration Server	83
7.6	Using the i.LON Configuration Server	84
7.7	Using L-IP in LNS (LonMaker) Networks	84
7.8	Using the L-IP as the Network Interface for LNS Applications	85
7.9	Remote LPA Operation	87
7.10	Internet Timing Aspects.....	88
7.10.1	Channel Timeout	89
7.10.2	Channel Delay	89
7.10.3	Escrowing Timer (Packet Reorder Timer).....	89
7.10.4	SNTP time server	89
7.11	Advanced Topics.....	90
7.11.1	Aggregation.....	90
7.11.2	MD5 Authentication.....	90
7.11.3	DHCP	90
7.11.4	Dynamic NAT Addresses.....	90
8	L-IP Redundant.....	92
8.1	Redundancy and Fault Detection in EIA709.1 Networks	92
8.1.1	Reasons for Communication Failures.....	92
8.1.2	Conventional Strategies for Redundancy	92
8.2	L-IP Redundant Operating Modes	93
8.2.1	Bus Loop Monitoring	93
8.2.2	Router Redundancy	94
8.2.3	Device and Network Monitoring.....	95
8.3	The L-IP Redundant in a Network	96
8.4	Installation.....	96

8.4.1	Installing the L-IP Redundant Plug-In.....	96
8.4.2	Registering the L-IP Redundant Plug-In	99
8.4.3	Adding the L-IP Redundant.....	100
8.4.3.1	L-IP Redundant Standalone	100
8.4.3.2	L-IP Redundant with Router Redundancy	101
8.5	L-IP Redundant Plug-In	103
8.5.1	Operation modes	103
8.5.1.1	On-line mode.....	103
8.5.1.2	Off-line mode	103
8.5.1.3	Standalone mode	103
8.5.2	Overview.....	103
8.5.3	Device Status	104
8.5.4	Channel Statistics.....	106
8.5.5	Alarm Log.....	108
8.5.6	Node List Config	110
8.5.6.1	Manually add and edit nodes	111
8.5.6.2	Import node list from LNS database	111
8.5.6.3	Change order of node list	112
8.5.6.4	Import/Export Node List.....	112
8.5.6.5	Downloading and Uploading the Node List.....	113
8.5.7	Parameters.....	114
8.6	Web Interface	117
8.6.1	Status.....	117
8.6.2	Channel Statistics.....	119
8.6.3	Alarm Log.....	119
8.6.4	Node List Configuration	120
8.6.5	Parameters.....	121
8.7	Network Interface.....	122
8.7.1	Node Object	122
8.7.2	Bus Loop Monitor Object.....	123
8.7.3	Device Monitor Object	124
8.7.4	Twin Router Object	125
8.7.5	Channel Monitor Objects.....	127
9	Network Media	131
9.1	TP-1250	131
9.2	FT-10	131
9.3	RS-485 Bit-Rate Auto-Detection	132
9.4	TP-1250 Collision-Less Backbone.....	133

10	L-IP Firmware Update.....	134
10.1	Firmware Update via the Network.....	134
10.2	Firmware Update via the Console.....	134
11	Troubleshooting.....	136
11.1	When commissioning the L-IP LonMaker responds with an error.....	136
11.2	L-IP packet routing fails if Channel Timeout is activated.....	137
11.3	Default Gateway Address is wrong	137
11.4	TP-1250 port does not work.....	138
11.5	EIA-709 Activity LED is flashing red	138
11.6	The EIA-709 activity LED and the status LED are flashing red	138
11.7	IP-852 traffic may flood the entire switched IP network.....	139
11.8	Technical Support	139
12	Application Notes	140
12.1	The LSD Tool	140
12.2	Using the L-IP with LNS based Installation Tools.....	140
12.3	L-IP Backbone Mode vs. a Standard TP-1250 Backbone	140
12.4	Using the L-Switch with an L-IP Backbone	140
13	Firmware Versions.....	141
14	Specifications.....	142
14.1	LIP-xECT.....	142
14.2	LIP-xECTB, LIP-xxECTB, and LIP-xxECRB	142
14.3	LIP-xxxxECTB	143
15	Revision History	144

Abbreviations

10BaseT	10 Mbps Ethernet network with RJ-45 plug
Aggregation	Collection of several EIA-709 packets into a single EIA-852 packet
BOOTP	Bootstrap Protocol, RFC 1497
CC	Configuration Client, also known as CN/IP Device
CN	Control Network
CN/IP	Control Network over IP
CN/IP Channel	logical IP channels that tunnels EIA-709 packets according EIA-852
CN/IP packet	IP packet that tunnels one or multiple EIA-709 packet(s)
CR	Channel Routing
CS	Configuration Server that manages EIA-852 IP devices
DHCP	Dynamic Host Configuration Protocol, RFC 2131, RFC 2132
DNS	Domain Name Server, RFC 1034
EIA-709	Protocol standard for control networks
EIA-852	Protocol standard for tunneling EIA-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 EIA-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 EIA-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 (EIA-852) and two FT-10 ports (EIA-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 EIA-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 3.4.10). 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 Section 12.1 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 Netscape. 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 EIA-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 EIA-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.

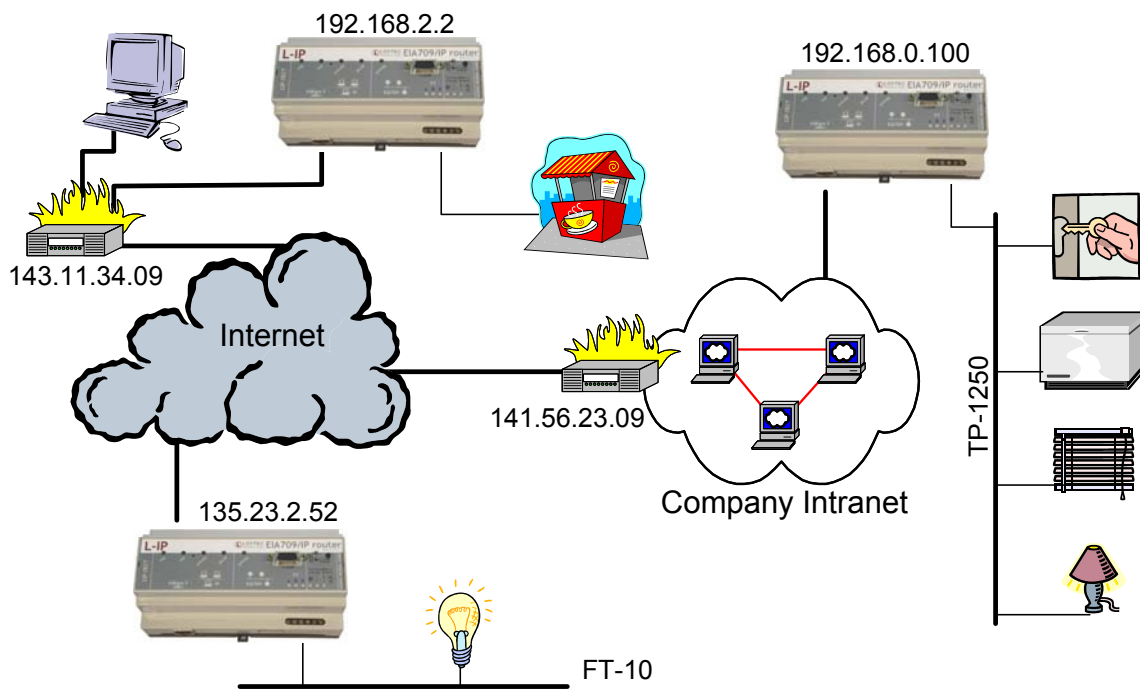


Figure 1: L-IP application example behind and without fire-walls and NAT routers.

The L-IP is used for:

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

1.1.2 L-IP Redundant

The L-IP Redundant EIA-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 to build redundant network infrastructure.

An L-IP Redundant EIA-709/IP Router can be used as a single device to achieve the redundancy on the EIA-709 (TP/FT-10) channel by building a ring structure. Full Redundancy on the IP-Channel¹ and on the EIA-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 EIA-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 EIA-709/IP Router can tunnel EIA-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 EIA-852 configuration server. If operated behind a router with network address translation (NAT or masquerading), the L-IP Redundant EIA-709/IP Router supports Auto-NAT to work with dynamic public IP addresses. When using the built in EIA-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 EIA-709/IP Router is ready to route packets between the EIA-709 network (ring structure) and the IP network. Thus, all EIA-709 networks connected to L-IP Routers can exchange data over the EIA-852 channel. If connected to untrusted networks, such as the Internet, all EIA-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 EIA-852 channel and EIA-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 EIA-709/IP

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

Router, setting up a redundant network which is comfortable to maintain becomes an easy task.

The L-IP Redundant is used for:

- ◆ Creating redundant EIA-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 EIA-709 network
- ◆ Determine location of a cable break
- ◆ Full redundancy with two L-IP Redundant EIA-709/IP Router in parallel for the IP-Channel and the EIA-709 channel
- ◆ Device redundancy by mutual monitoring of paired Redundant L-IPs
- ◆ Messages and alarming via SNVTs and LonMark-Alarming via Node Object

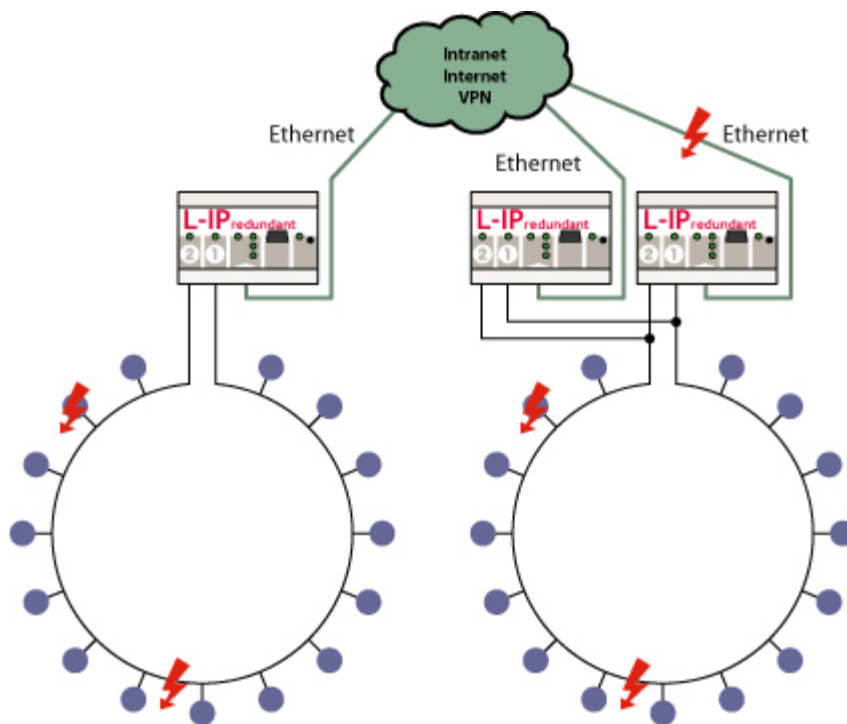


Figure 2: Using L-IP Redundant with redundant ring structure and device redundancy

1.2 Scope

This document covers L-IP devices with firmware version 4.5. See Section 13 for differences between the different L-IP firmware versions.

2 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.

2.1 Hardware installation

2.1.1 L-IP

Connect power 9-35 VDC or 12-24 VAC, the EIA-709 network, and the Ethernet cable as shown in Figure 3. More detailed instructions are shown in Chapter 3.

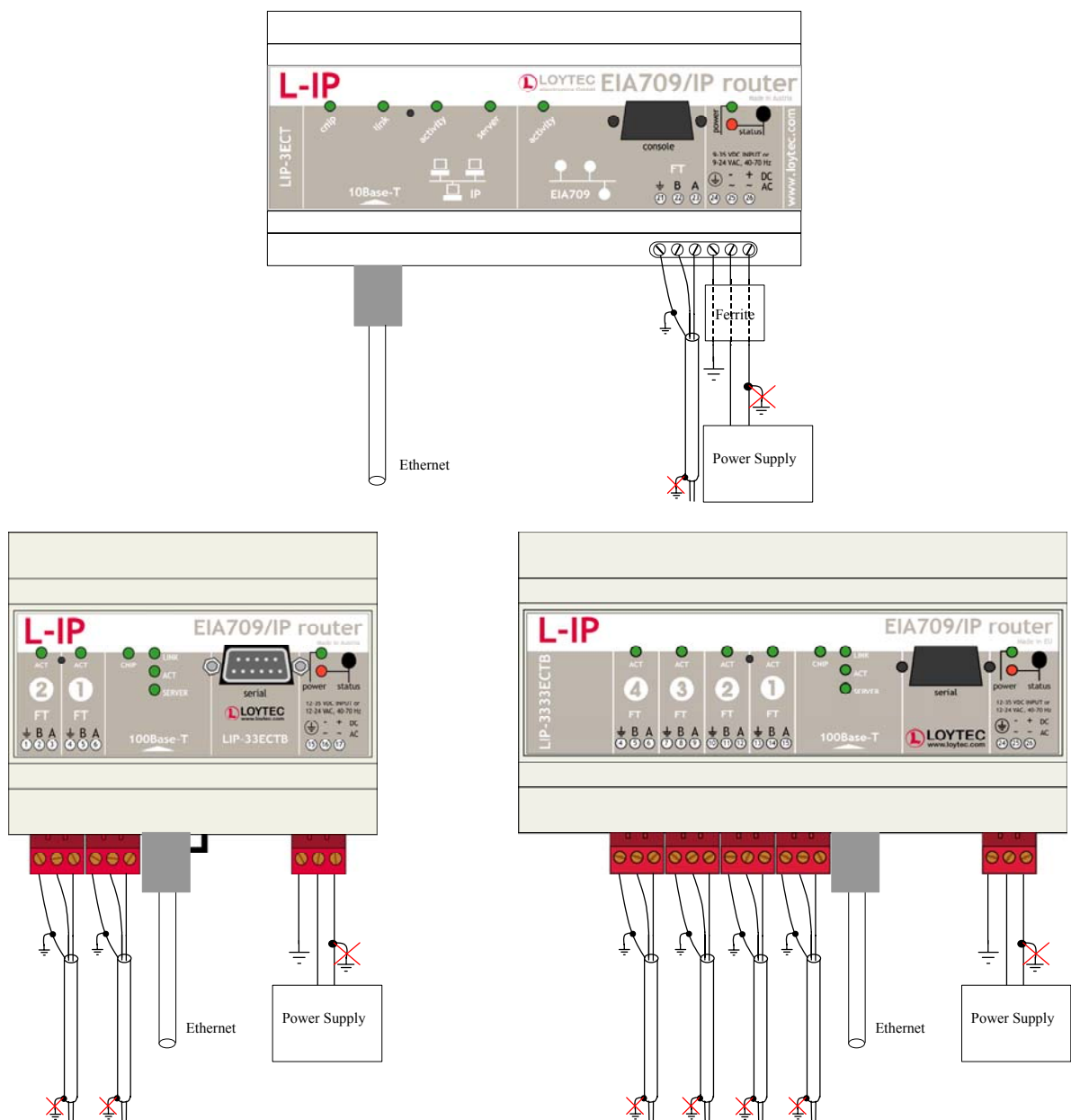


Figure 3: Basic Hardware installation.

Important: Do not connect terminal 26 (LIP-xECT and LIP-xxxxECTB) or terminal 17 (LIP-xECTB and LIP-xxECTB) with ground!

2.1.2 L-IP Redundant

Connect power 12-35 VDC or 12-24 VAC, the Ethernet cable and the EIA-709 network depending on the desired redundancy mode as shown in Figure 4 and Figure 5 to Figure 7. More detailed instructions are shown in Chapter 3.

Important: Do not connect terminal 17 to ground!

Important: When using shielded network cables connect the cable shield only to one port of the L-IP Redundant (terminal 1 or terminal 4)!

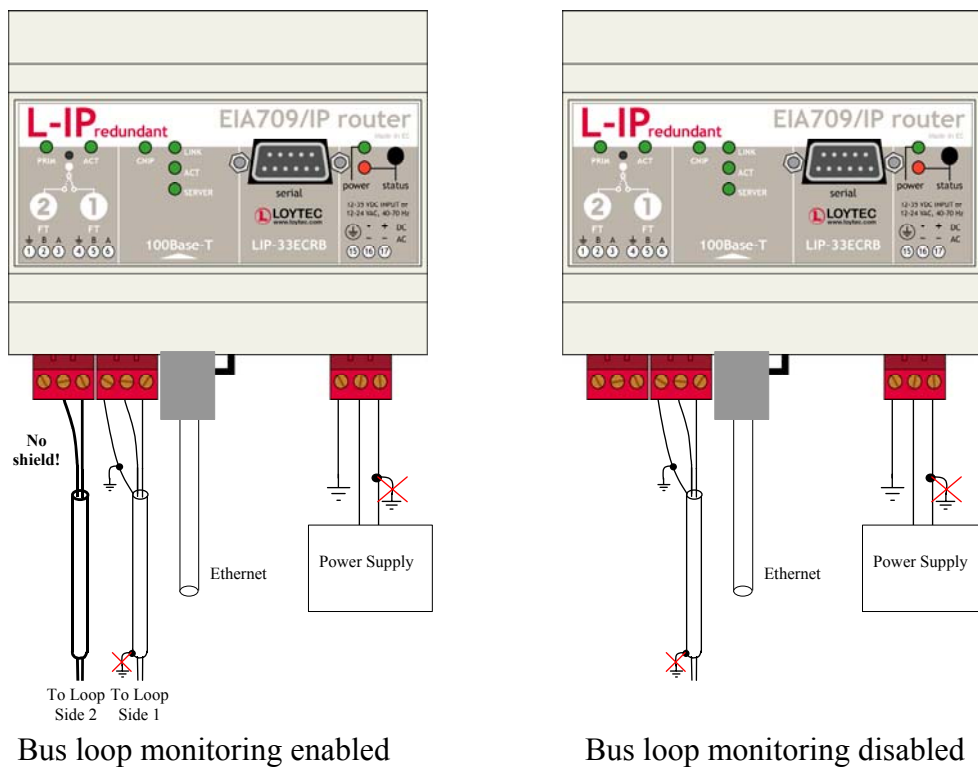


Figure 4: L-IP Redundant with and without Bus Loop Monitoring

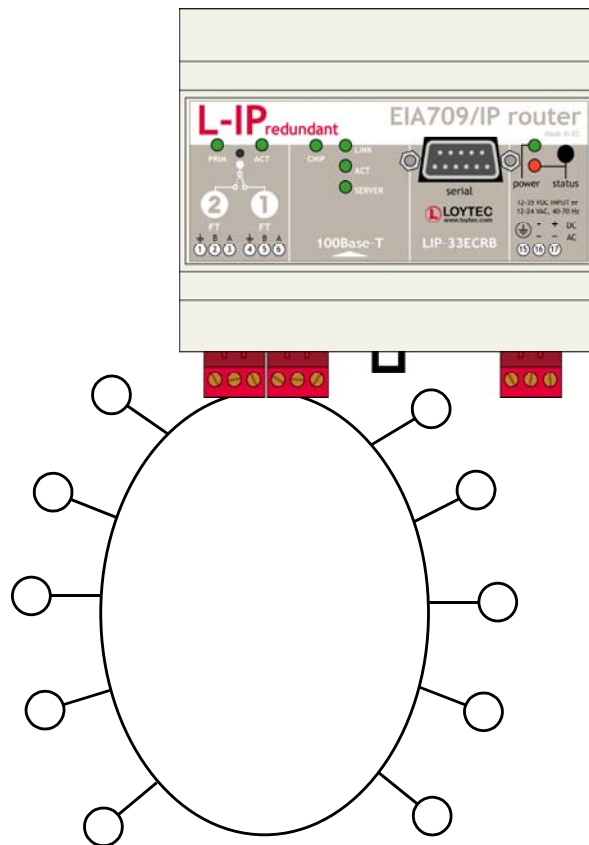


Figure 5: L-IP Redundant Standalone with Bus Loop Monitoring

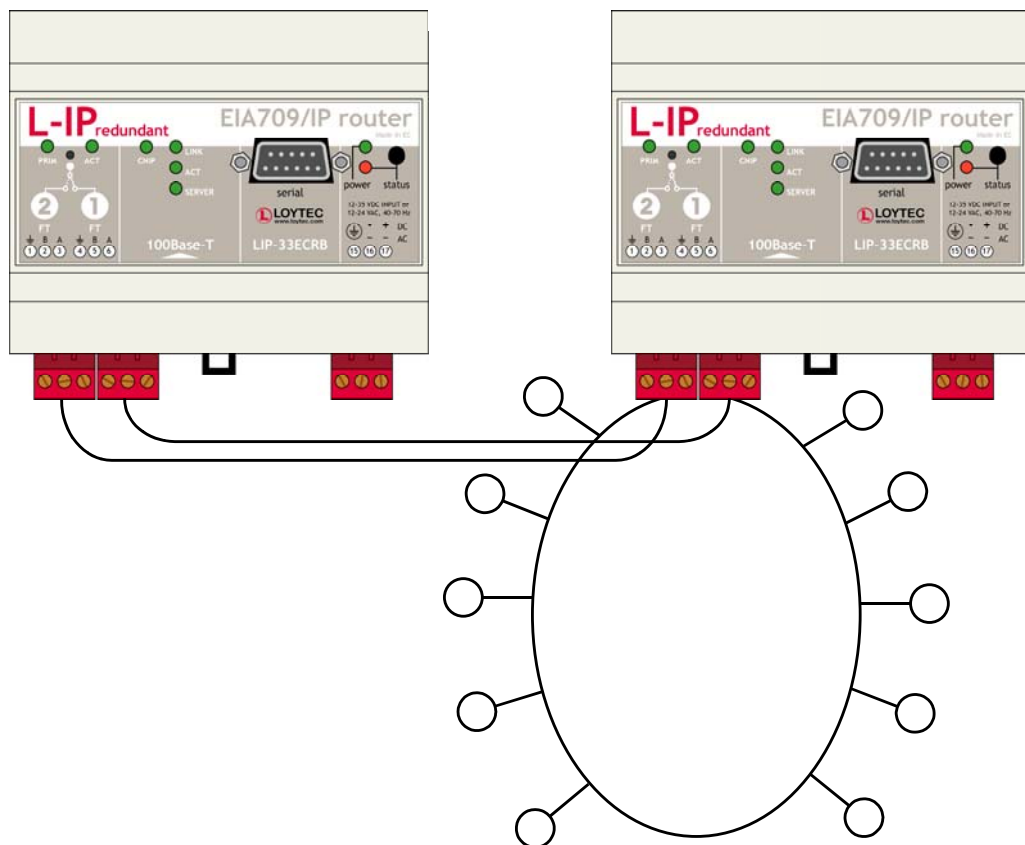


Figure 6: L-IP Redundant in Twin Router mode with Bus Loop Monitoring

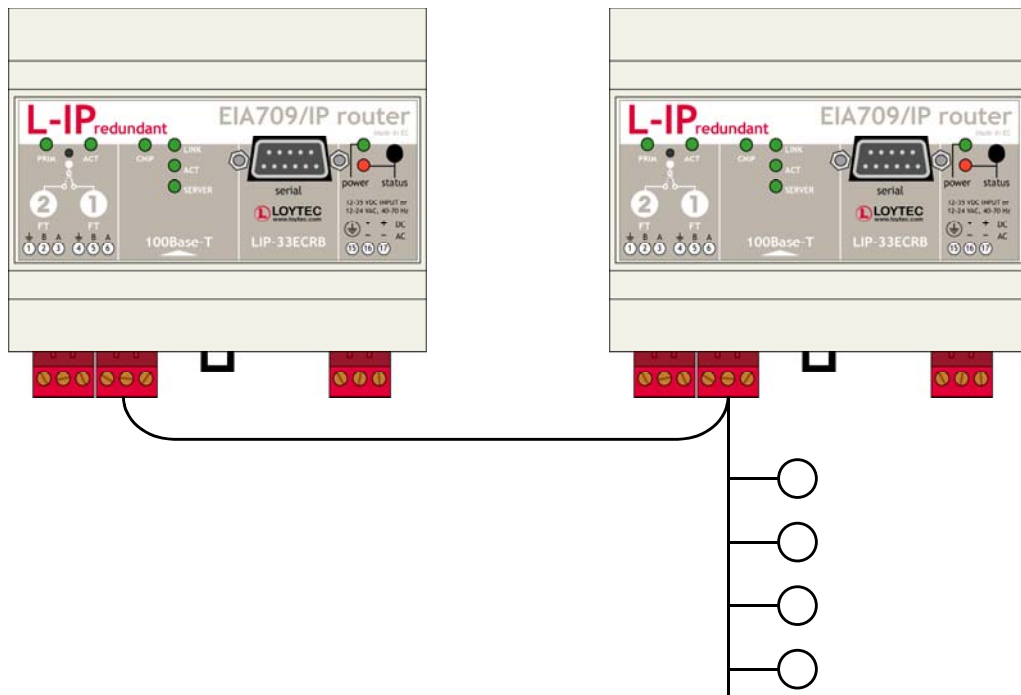


Figure 7: L-IP Redundant in Twin Router mode without Bus Loop Monitoring

2.2 IP Configuration for Client Device via Console

Use a PC terminal program with the communication settings set to 38,400 bps / 8 data bits / no parity / 1 stop bit / no handshake. On the LIP-xECT use a serial cable (1:1 male-female cable) to connect COM1 on the PC to the Console on the L-IP, on the LIP-xECTB, LIP-xxECTB, LIP-xxxxECTB, and LIP-xxECRB use a standard null-modem-cable with full handshaking. Power up the L-IP or press Return if the L-IP is already running. The following menu should appear on the terminal:

```
LOYTEC electronics GmbH
www.loytec.com

L-IP Configuration Menu
=====

[1] Show device information
[2] Serial firmware upgrade
[3] System configuration
[4] EIA-709 configuration
[5] IP configuration
[6] EIA-852 device configuration
[7] EIA-852 server configuration
[8] Reset configuration (factory defaults)
[9] Device statistics
[0] Reset device

Please choose:
```

Figure 8: Main L-IP menu.

Select 5 from the L-IP Configuration Menu and enter the IP address, netmask, and gateway address. Note that you must use different IP addresses if you are using multiple L-IPs in your setup.

IP Configuration Menu

=====

```
[1]  DHCP/BOOTP           : disabled
[2]  IP Address           : 192.168.1.254
[3]  IP Netmask           : 255.255.255.0
[4]  IP Gateway           : 192.168.1.1
[5]  Hostname             : newlip
[6]  Domainname           :
[7]  DNS Servers          : none
[8]  NAT Address          : Auto (no NAT)
[9]  MAC Address          : 00 0A B0 01 00 1D (factory default)
[0]  Multicast Address     : none
[a]  Connection Keep Alive : disabled
[b]  Link Speed & Duplex   : Auto Detect

[q]  Quit without saving
[x]  Exit and save
```

Please choose:

Figure 9: Enter basic IP settings.

Press x to save the IP settings and reset the L-IP with the main menu item 0 in order to let the new IP settings take effect.

You should now be able to add the L-IP to your CN/IP channel in the configuration server member list. More detailed instructions can be found in Section 4.6.

If the L-IP should also act as the configuration server please proceed to Section 2.4.

2.3 IP Configuration for Client Device via Web-Interface

Optionally to using the console interface one can also use the web interface to configure the client device. In your favorite web browser enter the default IP address 192.168.1.254 of the L-IP. Note that if your PC has an IP address in a subnet other than 192.168.1.xxx please open a command tool and enter the following route command to add a route to the L-IP.

Windows START → Run

command.com

Route add 192.168.1.254 %COMPUTERNAME%

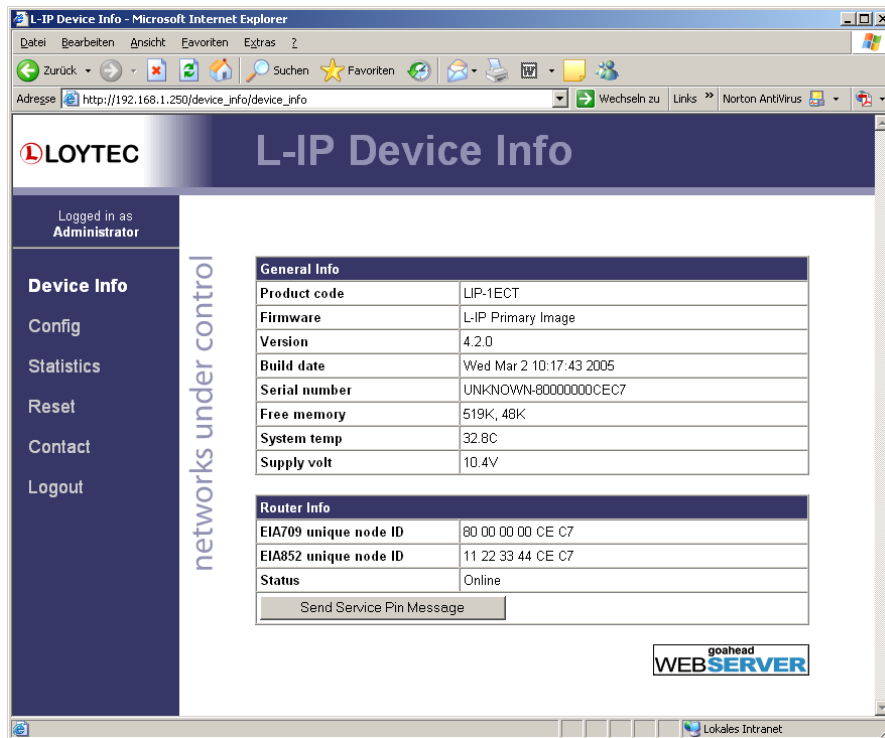


Figure 10: L-IP Start Screen.

Click on “Config” in the left menu. You will be asked to enter the administrator password in order to change the IP settings. Enter “admin” and select Login.

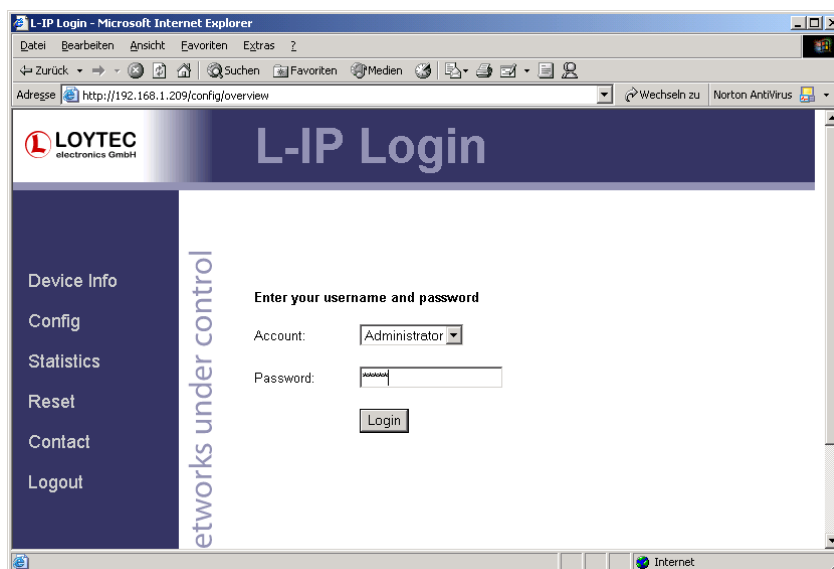


Figure 11: Enter admin as the default administrator password.

The Config menu opens. Click on IP in the Config menu and enter the IP address, the IP netmask, and IP gateway for this L-IP as shown in Figure 12.

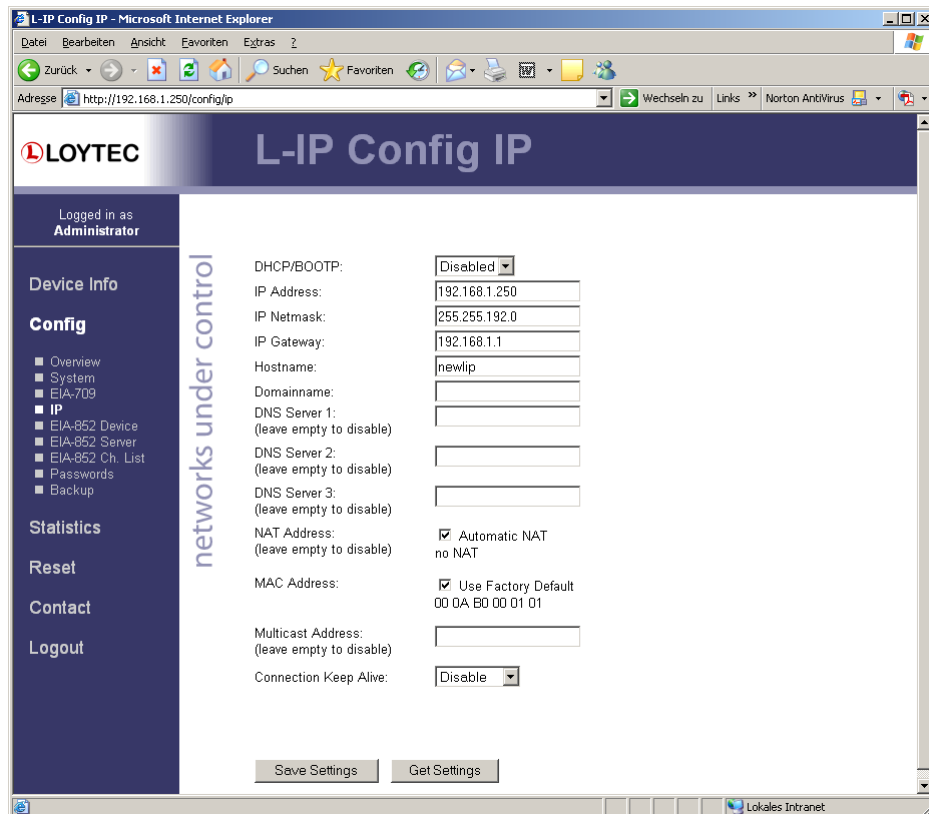


Figure 12: Enter IP address and gateway.

Press Save Settings and then reset the device by selecting “reset” in the highlighted text. This changes the IP settings of the L-IP.

2.4 Configuration Server Settings

If the L-IP should also act as the configuration server for the CN/IP channel go to the main menu item 7 and activate the EIA-852 configuration server menu. Enable the configuration server [1] and y and add the client devices with the menu item a. Client devices include all other L-IPs and all PCs, which should participate in the communication on the CN/IP channel.

Verify with the menu item l (lower case L) that the device(s) have been registered successfully.

Press x to save the new settings.

Optionally the configuration server settings can be set through the web interface by selecting the “EIA-852 Server” and the “EIA-852 Ch. List” menu item.

The cnip-LED on all L-IP devices should be green and the server-LED on the configuration server L-IP should be green as well.

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 Ethernet channel. For detailed instructions on how to configure the configuration server please refer to Section 4.8.

2.5 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 5). For operating the device in twin router mode (device redundancy, see Figure 6) 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 15. Furthermore, the PRIM LED on one of the two L-IP Redundant devices should be green and should be off on the other one.

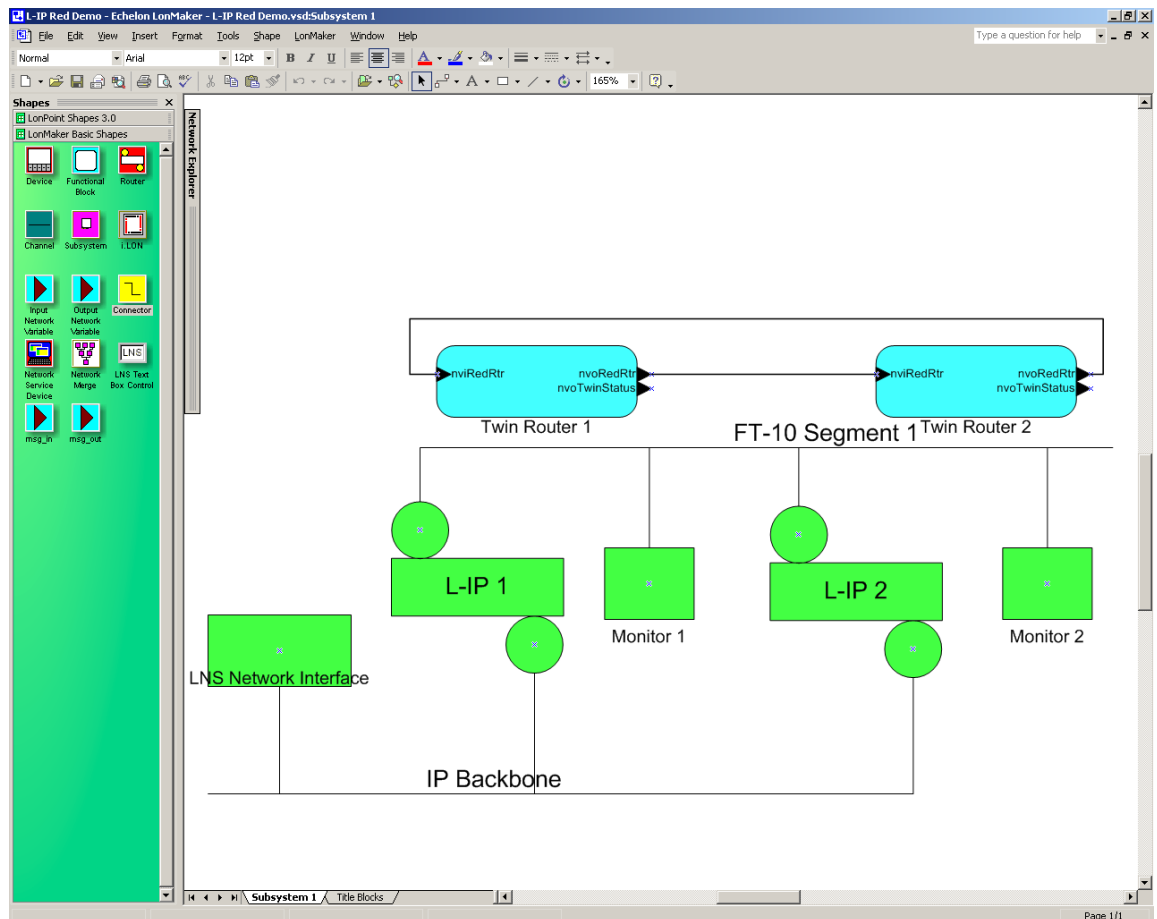


Figure 13: A pair of L-IP Redundant devices configured for twin router operation

For detailed instructions on how to configure the L-IP Redundant refer to Section 8.

3 Hardware Installation

3.1 Enclosure

3.1.1 L-IP

The L-IP enclosure is 9 TE (1 TE = 17.5 mm) wide for DIN rail mounting, following DIN 43 880 (see Figure 14).

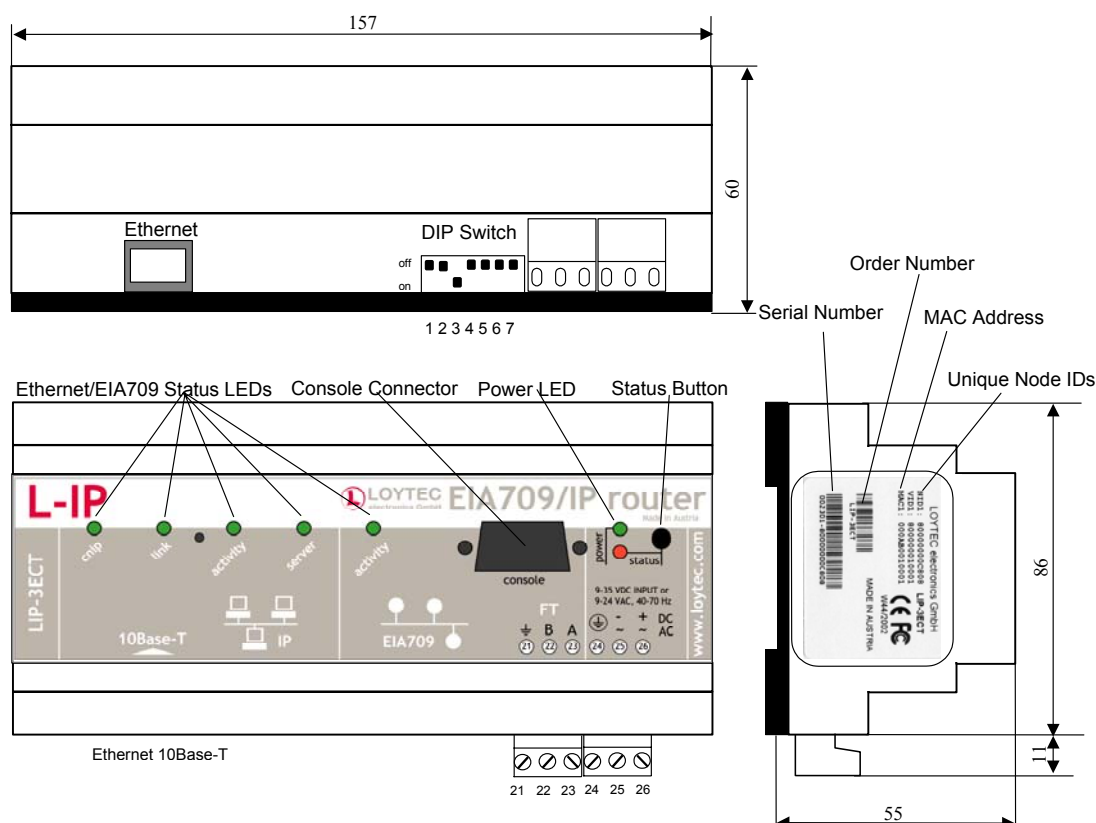


Figure 14: L-IP enclosure (dimensions in mm)

The small multi-port L-IP(B) enclosure is 6 TE (1 TE = 17.5 mm) wide for DIN rail mounting, following DIN 43 880 (see Figure 15).

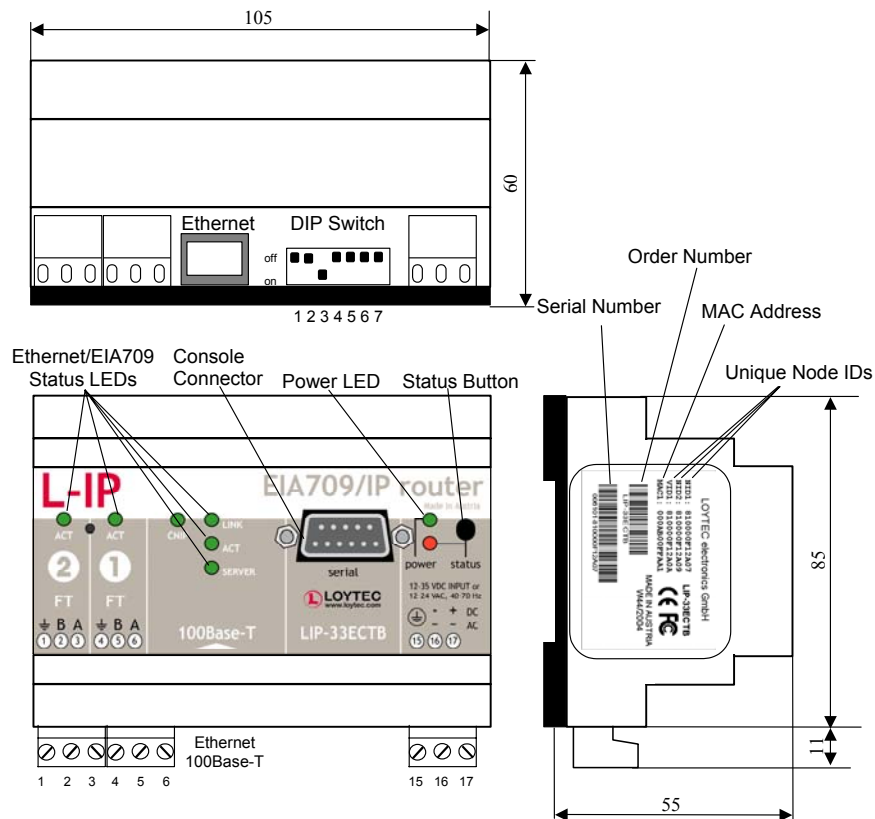


Figure 15: Small multi-port L-IP enclosure (dimensions in mm)

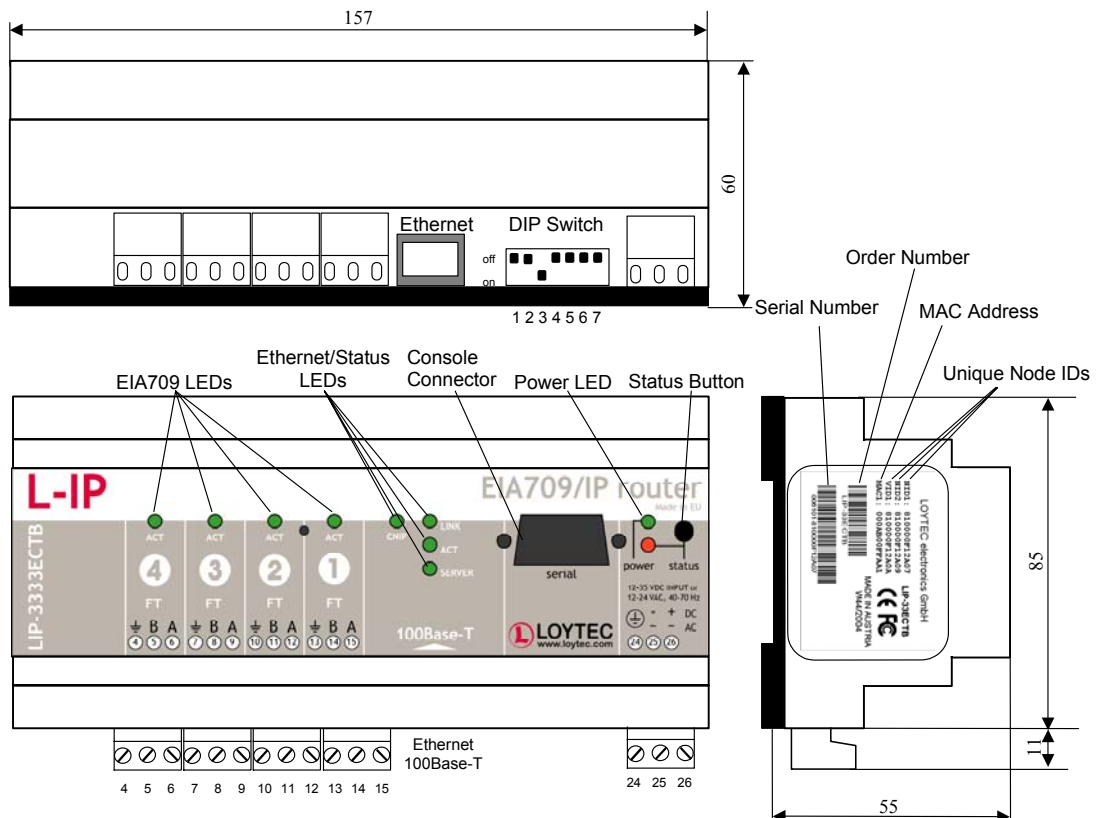


Figure 16: Large multi-port L-IP enclosure (dimensions in mm)

The large multi-port L-IP(B) enclosure is 9 TE (1 TE = 17.5 mm) wide for DIN rail mounting, following DIN 43 880 (see Figure 16).

3.1.2 L-IP Redundant

The L-IP Redundant enclosure is 6 TE (1 TE = 17.5 mm) wide for DIN rail mounting, following DIN 43 880 (see Figure 17).

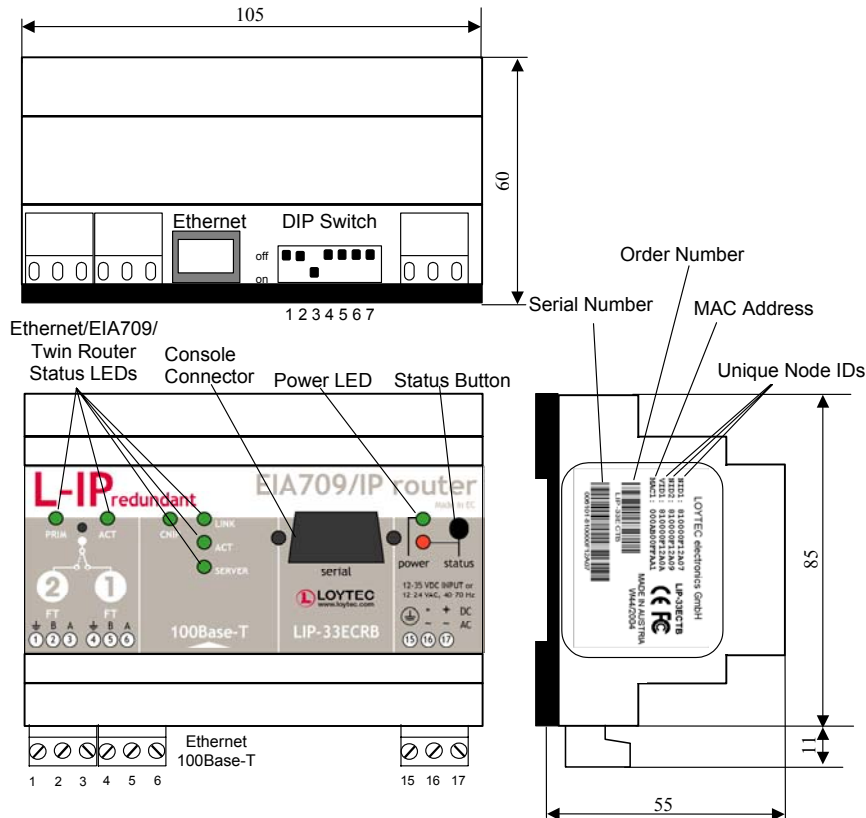


Figure 17: L-IP Redundant enclosure (dimensions in mm)

3.2 Product Label

The product label on the side of the L-IP contains the following information (see Figure 14 and Figure 15):

- ◆ L-IP order number with bar-code (Code 128, e.g. LIP-3ECT, LIP-33ECTB, or LIP-33ECRB)
- ◆ Serial number with bar-code (Code 128)
- ◆ Unique node ID and virtual ID of each port (NIDx and VIDx)

An additional label is also supplied with the L-IP for documentation purposes. A virtual ID (VID) is a Node ID on the IP channel.

3.3 Mounting

The device comes prepared for mounting on DIN rails following DIN EN 50 022. Then the L-IP is snapped on the rail.

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 (see Section 13).

3.4 LED signals

3.4.1 Power LED

The L-IP power LED lights up green when power is supplied to terminals 24, 25, and 26.

3.4.2 Status LED

The L-IP is equipped with a red status LED (see Figure 14). This LED is normally off.

During boot-up the status LED is used to signal error conditions (red).

After boot-up the status LED is used to signal write accesses to flash memory (illuminates red for the duration of every write access).

If the fall-back image is executed the status LED flashes red once every second.

3.4.3 EIA-709 Activity LED

The EIA-709 port on the L-IP has a three color LED (green, red and orange, see Figure 14). Table 1 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 EIA-709 router (see Section 6.1.1)
RED permanent	Port damaged	
RED flashing fast	Traffic with high amount of errors L-IP redundant: Loop open (see Section 3.4.10)	
RED flashing at 1 Hz (all ports)	Firmware image corrupt Please upload new firmware	
ORANGE permanent	Port disabled	e.g. using LSD Tool (see Section 12.1)
ORANGE flashing fast	Traffic on port configured as management port	e.g. using LSD Tool (see Section 12.1)
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 1: EIA-709 Activity LED patterns

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

The L-IP Redundant has a three color LED (green, red and orange, see Figure 17) showing the twin router status of the device. This LED is labeled “PRIM”. Table 2 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 2: 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.

3.4.5 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.

3.4.6 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.

3.4.7 EIA-852 Status LED (CNIP LED)

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

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

Green flicker: If a valid EIA-709 packet is received or transmitted over the IP channel the CNIP LED turns off for 50ms. Only valid EIA-709 IP packets sent to the IP address of the L-IP can be seen. Stale packets or packets not addressed to the L-IP are not seen. This LED behavior is new with firmware version 1.1.

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 CN/IP channel or shut-down itself due to an internal error condition.

Off: Device is non-functional because the CNIP module has not started. This can be the case if the L-IP 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 CNIP module is started but has not been configured. Please add the device to a CN/IP channel (register in configuration server).

Flashing green or orange at 1 Hz: The router of the port has not been commissioned yet. The color indicates the CNIP channel status as described above.

3.4.8 Configuration Server LED

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

3.4.9 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 EIA-709 activity LEDs. The EIA-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 EIA-709 activity LED flashes orange six times if the wink command was received on the EIA-709 channel. After that the L-IP LEDs return to their normal behavior.

3.4.10 Network Diagnostics

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

- 1) 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.
- 2) If the LED is flashing green the network segment connected to this port is ok.
- 3) 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 8).

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 Section 12.1).

3.5 Status Button

The L-IP is equipped with a status button (see Figure 14). When pressing the status button shortly during normal operation of the L-IP it sends a "Service Pin Message" on both 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 5.2).

If the multi-port L-IP is operated as an EIA-709 router (see Section 6.1.1) pressing the status button longer than 2 seconds will allow you to select the port to 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.

When pressing the status button during normal operation for more than 20 seconds, the L-IP forwarding tables will be reset (see Section 3.5.1).

3.5.1 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 EIA-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 EIA-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 by selecting the menu item "Reset to factory defaults" in the console menu (see Section 4.3.8).

Important: If the L-IP 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!

3.6 DIP Switch Settings

3.6.1 L-IP

The L-IP has 7 switches to select the operating mode. For details see Table 3 and Chapter 6.

DIP Switch #	Function	Factory Default
1, 2	ON, ON: Smart switch mode ON, OFF: Repeater mode OFF, ON: Smart switch mode/ subnet learning OFF, OFF: Configured EIA-709 router	OFF, OFF
3	Bit-rate auto detection On/Off (RS-485 version only)	ON
4	Must be OFF	OFF
5	Reserved	OFF
6	Reserved	OFF
7	Reserved	OFF

Table 3: DIP switch settings for L-IP

3.6.2 L-IP Redundant

The L-IP Redundant has 7 switches to select the operating mode. For details see Table 4 and Chapter 6.

DIP Switch #	Function	Factory Default
1	Reserved	OFF
2	Reserved	OFF
3	Bit-rate auto detection On/Off (RS-485 version only)	ON
4	Must be OFF	OFF
5	Reserved	OFF
6	Reserved	OFF
7	Reserved	OFF

Table 4: DIP switch settings for L-IP Redundant

3.7 Power Supply

The L-IP can either be DC or AC powered. The 2-port L-IP (LIP-xECT) has the power terminals as listed in Table 5, the small multi-port L-IP (LIP-xECTB and LIP-xxECTB) and L-IP Redundant (LIP-xECRB) as listed in Table 6, and the large multi-port L-IP (LIP-xxxxECTB) as listed in Table 7.

Terminal	Function	Note
24	Main Earth Ground	
25, 26	Power Inputs	9-35 VDC or 12-24 VAC $\pm 10\%$

Table 5: Power Terminals on LIP-xECT

Terminal	Function	Note
15	Main Earth Ground	
16, 17	Power Inputs	12-35 VDC or 12-24 VAC $\pm 10\%$

Table 6: Power Terminals on LIP-xxECTB, LIP-xECTB, and LIP-xxECRB

Terminal	Function	Note
24	Main Earth Ground	
25, 26	Power Inputs	12-35 VDC or 12-24 VAC $\pm 10\%$

Table 7: Power Terminals on LIP-xxxxECTB

Important: *Do not ground the power supply wire on terminal 26 (LIP-xECT and LIP-xxxxECTB) or terminal 17 (LIP-xECTB, LIP-xxECTB, and LIP-xxECRB) as shown in Figure 19!*

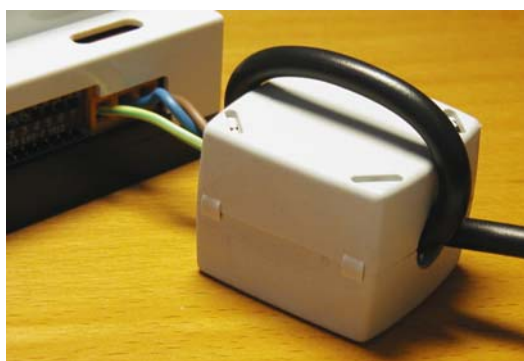


Figure 18: Attach the ferrite to the power cord

Attach the ferrite if shipped with the L-IP to the power cord as shown in Figure 18 (LIP-xECT only). Make sure the power cord passes the ferrite twice.

The following power supplies are recommended for use with the L-IP:

Manufacturer: IDEC IZUMI CORPORATION

Manufacturer part number: PS5R-A12

Description: Power Supply, 12V, 7.5W, UL 508, CSA C22.2 No.14, EN60950, 100-240VAC

LOYTEC order number: LS-PS7W

Note: Switched power supplies like the IDEC IZUMI PS5R-A12 might interfere with power-line communication. If you are using communication over the power-line we strongly recommend a linear power supply or have the switched power supply tested against interference with power-line communication signals. The IDEC power supply is not recommended for use with the power-line communication.

3.8 Terminal Layout

The L-IP provides screw terminals to connect to the network as well as to the power supply. The screw terminals can be used for wires having a maximum thickness of 1.5 mm²/AWG12.

3.8.1 LIP-3ECT (FT-10)

Terminal	Function
4	Ethernet 10BaseT
21	Earth Ground
22, 23	EIA-709 A, B of FT-10 Channel
24	Main Earth Ground
25, 26	Power Supply (do not connect 26 to ground)

Table 8: L-IP Terminals LIP-3ECT

3.8.2 LIP-1ECT (TP-1250)

Terminal	Function
4	Ethernet 10BaseT
21	Earth Ground
22, 23	EIA-709 A, B of TP-1250 Channel
24	Main Earth Ground
25, 26	Power Supply (do not connect 26 to ground)

Table 9: L-IP Terminals LIP-1ECT

3.8.3 LIP-33ECTB (2 x FT-10)

Terminal	Function
1	Earth Ground
2, 3	EIA-709 A, B of FT-10 Channel Port 2
4	Earth Ground
5, 6	EIA-709 A, B of FT-10 Channel Port 1
8	Ethernet 100BaseT
15	Main Earth Ground
16, 17	Power Supply (do not connect 17 to ground)

Table 10: L-IP Terminals LIP-33ECTB

3.8.4 LIP-33ECRB (L-IP Redundant with FT-10)

Terminal	Function
1	Do not connect
2, 3	EIA-709 A, B of FT-10 Loop Port 2
4	Earth Ground
5, 6	EIA-709 A, B of FT-10 Loop Port 1
8	Ethernet 100BaseT
15	Main Earth Ground
16, 17	Power Supply (do not connect 17 to ground)

Table 11: L-IP Terminals LIP-33ECRB

Note: The L-IP redundant LIP-33ECRB is compatible with link power.

3.8.5 LIP-3333ECTB (4 x FT-10)

Terminal	Function
4	Earth Ground
5, 6	EIA-709 A, B of FT-10 Channel Port 4
7	Earth Ground
8, 9	EIA-709 A, B of FT-10 Channel Port 3
10	Earth Ground
11, 12	EIA-709 A, B of FT-10 Channel Port 2
13	Earth Ground
14, 15	EIA-709 A, B of FT-10 Channel Port 1
17	Ethernet 100BaseT
24	Main Earth Ground
25, 26	Power Supply (do not connect 26 to ground)

Table 12: L-IP Terminals LIP-3333ECTB

3.9 Wiring

3.9.1 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 8.2.1).

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: *All Earth ground terminals must be connected to the main Earth ground terminal 24 (LIP-xECT and LIP-xxxxECTB) or terminal 15 (LIP-xECTB and LIP-xxECTB). When using shielded network cables only one side of the cable should be connected to ground. Thus, the shield must be connected to earth ground either at the L-IP terminals or somewhere else in the network, but never at more than one place (see Figure 19)!*

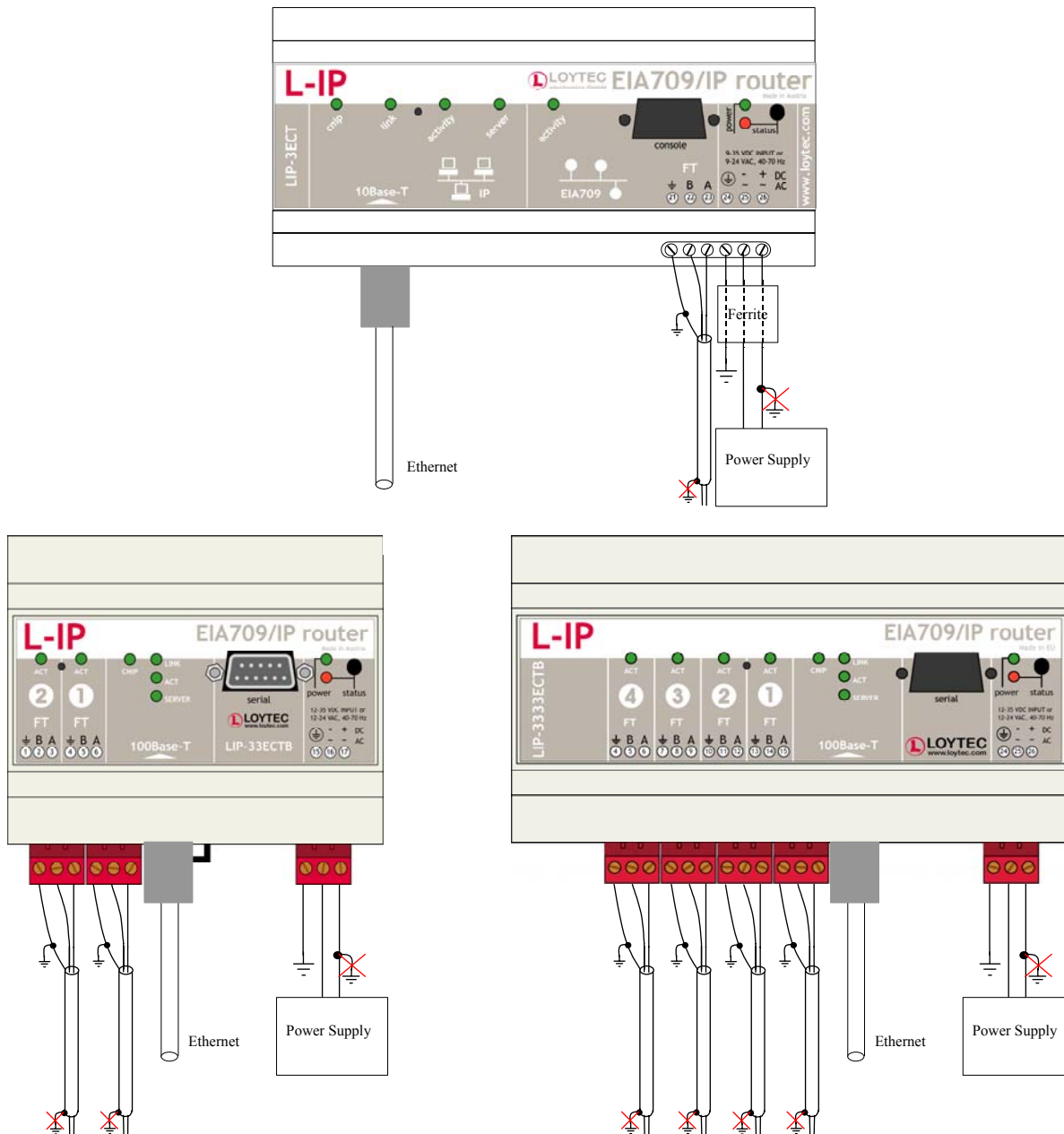


Figure 19: Connecting the Earth Ground to the L-IP

3.9.2 L-IP Redundant

Every network segment connected to the L-IP Redundant needs to be terminated according to the rules found in the specification of the transceiver (see Chapter 8.2.1).

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: All Earth ground terminals must be connected to the main Earth ground terminal 15. When using shielded network cables only one side of the cable should be connected to 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 20)!

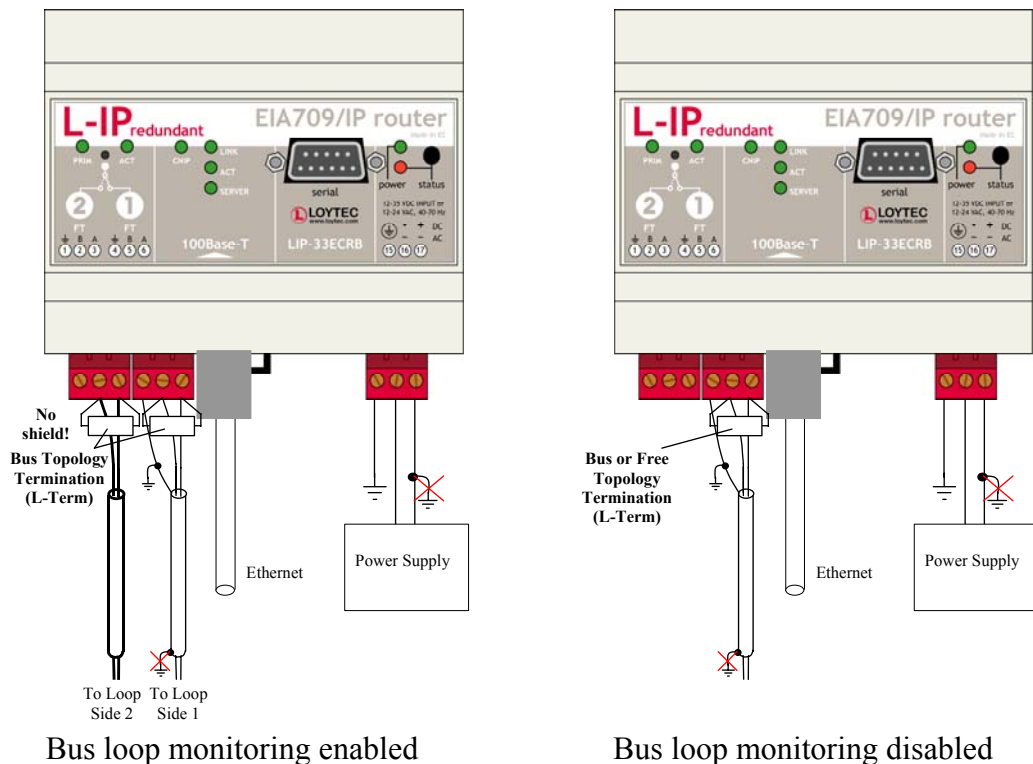


Figure 20: L-IP Redundant with and without Bus loop Monitoring

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 20). 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!

4 Console Interface

4.1 Console Connection

The L-IP is equipped with a serial interface to

- ◆ display the results of the self test,
- ◆ allow configuration via a console menu,
- ◆ upgrade the L-IP firmware.

To use the serial interface the console connector (see Figure 14) of the L-IP can be connected to the RS-232 port of a PC. The PC can communicate with the L-IP using a standard terminal program with the communication settings set to 38,400 bps / 8 data bits / no parity / 1 stop bit / no handshake.

For the LIP-xECT series a 1:1 female-male serial cable is required to connect the L-IP to the RS-232 port of a PC, while on the LIP-xECTB, LIP-xxECTB, LIP-xxxxECTB, and LIP-xxECRB series a standard null-modem-cable with full handshaking must be used.

Important: It is mandatory to at least set the proper IP configuration in order to operate the device!

4.2 Self Test

Whenever the L-IP comes out of reset it performs a self-test. If the self-test passed successfully, the EIA-709 activity LED turns green for 0.5 seconds. If a failure occurs during the self-test, the status LED is flashing red and the L-IP resets.

The console output of a successful boot sequence on an L-IP reads as follows:

```
LOYTEC electronics GmbH
www.loytec.com

Testing Board ID (0D)                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

Programming CPLD                      Passed
Port 1 detected (FT-10)               Passed

Starting TCP/IP networking            Passed
Ethernet device eth0 detected         Passed

L-IP(c)
LOYTEC electronics GmbH
Sep  1 2004 - V3.0.0
System has passed self-test and is active ...
```

Figure 21: Console messages during the boot phase.

The duration of a successful boot sequence of an L-IP is typically 12 seconds.

4.3 L-IP Configuration Menu (Main Menu)

After booting completed the L-IP displays the following console menu:

```
LOYTEC electronics GmbH
www.loytec.com

L-IP Configuration Menu
=====

[1] Show device information
[2] Serial firmware upgrade
[3] System configuration
[4] EIA-709 configuration
[5] IP configuration
[6] EIA-852 device configuration
[7] EIA-852 server configuration
[8] Reset configuration (factory defaults)
[9] Device statistics
[0] Reset device

Please choose:
```

Figure 22: L-IP main menu.

The menu items are described below:

4.3.1 Option 1 - Show device information

This menu item shows information about the L-IP and the current firmware version. The output should look like what is shown in Figure 23.

```
Product information
=====

Product code:  LIP-3ECT
Firmware:      L-IP Primary image
Version:       4.2.2
Build date:    Fri Mar 18 10:41:29 2005
Serial number: 002304-80000000E73C
Free memory:   557K,57K
System temp:   33.3C
Supply volt:   12.0V

Unique Node IDs
=====

Port 1: 80 00 00 00 E7 3C
EIA852: 80 00 00 00 F7 92
```

Figure 23: Device information.

4.3.2 Option 2 - Serial firmware upgrade

This menu item allows updating the L-IP firmware via the serial interface (console). See Section 10.2 for detailed instructions.

4.3.3 Option 3 - System configuration

Select this menu item to change system configuration settings. See Section 4.4 for details.

4.3.4 Option 4 - EIA-709 configuration

Select this menu item to change the EIA-709 configuration settings. See Section 4.5 for details.

4.3.5 Option 5 - IP configuration

Select this menu item to change the IP configuration settings like IP address, default gateway, DHCP, NAT address, MAC address, multi-cast address or to enable the automatic IP connection keep-alive feature. See Section 4.6 for details.

4.3.6 Option 6 - EIA-852 client configuration

Select this menu item to change the EIA-852 client configuration settings like configuration server IP address, device name, SNTP server, escrow timeout, aggregation timeout, MD5 authentication secret. See Section 4.7 for details.

4.3.7 Option 7 - EIA-852 server configuration

Select this menu item to change the EIA-852 server configuration settings like the channel name, channel membership list, the SNTP time server, channel timeout, MD5 authentication. See Section 4.8 for details.

4.3.8 Option 8 - Reset configuration (factory defaults)

This menu item resets the L-IP to factory defaults. See Section 3.5.1 for details on how to reset the forwarding tables by pressing the status button and Section 4.9 on how to load factory defaults through the console menu.

4.3.9 Option 9 - Device statistics

Select this menu item to display advanced IP and EIA-852 device statistics information like number of packets sent and received, number of channel members, ... See Section 4.10 for details.

4.4 System Configuration Menu

The system configuration menu allows setting the principal operating modes of the L-IP.

```
System Configuration Menu
=====

[1] Set date/time (GMT)           : 2002-10-29 08:37:15
[2] Router mode                   : Configured Router Mode (DIP)
[8] Webserver                     : enabled
[9] Change webserver passwords
[0] Webserver Port                : 80 (default)

[q] Quit without saving
[x] Exit and save

Please choose:
```

Figure 24: System Configuration Menu in configured router mode

4.4.1 Option 1 - Set date/time

If no SNTP server is selected use this menu to set the battery powered on-board real-time clock. This feature is supported in version 1.1 and higher.

4.4.2 Option 2 - Router mode

The router mode menu allows setting the principal operating mode of the L-IP routing core. Normally the operating mode of the routing core is set with the DIP switches 1 and 2 but can be overridden in this menu.

```
Set router mode
=====

[1]  Enable Configured Router Mode
[2]  Enable Smart Switch Mode
[3]  Set router configuration according to DIP switch

Please choose:
```

Figure 25: Router mode configuration menu.

4.4.2.1 Option 1 - Enable Configured Router Mode (Default)

Select this menu item if you want to use the L-IP as a standard configured EIA-709 router that can be configured in a network management tool like LonMaker or NL-220. This operating mode is also the factory default mode (see Table 3 on page 33).

Note! If you change the router mode of the L-IP you must reset the device in the main menu item 0 in order to have the changes take effect.

4.4.2.2 Option 2 - Enable Smart Switch Mode

Select this menu item if you want to use the L-IP as a self-learning router like the L-Switch ("smart switch mode"). In this configuration the L-IP 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. If Smart Switch Mode is enabled the system configuration menu has 3 additional entries as shown in Figure 26. It is preferable to select the switch mode via DIP switch settings see Table 3. The switch mode should only be used in LAN networks.

Note! If you change the router mode of the L-IP you must reset the device with the main menu item 0 or by pressing the reset button in order to have the changes take effect.

```
System Configuration Menu
=====

[1]  Set date/time (GMT)           : 2004-09-11 17:44:59
[2]  Router mode                  : Smart Switch Mode
[3]  Subnet/node learning         : subnet/node
[4]  Group learning               : enabled
[7]  Block unknown domains       : disabled
[8]  Webserver                    : enabled
[9]  Change webserver passwords
[0]  Webserver Port               : 80 (default)

[q]  Quit without saving
[x]  Exit and save
```

Please choose:

Figure 26: System Configuration Menu in Smart Switch Mode.

Entry 3 allows setting the mode for learning of subnet/node addresses. The selection can be Subnet/node learning, Subnet learning, Disable or DIP Switch. If subnet/node learning is

selected the L-IP will learn based on subnet/node addresses (see Section 6.1.2). Subnet broadcasts are flooded. This mode is plug&play.

If subnet learning is disabled, all subnet-wide broadcasts are forwarded by the L-IP from one side to the other side. If subnet learning is enabled the L-IP will learn the subnet addresses on both network ports and will only flood subnet broadcasts if the destination subnet address doesn't exist on the local channel. Subnet learning should be enabled if group overloading is used in the case that more than 256 group addresses are needed. Subnet learning is not plug&play. Please use LonMaker, NL-220, or other network management tools to ensure that one subnet address is only used behind one L-IP device. This can be achieved by using our L-IP LonMaker shapes or by placing phantom routers in e.g. NL-220. Please contact LOYTEC support if you think you need this feature!

Entry 4 allows enabling or disabling learning of group addresses.

Entry 7: The L-IP in Smart Switch Mode will learn up to four domains. If your network contains more than four domains please contact LOYTEC support for advice!

4.4.2.3 Option 3 - Set router configuration according to DIP switch

If this menu item is selected the DIP switch settings determine if the L-IP is used in router or in smart switch mode.

4.4.3 Option 8 - Webserver

This menu item allows enabling and disabling the web server on the L-IP. You can disable the web server if you don't want to give anybody access to the L-IP configuration via the web interface. This menu item toggles between enabled and disabled.

4.4.4 Option 9 - Change Web server Password

This menu item allows changing the passwords for the guest and the administrator account on the L-IP web server. Select [1] to set the password for the administrator account and [2] to set the password for the guest account. If no password is entered for the administrator account, the password protection is turned off and everybody can access the L-IP configuration via the web interface without a password. By default the guest password is empty (disabled) and the administrator password is "admin". Use this menu item to set the administrator or guest password if you have forgotten the passwords.

```
Change Webserver Passwords
=====
```

```
[1] Change Password for user 'Administrator'
[2] Change Password for user 'Guest'
```

```
[q] Quit
```

4.4.5 Option 0 - Web Server Port

This menu item allows the user to alter the web server port. The default is 80. Select this menu item and enter a non-default port.

4.5 EIA-709 Configuration Menu

This menu allows changing the EIA-709 transceiver configuration, enabling the backbone mode for TP-1250 transceivers, and enabling bit-rate auto-detection for RS-485 transceivers.

```
EIA709 Configuration Menu
=====

[1]  Port 1: XF/TP-1250 (1250 kBit)
      Port 2: IP-852

[q]  Quit without saving
[x]  Exit and save

Please choose:
```

Figure 27: EIA-709 configuration menu.

4.5.1 Option 1 - Change transceiver configuration for Port 1

This menu item allows setting the default transceiver configuration for port 1 if there are different possible transceiver configurations. Please contact LOYTEC support (see Section 11.8) if you want to change the default transceiver configuration (e.g. PLT-22 in CENLEC or NON-CENELEC mode).

For TP-1250 transceivers it is possible to set the transceiver settings to backbone mode. See Section 12.3 for an in-depth discussion and a step-by-step instruction on how to use this feature.

4.6 IP Configuration Menu

The IP configuration menu holds relevant IP settings. Here are some general guidelines for setting IP addresses, port numbers, and time values.

<p>Enter 0.0.0.0 to clear an IP address</p> <p>Enter 0 to select the default port number</p> <p>Enter 0 to disable a time setting.</p> <p>Press Return to keep the current setting.</p>

The IP configuration menu when DHCP is disabled is shown in Figure 28.

```

IP Configuration Menu
=====

[1]  DHCP/BOOTP           : disabled
[2]  IP Address           : 192.168.24.250
[3]  IP Netmask           : 255.255.192.0
[4]  IP Gateway           : 192.168.1.1
[5]  Hostname             : newlip
[6]  Domainname           :
[7]  DNS Servers          : none
[8]  NAT Address          : Auto (no NAT)
[9]  MAC Address          : 00 0A B0 01 02 DB (factory default)
[0]  Multicast Address     : none
[a]  Connection Keep Alive : disabled
[b]  Link Speed & Duplex   : Auto Detect

[q]  Quit without saving
[x]  Exit and save

Please choose:

```

Figure 28: IP configuration menu when DHCP is disabled.

The IP configuration menu when DHCP is enabled is shown in Figure 29.

```

IP Configuration Menu
=====

[1]  DHCP/BOOTP           : DHCP
      IP Address           : 192.168.24.250
      IP Netmask           : 255.255.192.0
      IP Gateway           : 192.168.1.1
[5]  Hostname             : lip1
      Domainname           :
      DNS Servers          : none
[8]  NAT Address          : Auto (no NAT)
[9]  MAC Address          : 00 0A B0 01 02 DB (factory default)
[0]  Multicast Address     : none
[a]  Connection Keep Alive : disabled
[b]  Link Speed & Duplex   : Auto Detect

[q]  Quit without saving
[x]  Exit and save

Please choose:

```

Figure 29: IP configuration menu when DHCP is enabled.

4.6.1 Option 1 - DHCP/BOOTP

Switches between manual entry of the IP address (0), netmask, and gateways address or automatic configuration from a BOOTP (1) or DHCP (2) server. If DHCP/BOOTP is disabled (0) one must enter the following configuration data. If DHCP/BOOTP is enabled (1 or 2) please skip menu items 2 through 7.

DHCP/BOOTP should not be used on the configuration server, if the IP address might change over time. It is very important that the configuration server always has the same IP address assigned.

If DHCP/BOOTP is enabled on a client device and the IP address assigned to the L-IP by the DHCP server on the network might change over time it is important to activate the “Roaming Member” support on the configuration server for this CN/IP channel (see Section 4.8.8).

4.6.2 Option 2 - IP Address, 3 - IP Netmask, 4 - IP Gateway

Please enter the IP address for the L-IP device, the netmask (e.g. 255.255.255.0), and the default gateway address.

4.6.3 Option 5 - Hostname, 6 - Domainname

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 to get information about how to configure DHCP to acquire an IP address.

4.6.4 Option 7 - DNS Servers

You can configure up to 3 Domain Name Servers. The DNS server entries are not currently used.

4.6.5 Option 8 - NAT Address

If the L-IP is used behind a NAT router the public IP address of the NAT router or firewall must be known. This address can either be entered manually or can be determined automatically. Automatic NAT router discovery allows to operate the L-IP behind a NAT router or firewall, which has a dynamic public IP address, and determines the correct NAT address from the L-IP CS. This is the default setting in firmware version 3.0 and up.

Automatic NAT router discovery is a feature available in firmware version 2.2 and up.

Enable automatic NAT router discovery (y/n):

Figure 30: Enable/Disable automatic NAT router discovery

To enable/disable automatic NAT router discovery select this menu option. The question in Figure 30 will be prompted on the console. Choose ‘y’ to enable automatic NAT router discovery. To manually enter a NAT address, choose ‘n’ and enter the NAT address when requested to do so. To completely disable the NAT router support, choose ‘n’ and enter the IP address 0.0.0.0 when requested to enter the NAT address.

Important: Automatic NAT router discovery does not work if the configuration server is enabled! If the configuration server is operated behind a NAT router or firewall enter the NAT address manually! The configuration server needs a fixed IP address! Automatic NAT router discovery only works with L-IP configuration servers!

If an L-IP uses automatic NAT router discovery and the NAT address is known beforehand then the L-IP can simply be added to the channel in the L-IP configuration server by specifying the NAT address and correct port. To add more than one L-IP behind a NAT refer to Section 6.3.2.

If the NAT address is not known, take the following steps to add the L-IP to a CN/IP channel in the configuration server:

1. On the L-IP turn on automatic NAT router discovery (this is the default setting). The NAT address should show "Auto (no NAT)".
2. Enter the IP address of the configuration server in the EIA-852 device configuration menu. Exit and save but do not reboot.
3. Go back to the main menu. Wait 15 seconds.
4. Go to the IP configuration menu. The NAT address should show the public IP address of the NAT router or firewall (e.g. "Auto (198.18.76.1)").
5. On the configuration server add the L-IP to the configuration server using this IP address.

4.6.6 Option 9 - MAC Address

The L-IP comes configured with a unique MAC address. This address can be changed in order to clone the MAC address of another device. It can be dangerous to change the MAC address. Please contact your system administrator to avoid MAC address conflicts. After selecting menu item 9 the following message appears.

```
Override factory MAC address (y/n):
```

Enter "y" to input a new MAC address or enter "n" to clear the current MAC address and return to the factory default MAC address.

4.6.7 Option 0 - Multicast Address

This menu option allows the user to add the L-IP into a multi-cast group for the CN/IP channel. Enter the channel's IP multi-cast address here. On how to obtain a valid multi-cast address please contact your system administrator. To learn when it is beneficial to use multi-cast addresses in your channel please refer to Section 6.5.

4.6.8 Option a - Connection Keep Alive

This feature is new with firmware version 1.1. The L-IP allows to automatically ping other devices on the IP channel 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). The options to choose are:

```
Select connection keep alive mode  
(0 - disabled, 1 - auto IP, 2 - custom IP):
```

Enter 0 to disable this feature, enter 1 for auto IP mode and 2 to specify one IP address that should receive the pings. If auto IP mode is selected and the L-IP works as a configuration server, a ping message is sent to all devices in the device list of the configuration server. If the configuration server is disabled on this L-IP a ping message is sent to the configuration server for the CN/IP channel.

Please refer to Section 4.10.5 on how to monitor the automatic keep-alive feature and to display the ping response times for the different devices on the CN/IP channel.

4.6.9 Option b - Link Speed & Duplex

This feature is new with L-IPs that feature a 100Mbit/s Ethernet port (100Base-T). If the L-IP is operated with an old 10Mbit/s-only hub the link speed should be switched from “Auto Detect” to “10Mbps/Half-Duplex”. With modern 100/10Mbit/s switches this setting can be left at its default.

```
Change Link Speed & Duplex
=====
```

```
[1] Auto Detect (default)
[2] 100Mbps/Full-Duplex
[3] 100Mbps/Half-Duplex
[4] 10Mbps/Full-Duplex
[5] 10Mbps/Half-Duplex
```

4.7 EIA-852 Device Configuration Menu

This menu holds relevant information regarding the configuration of the CN/IP device. Depending on the configuration method of the L-IP one can either input the configuration data in this menu and the L-IP then contacts the configuration server or the preferred method is to enter the information at the configuration server and the configuration server then contacts the device (L-IP) and fills in the relevant information in this menu. The device configuration menu is shown in Figure 31.

```
EIA-852 Client Configuration Menu
=====
```

```
[1] Config server address      : none
[2] Config server port        : 1629
[3] Config client port         : 1628 (default)
[4] Device name                : local
    Channel mode                : Standard
    Pri. SNTP server            : none
    Sec. SNTP server            : none
    Channel timeout             : off
[5] Escrow timeout             : on (64 ms)
[6] Aggregation timeout        : on (16 ms)
[7] MD5 authentication         : off
[8] MD5 secret                 : not displayed
[9] Location string            : Room 0815

[q] Quit without saving
[x] Exit and save
```

Please choose:

Figure 31: EIA-852 device configuration menu.

In case that the configuration server contacts the device (L-IP) only the MD 5 secret in menu item 8 must be entered if authenticated communication is required. In networks that communicate over the Internet one may also experiment with the escrow timeout in menu item 5.

If the L-IP serves as configuration server and as device some entries in the EIA-852 device configuration menu are set through the configuration server and cannot be set manually.

4.7.1 Option1 - Config server address, 2 - Config server port

Please enter the IP address and port of the configuration server, if the L-IP needs to contact the configuration server. Enter "0" for the configuration server port if you want to return to the default port setting.

4.7.2 Option 3 - Config client port

If not more than one L-IP is used behind a NAT router, this field should be left at the default setting. If changed, it must not be the same as the config server port.

4.7.3 Option 4 - Device name

You can enter a device name with up to 15 characters. It is recommended to use unique device names.

4.7.4 Channel Mode

This field reflects the current channel mode of the 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 L-IPs behind one NAT router) the channel switches to "Extended NAT mode". Please refer to Section 6.3.2 to learn more about the implications of this mode. Otherwise the mode is "Standard".

4.7.5 SNTP server, channel timeout

The configuration server sets the SNTP server addresses and the channel timeout.

4.7.6 Option 5 - Escrow timeout

Defines how long the L-IP waits for out-of-sequence CN/IP packets before they are discarded. Please enter the time in ms or 0 to disable escrowing. The maximum time is 255 ms.

4.7.7 Option 6 - Aggregation Timeout

Defines the time interval in which multiple EIA-709 packets are combined into a single CN/IP 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 L-IP device.

4.7.8 Option 7 - MD5 authentication

This menu item enables or disables MD5 authentication.

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

4.7.9 Option 8 - MD5 secret

Enter the 16-byte MD5 secret. Note that for security purposes the active MD5 secret is not displayed. Either 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

4.7.10 Option 9 - Location string

Enter a location string with a maximum length of 255 characters. This is optional and for informational purposes only.

4.8 EIA-852 Server Configuration Menu

This menu holds relevant information regarding the configuration of the CN/IP server.

```
EIA-852 Server Configuration Menu
=====

[1] Config server status      : enabled
[2] Config server port       : 1629 (default)
[3] Channel name              : default
    Channel members           : 3
    Channel mode               : Standard
[4] Pri. SNTP server          : 192.168.1.2:123
[5] Sec. SNTP server          : none
[6] Channel timeout           : off
[7] Auto members support      : off
[8] Roaming members support   : on
[9] MD5 authentication        : off
[0] MD5 secret                : not displayed

[a] Add device
[e] Edit device
[d] Delete device
[n] Enable/Disable device
[s] Show device statistics
[l] List channel members
[r] Re-contact devices & list channel members

[q] Quit without saving
[x] Exit and save
```

Please choose:

Figure 32: Configuration Server Menu.

If the built-in configuration server is used to manage the devices on the CN/IP channel, all CN/IP devices on the CN/IP channel must be entered in the device list of the server. The CN/IP devices themselves then only need to have a unique IP address, device name, and if operated behind a NAT router the NAT address assigned. The configuration server will contact all devices in the device list and update the relevant information in the client devices.

The server configuration menu is shown in Figure 32. The device name can also be set by the configuration server.

4.8.1 Option 1 - Config server status

The menu item allows enabling and disabling the built-in configuration server. If the configuration server is enabled the green configuration server LED labeled “server” will be on, otherwise it will be off.

4.8.2 Option 2 - Config server port

The menu item allows changing the port for the configuration server. It is recommended to keep the default port setting of 1629.

4.8.3 Option 3 - Channel name

The menu item allows setting a channel name that can consist of up to 15 characters.

The number of channel members is shown below the channel name.

4.8.4 Item Channel Mode

This field reflects the current channel mode. The L-IP configuration server automatically determines this mode depending if there are any two devices in the channel which use the same IP address but different ports (e.g. multiple L-IPs 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 6.3.2 to learn more about the implications of this mode.

4.8.5 Option 4 - Primary SNTP server, 5 - Secondary SNTP server

The two menu items allow setting the IP address of the primary and secondary SNTP time server. Please specify one or better 2 SNTP servers if CN/IP devices are communicating over the Internet rather than an Intranet. A list of available timeservers can be found at www.ntp.org. A subset of this list is shown in Table 13.

Country	Service Area	Hostname	IP Address
AT	Austria/Europe		130.149.17.21
CH	Swiss/Europe	swisstime.ethz.ch	129.132.2.21
DE	Germany/Europe	ntp0.fau.de	131.188.3.220
DK	Denmark	GPS.dix.dk	192.38.7.240
FR	France	canon.inria.fr	192.93.2.20
IT	Italy/Europe	ntp1.iien.it	193.204.114.232
JP	Japan/Pacific Area	clock.nc.fukuoka-u.ac.jp	133.100.9.2
NL	Netherlands/Europe	ntp0.nl.net	193.67.79.202
NO	NordUnet	time.service.uit.no	
SE	Sweden	ntp1.gbg.netnod.se	192.36.133.130
SG	Singapore/Asia	jamtepat.singnet.com.sg	165.21.110.7
UK	United Kingdom, Western Europe	chronos.csr.net	194.35.252.7

Country	Service Area	Hostname	IP Address
US	BARRnet, Alternet-west, CIX-west	clock.isc.org	192.5.5.250

Table 13: NTP timer server locations.

More SNTP servers can be found at <http://www.eecis.udel.edu/~mills/ntp/clock1.html>.

4.8.6 Option 6 - Channel Timeout

This menu item allows setting the channel timeout. The channel timeout is a CN/IP 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 7.10. Setting a channel timeout other than 0 requires a valid SNTP server entry on the configuration server (see Section 4.8.5).

4.8.7 Option 7 - Auto members support

This menu item allows members to be automatically added to the channel. If turned on, CN/IP devices can register on the CN/IP 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 CN/IP devices can add themselves to the channel without knowledge of the system operator. This could cause a potential security hole.

4.8.8 Option 8 - Roaming members support

This menu item allows to track CN/IP 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 L-IPs can also be operated behind NAT routers, which change their IP address between connection setups. For more information on this topic refer to Section 6.3.1.

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.

4.8.9 Option 9 - MD5 authentication

This menu item allows enabling and disabling MD5 authentication. If MD5 authentication is enabled all devices on the CN/IP channel must have MD5 enabled and must use the same secret.

Note that MD5 authentication cannot be used together with the i.LON 1000 since the i.LON 1000 is not fully compliant with the EIA-852 authentication method. MD5 can be used with the i.LON 600.

4.8.10 Option 0 - MD5 secret

Enter the 16-byte MD5 secret. Note that for security purposes the currently set MD5 secret is not displayed. Either 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

4.8.11 Option a - Add device

Select this menu item to add a CN/IP device to the CN/IP channel. A new menu appears.

```
Add CNIP member
=====
[1] IP Address           : none
[2] Port                 : none
[3] NAT Address          : none
[4] Device name          :

[q] Quit without saving
[x] Exit and Save
```

Figure 33: Add CN/IP device.

Please enter the IP address and device name of the new CN/IP device that should join the CN/IP channel. If the port is different from the default port 1628 you must also enter the port address otherwise the default port address will be entered automatically. If the device is behind a NAT router enter the local address in item 1 and the NAT routers address in item 4. Do not forget to set up a port forwarding rule in the NAT router for the port specified in item 2.

4.8.12 Option e - Edit device

Select this menu item to edit a CN/IP device on the CN/IP channel. The L-IP prompts the device number which shall be edited. A list of available CN/IP devices is displayed with the menu item [1]. A new menu appears.

```
Edit CNIP member
=====
[1] IP Address           : 10.0.2.3
[2] Port                 : 1630
[3] NAT Address          : 80.168.1.250
[4] Device name          : lipnat1

[q] Quit without saving
[x] Exit and Save
```

Figure 34: Edit CN/IP device in channel member list.

You can now change the IP address, port, NAT address or device name of the CN/IP device.

4.8.13 Option d - Delete device

Select this menu item to delete a CN/IP device on the CN/IP channel. The L-IP prompts the device number which shall be deleted. A list of available CN/IP devices is displayed with the menu item [1].

4.8.14 Option n - Enable/Disable device

Select this menu option to enable or disable a CN/IP device on the CN/IP channel. An enabled device can be disabled and a disabled device can be enabled. The L-IP prompts the device number which shall be enabled/disabled. A list of available CN/IP devices with their current status is displayed with the menu item [1]. Disabled members are temporarily removed from the CN/IP channel and do not receive messages.

4.8.15 Option s - Show device statistics

Select this menu item to display statistics information for the client devices. The L-IP prompts the device number which shall be examine. This number can be found in the Channel Member List (see Section 4.8.16). Please note that this feature allows extracting the statistics information from remote client devices over the CN/IP channel.

4.8.16 Option l - List channel members

Select this menu item to list all CN/IP channel members.

```
List of channel members
=====
```

No	Name	IP Address	Status	Flags
000	local	80.125.123.100:1628	registered	
NAT Router		80.168.1.250		
+ 001	lipnat1	10.0.2.3:1628	registered	
+ 002	lipnat1	10.0.2.4:1630	registered	
003	sony	80.168.1.135:1628	registered	
004	lip2	80.168.1.251:1628	disabled	X
005	lpa-ip	80.168.1.215:1628	registered	A

```
Press <RETURN> to continue
```

Figure 35: List all CN/IP channel members.

The list shows the list entry number, the device name, the IP address and the current status of this device. Note that the first entry is always the local device, which is the CN/IP device built into the configuration server. Devices behind a NAT router are listed in a tree view style. The A-flag indicates that this device is an auto member. The X-flag indicates that the device got disabled because it does not support the extended NAT mode (e.g. pre 3.0 L-IP or i.LON 1000). If the channel mode falls back to standard, these devices are enabled again.

<i>Status</i>	<i>Description</i>
registered	The CN/IP device has been successfully registered with the CN/IP channel and is fully functional.
unregistered	The CN/IP device has never been registered with the CN/IP channel.
not contacted	The CN/IP device has not been contacted since the configuration server has started.
not responding	The CN/IP device has been registered but is not responding at the moment.
disabled	The CN/IP device has been disabled on the channel (or rejected).
internal error	The configuration server has detected an internal error. Please contact LOYTEC support in this case.

Table 14: Possible CN/IP device states.

4.8.17 Option r - Recontact devices & list channel members

Select this menu item to contact all CN/IP devices on the CN/IP channel and watch the state of the individual CN/IP devices.

This menu item can also be used when a CN/IP device (e.g. L-IP) is replaced and the CN/IP configuration must be propagated to the new device without deleting the device in the configuration server and adding the device again.

This menu item can also be used to remove all auto members from the configuration server that are no longer responding (see 4.8.7).

4.9 Reset configuration (load factory defaults)

This menu item allows to reset the device into its factory default state. The following menu appears.

```
Reset Configuration Menu
=====

[1]  Reset everything to factory defaults
[2]  Reset switch configuration to factory defaults

[q]  Back to main menu

Please choose:
```

Figure 36: Reset to factory defaults menu.

4.9.1 Option 1 - Reset everything to factory defaults

Pressing “1” resets the complete device to factory defaults. This includes IP settings and the EIA-709 routing functionality according to the DIP-switch settings. The factory default values are shown in Figure 37.

```
[2]  IP Address           : 192.168.1.254
[3]  IP Netmask          : 255.255.255.0
[4]  IP Gateway          : 192.168.1.1
[5]  Hostname            : newlip
[6]  Domainname          :
```

Figure 37: Factory default settings.

4.9.2 Option 2 - Reset switch configuration to factory defaults

Pressing “2” resets only the forwarding tables for the L-IP when used in smart switch mode (see Section 6.1.1). Use this menu item if you are moving EIA-709 network nodes between different EIA-709 channels.

4.10 Device Statistics Menu

This menu holds relevant information regarding the device statistics of the L-IP. It also holds the menu item to monitor the connection keep-alive feature of the L-IP. The device statistics menu is shown in Figure 38. Use this menu only for debugging purposes. There is no need to access this menu if the network is running smoothly. This menu is new with firmware version 1.1.

```
Device Statistics Menu
=====

[1]  Show EIA852 device statistics
[2]  Show extended EIA852 device statistics
[3]  Clear all EIA852 device statistics
[4]  Show IP statistics
[5]  Monitor connection keep alive
[6]  Enhanced communications test

[q]  Back to main menu

Please choose:
```

Figure 38: Device Statistics Menu.

4.10.1 Option 1 - EIA852 device statistics

A sample console output is shown in Figure 39.

EIA852 Device Statistics

=====

```

Seconds since cleared           : 511
Date/Time of clear (GMT)       : Fri Jan 17 06:43:06 2003
No. of members                 : 6
LT Packets received            : 120
LT Bytes received              : unknown
LT Packets sent                : 410
LT Bytes sent                  : unknown
IP Packets sent                : 124
IP Bytes sent                  : 4588
IP Packets received            : 827
IP Bytes received              : 33277
IP Packets data sent           : 0
IP Packets data received       : 0
LT Stale packets               : 415
RFC Packets sent               : 21
RFC Packets received           : 32
Avg. aggregation to IP        : unknown
Avg. aggregation from IP      : unknown
UDP Packets sent               : unknown
TCP Packets sent               : unknown
Multi-cast Packets sent        : unknown

```

Figure 39: EIA-852 device statistics.

4.10.2 Option 2 - Extended EIA852 device statistics

A sample console output is shown in Figure 40.

Extended EIA852 Device Statistics

=====

```

Session ID                     : 0x45d78f35
SNTP synchronized              : yes
Number of CR member infos      : 5
Current channel routing mode   : CR
Message alloc count            : 0
Dropped failed authentication   : 0
Dropped invalid frame          : 0
Dropped out-of-sequence        : 416
Dropped duplicates             : 14
Dropped missing timestamp      : 0
Active DC datetime              : 0xc1d2247b
Active CM datetime              : 0xc1d2247c
Active SL datetime              : 0x00000000
Stale DC messages               : 0
Stale CM messages               : 0
Stale SL messages               : 0
Stale CR messages               : 8
Number of DC updates            : 6
Number of CM updates            : 1
Number of SL updates            : 0
Number of CR updates            : 5
CR packets sent to CS           : 1

```

Figure 40: Extended EIA-852 device statistics.

4.10.3 Option 3 - Clear all EIA852 device statistics

Selecting this menu items clears the device statistics.

4.10.4 Option 4 - IP statistics

A sample console output is shown in Figure 41.

```
***** INTERFACE STATISTICS *****
***** lo0 *****
Address:127.0.0.1
Flags: Up Loopback Running Multicast
Send queue limit:50   length:0   Dropped:0
***** eth0 *****
Address:192.168.0.2      Broadcast Address:192.168.0.255
Flags: Up Broadcast Running Simplex Multicast
Send queue limit:50   length:0   Dropped:0
Network Driver Stats for CS8900 :
    rx ready len -      50          rx loaded len -      0
    rx packets -      931          tx packets -      165
    rx bytes -      78480          tx bytes -      13627
    rx interrupts -      931          tx interrupts -      165
    rx dropped -      0          rx no mbuf -      0
    rx no custers -      0          rx oversize errors -      0
    rx crc errors -      0          rx runt errors -      0
    rx missed errors -      0          tx ok -      165
    tx collisions -      0          tx bid errors -      0
    tx wait for rdy4tx -      0          tx rdy4tx -      0
    tx underrun errors -      0          tx dropped -      2
    tx resends -      0          int swint req -      2094
    int swint res -      2094          int lockup -      0
    interrupts -      3189

***** MBUF STATISTICS *****
mbufs: 512   clusters: 64   free: 14
drops: 0     waits: 0   drains: 0
    free:461      data:51      header:0          socket:0
    pcb:0         rtable:0     htable:0         atable:0
    soname:0      soopts:0     ftable:0         rights:0
    ifaddr:0      control:0    oobdata:0

***** IP Statistics *****
    total packets received      922
datagrams delivered to upper level      922
    total ip packets generated here      158

Destination      Gateway/Mask/Hw      Flags      Refs      Use Expire
Interface
default          192.168.0.1          UGS         6         0         0 eth0
62.178.55.77     192.168.0.1          UGH         0         1       3606 eth0
62.178.95.96     192.168.0.1          UGH         0         1       3606 eth0
81.109.145.243   192.168.0.1          UGH         0         1       3606 eth0
81.109.251.36    192.168.0.1          UGH         0         1       3606 eth0
127.0.0.1        127.0.0.1            UH          0         0         0 lo0
130.140.10.21    192.168.0.1          UGH         1         6         0 eth0
192.168.0.0      255.255.255.0        U           0         0         3 eth0
192.168.0.1      00:04:5A:26:96:1F    UHL         7         0      1722 eth0
213.18.80.166    192.168.0.1          UGH         1        148         0 eth0
***** TCP Statistics *****

***** UDP Statistics *****
    total input packets      924
    total output packets      158

***** ICMP Statistics *****
```

Figure 41: IP statistics.

This statistics menu has another feature in firmware 3.0 and up. It displays any IP address conflicts. If the L-IP's IP address conflicts with another host on the network the banner shown in Figure 42 is displayed.

```
WARNING: Conflicting IP address detected!  
         IP address 10.125.123.95 also used by device with MAC address  
         00 04 5A CC 10 41!
```

```
Clear IP conflict history (y/n):
```

Figure 42: IP Address conflict.

As a useful information the MAC address of the conflicting host is shown. If the information about this conflict shall be cleared hit 'y'. If 'n' is selected, the conflict will show up again the next time this menu is entered.

4.10.5 Option 5 - Monitor Connection Keep Alive

This menu item allows monitoring of the automatic connection keep-alive feature in the L-IP. The console will display the ping delays to the different destination L-IP devices. If a device doesn't respond the text "Timeout" will be displayed instead. Pressing "Return" terminates this output. A sample console output is shown in Figure 43.

```
Monitoring connection keep alive...  
Press <RETURN> to return to menu  
  
Sending ping to 192.168.1.236 ... Timeout  
Sending ping to 192.168.1.135 ... 3 ms  
Sending ping to 192.168.1.251 ... 4 ms  
Sending ping to 192.168.1.236 ... Timeout  
Sending ping to 192.168.1.135 ... 3 ms  
Sending ping to 192.168.1.251 ... 4 ms  
Sending ping to 192.168.1.236 ... Timeout  
Sending ping to 192.168.1.135 ... 3 ms  
Sending ping to 192.168.1.251 ... 4 ms  
Sending ping to 192.168.1.236 ... Timeout
```

Figure 43: Console output for the connection keep-alive monitor.

4.10.6 Option 6 - Enhanced Communications Test

This menu item allows testing the communication path between L-IP devices. It tests the EIA-852 data communication. This test can be used to determine if there is a working TCP/IP connection as well as a working EIA-852 connection between the individual devices. The test has been re-worked in firmware 3.0 and up to diagnose more thoroughly the paths between individual members and the configuration server in each direction.

A typical console output is shown in Figure 44.

Enhanced Communications Test

=====

Address	Result	RTT (ms)	Comment
-----	-----	-----	-----
192.168.1.253:1629 (CS)	OK	6	
192.168.1.250:1628	OK	6	
192.168.1.250:1631	OK	6	
192.168.1.37:1628	FAILED	n/a	Peer not reachable

Figure 44: Enhanced communication test console output.

The round-trip value (RTT) is measured as the time a packet sent to the peer device needs to be routed back to the L-IP. 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 15.

A warning “Incorrect NAT configuration detected!” is displayed if the enhanced communications test determines that the L-IP is operated behind a NAT router, but it has no NAT address configured. In this case go to the IP configuration menu and configure the correct NAT address or set it to Auto-NAT.

<i>Text displayed (Web icon)</i>	<i>Meaning</i>
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 L-IP). 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 L-IP is located behind a NAT router and the port-forwarding for the L-IP in the NAT-Router (usually 1628) 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 the NAT router. Execute this test on the suspicious device to determine any NAT configuration problem.

Table 15: Possible communication problems.

5 Web Interface

Starting with firmware version 2.0 the L-IP comes with a built-in web server and a web interface to configure the L-IP, extract statistics information, save the configuration to a file on your hard disk and to restore a previously saved configuration. The web interface allows configuring the IP settings, the EIA-852 device settings, and it allows adding and removing CN/IP devices to the configuration server device list. This interface is very simple to use and has an intuitive, self-explanatory user interface.

5.1 Start Screen and Account Management

In your favorite web browser enter the default IP address 192.168.1.254 of the L-IP. Note that if your PC has an IP address in a subnet other than 192.168.1.xxx please open a command tool and enter the following route command to add a route to the L-IP.

Windows START → Run

command.com

```
Route add 192.168.1.254 %COMPUTERNAME%
```

Also make sure that the web server has not been disabled in the console interface (see Section 4.4.3). The start screen should appear and show the information from Figure 45.

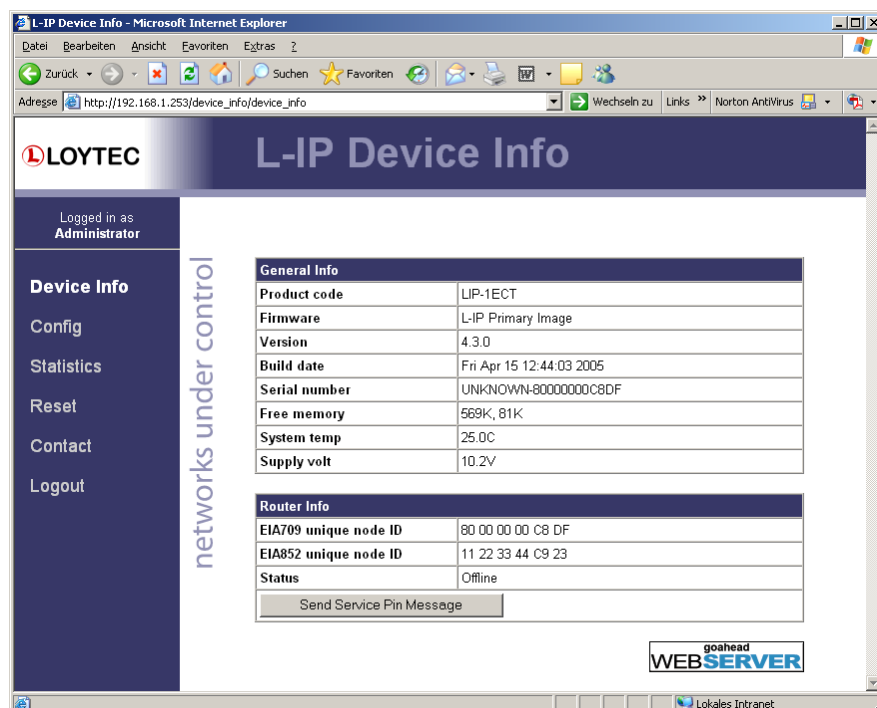


Figure 45: Example L-IP Start Screen.

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. Enter the default administrator password “admin” and select Login.

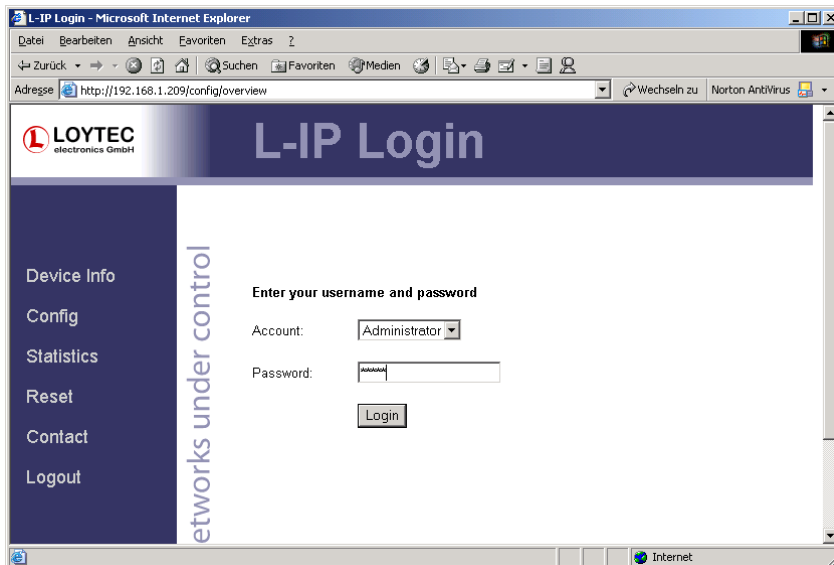


Figure 46: Enter admin as the default administrator password.

The Config menu opens. Click on IP in the Config menu and look at the IP settings as shown in Figure 47.

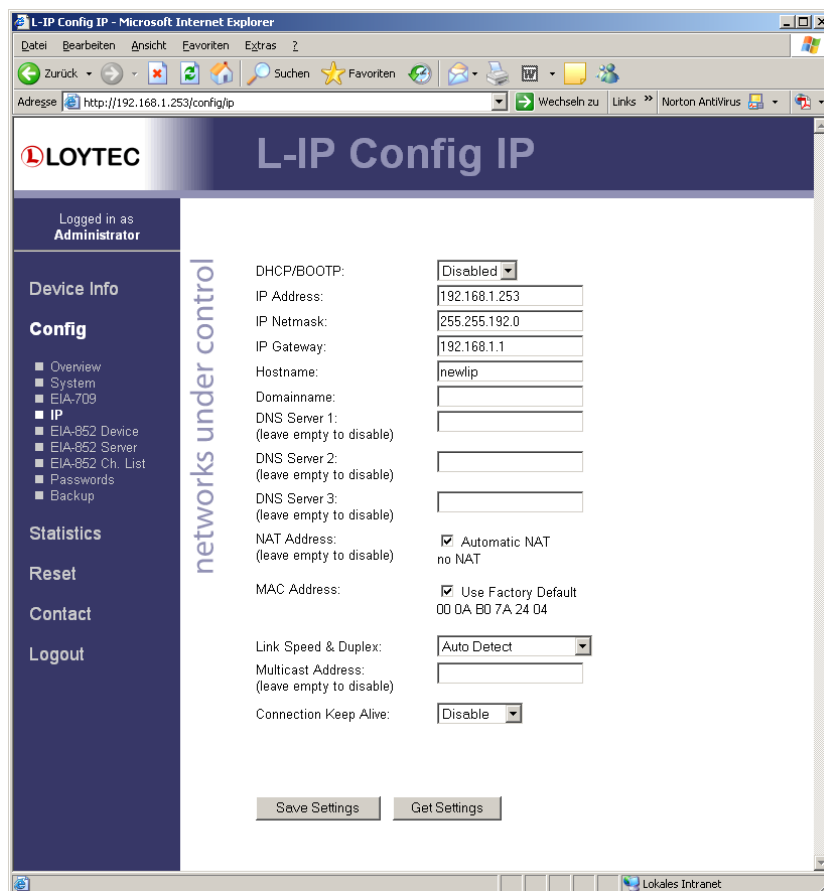


Figure 47: IP settings configuration screen.

The L-IP has 2 different accounts. The “guest” account can only view information whereas the administrator account has full access and can make changes to the L-IP configuration. Please change the administrator password in order to protect yourself from unwanted configuration changes by anyone else. If the administrator password is left empty, password protection is turned off and everyone can access the L-IP without entering a password.

5.2 Device Information

The device information page shows information about the L-IP and the current firmware version. It includes the unique node IDs (“Neuron IDs”) of the network interfaces on the EIA-709 side (EIA-709 unique node ID) and the CN/IP side (EIA-852 unique node ID). Further, it allows to send a service pin message on both sides. This is a very useful feature when commissioning the L-IP in configured router mode, since it is not necessary to be physically present at the site of the L-IP to press the status button.

The multi-port L-IP displays the external node IDs as well as the node IDs for the internal backbone in separate sections as shown in Figure 48. Each section contains the data associated with one router for each port. In each section it is possible to send a service pin message for the respective router.

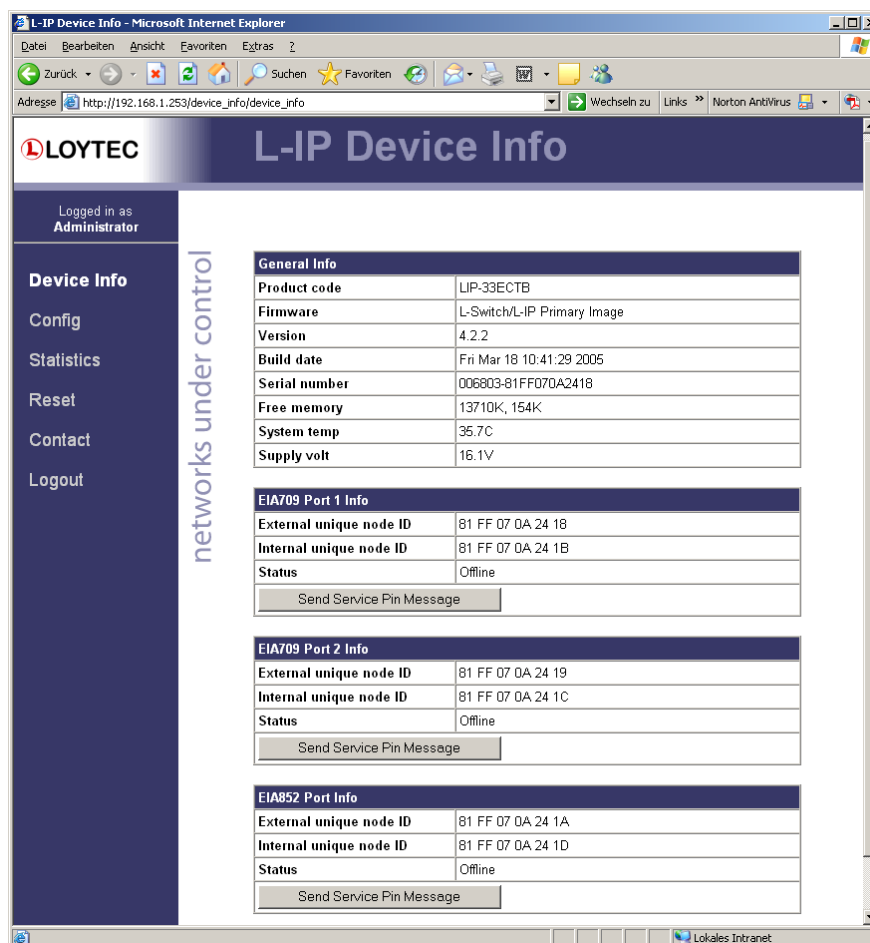


Figure 48: Device information page

5.3 Device Configuration

The device configuration page allows viewing and changing the device settings for the L-IP.



Figure 49: Device configuration setup screen.

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.

5.3.1 EIA-852 Channel List

On a CN/IP configuration server the CN/IP device list can be seen in the EIA-852 channel list menu. An example is given in Figure 50.

The Add Device button is used to add another CN/IP device to the CN/IP channel. The Reload button updates the website 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 checked 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 6.3.2.

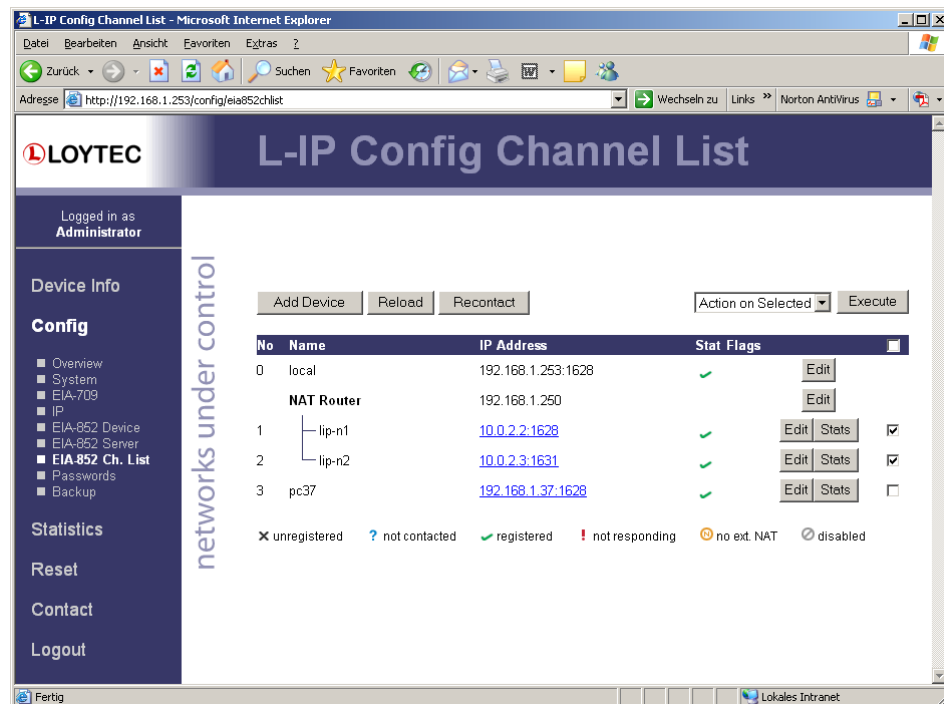


Figure 50: CN/IP device list.

The device status information is indicated with the bullets of different colors. The description for the different status indicators is shown in Table 14. The Flags column indicates with an **A** that the device is an auto member. An orange sphere indicates that the device is not compatible with extended NAT and has been disabled.

Click on the Edit button to change the device name, IP address, or 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.

5.3.2 Backup/Restore the L-IP Configuration

The Backup/Restore menu allows to backup the entire L-IP configuration including the EIA-852 Channel List on the configuration server. The backup file can be stored on your PC and restored to the same L-IP or a replacement L-IP at a later date. The Backup/Restore page is shown in Figure 51.

For more information on the additional device settings please consult the corresponding paragraphs in Section 4.3.

Important: Backups created with the L-IP firmware 4.4 and up cannot be used with firmware versions prior to 4.4!

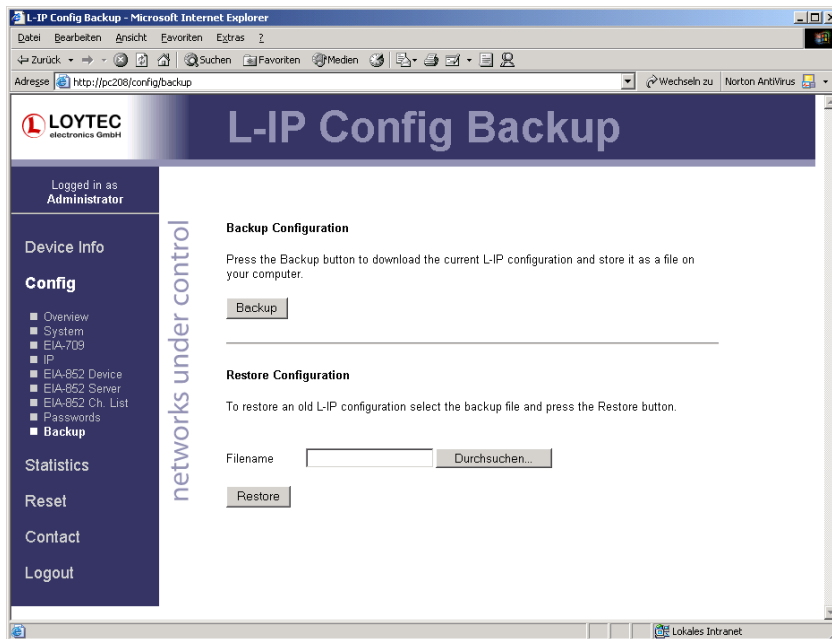


Figure 51: Web page to Backup and Restore the L-IP configuration.

5.4 Device Statistics

The device statistics menu provides advanced statistics information about the EIA-852 (CN/IP) device and the Ethernet interface.

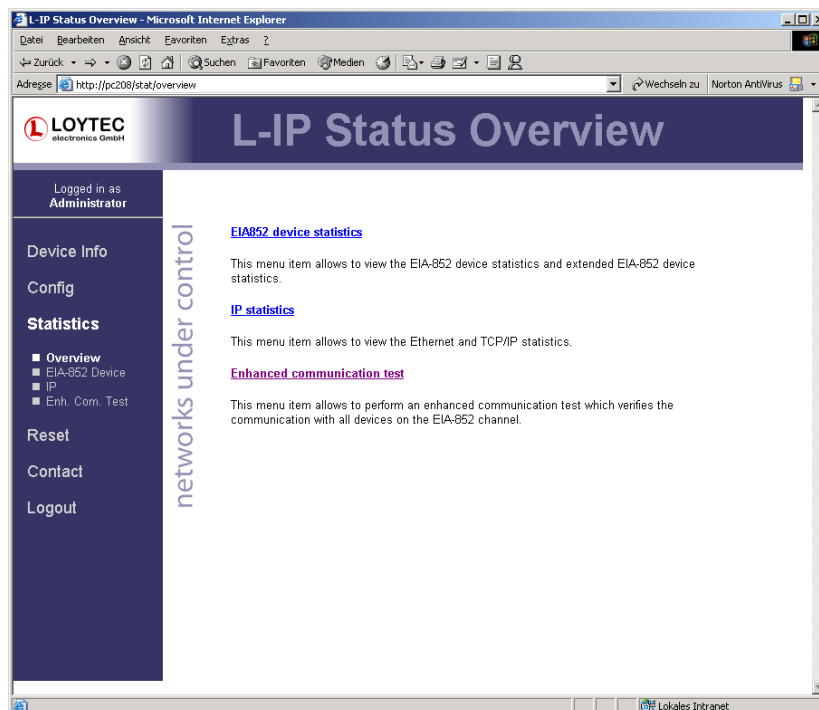


Figure 52: L-IP device statistics overview page.

The Enhanced Communications Test allows testing the EIA-852 communication path between L-IP devices and the configuration server. The test has been re-worked in firmware

3.0 and up to diagnose more thoroughly the paths between individual members 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 new 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 53.

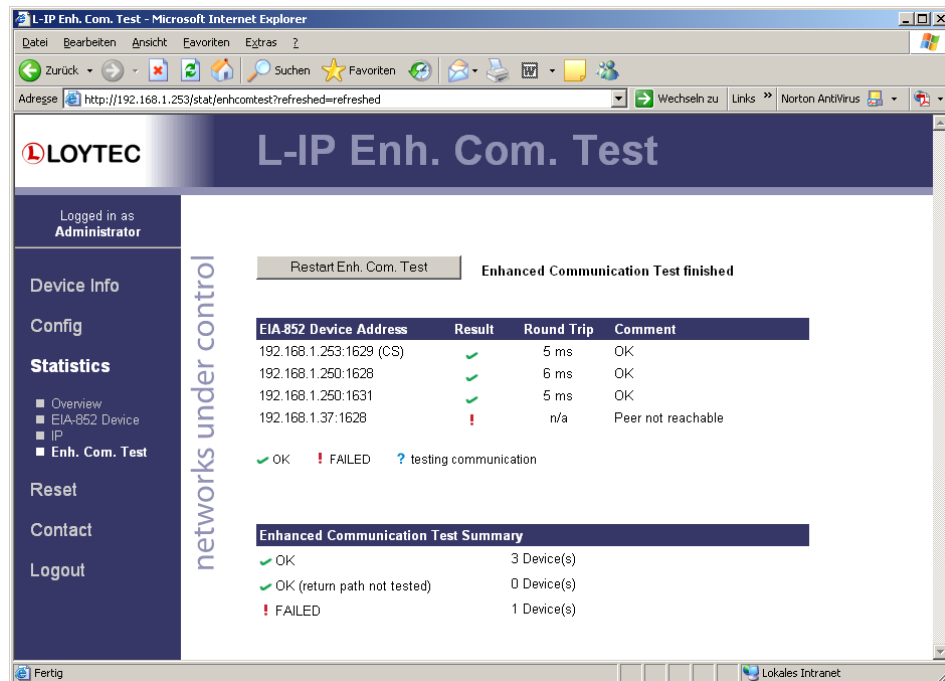


Figure 53: Enhanced communication test output.

The round-trip value (RTT) is measured as the time a packet sent to the peer device needs to be routed back to the L-IP. 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 15.

5.5 Reset, Contact, Logout

The menu item “Reset” allows resetting the L-IP from a remote location. 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.

6 Operating Modes

The L-IP routes EIA-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 EIA-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.

6.1 EIA-709 Router - Operating Modes

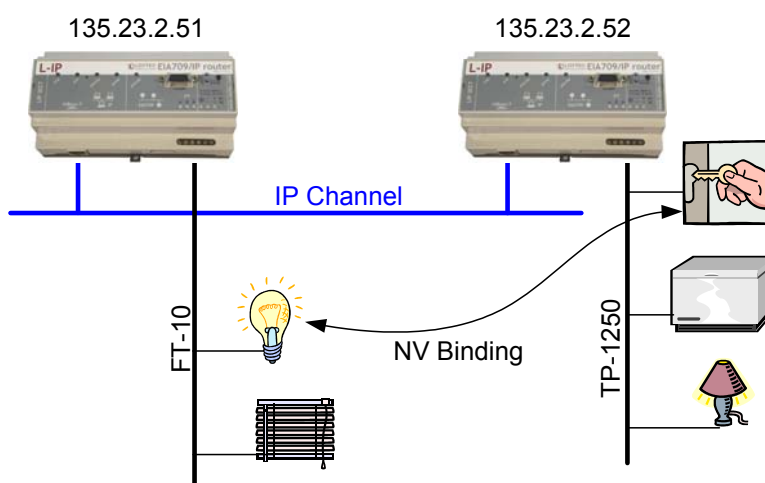


Figure 54: The L-IP supports different methods to route packets between the EIA-709 and IP channel.

Depending on the DIP switch settings of DIP switch 1 and 2 the L-IP supports 4 different methods to route packets between the EIA-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 EIA-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!

6.1.1 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 Internet Server and the i.LON 600 LonWorks/IP Server.

Figure 55 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.

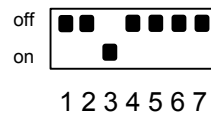


Figure 55: OFF-OFF: DIP-switch settings for configured router mode (factory default).

This operating mode uses the “channel routing” routing strategy on the IP channel. In this mode the L-IP is fully compatible with i.LON 1000/600 devices. This operating mode should also be used in networks with more than 10 L-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 L-IP device(s) that connect to the EIA-709 node(s) addressed in this IP packet and not to all L-IP devices on the IP channel. This is the standard operating mode.

6.1.2 Smart Switch Mode

The L-IP can be configured to act as a learning switch in an EIA-709 network. This operating mode is called smart switch mode. In this operating mode the L-IP 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 56 shows the proper DIP-switch setting to put the L-IP into smart switch mode.

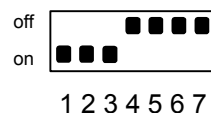


Figure 56: ON-ON: DIP-switch setting for smart switch mode.

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 L-IP by pressing the status button for at least 20 seconds (see Section 3.5.1).*

The L-IP 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 L-IP keeps track and modifies its forwarding tables accordingly.

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

The L-IP supports group learning. Groups can span multiple L-IP 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 L-IP 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 6.1.4).

The L-IP 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 L-IP devices and packet rates of more than 500 packets/s. Please use the configured router mode from Section 6.1.1 for larger IP channel configurations.

For firmware versions 3.0 and up it is recommended to configure a multi-cast group for L-IPs in the smart switch mode to reduce the traffic burden and improve scalability. Refer to Section 6.5 on how to configure the L-IP to use multi-cast.

6.1.3 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:

1. DIP-switch number 1 must be on, see Table 3.
2. DIP-switch number 2 must be off, see Table 3.
3. The forwarding tables must be reset by pressing the status button for at least 20 seconds (see Section 3.5.1).

Figure 57 shows the proper DIP-switch settings for repeater mode, assuming all other DIP switches remain in the factory default position.

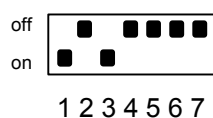


Figure 57: ON-OFF: DIP-switch settings for repeater mode

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.

For firmware versions 3.0 and up it is recommended to configure a multi-cast group for L-IPs in repeater mode to reduce the traffic burden and improve scalability. Refer to Section 6.5 on how to configure the L-IP to use multi-cast.

6.1.4 Smart Switch Mode with No Subnet Broadcast Flooding

This operating is the same as the smart switch mode from Section 6.1.2 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 58 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.

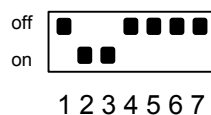


Figure 58: OFF-ON: DIP-switch settings for smart switch mode without subnet broadcast flooding.

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.

For firmware versions 3.0 and up it is recommended to configure a multi-cast group for L-IPs in the smart switch mode to reduce the traffic burden and improve scalability. Refer to Section 6.5 on how to configure the L-IP to use multi-cast.

6.2 EIA-852 Operating Modes

Every logical IP channel requires one configuration server that manages all CN/IP devices (L-IP, LOYTEC NIC852, i.LON 1000, i.LON 600, LonMaker, etc.) on this channel. Traditionally a dedicated Windows PC is used to act as the configuration server. The L-IP

can replace the PC and act as the configuration server in parallel to its normal client operation. The simple network from Figure 59 uses 2 L-IP devices to connect 2 EIA-709 channels. One L-IP acts as router and as configuration server for this IP channel. The second L-IP acts as a normal EIA-709 to IP router.

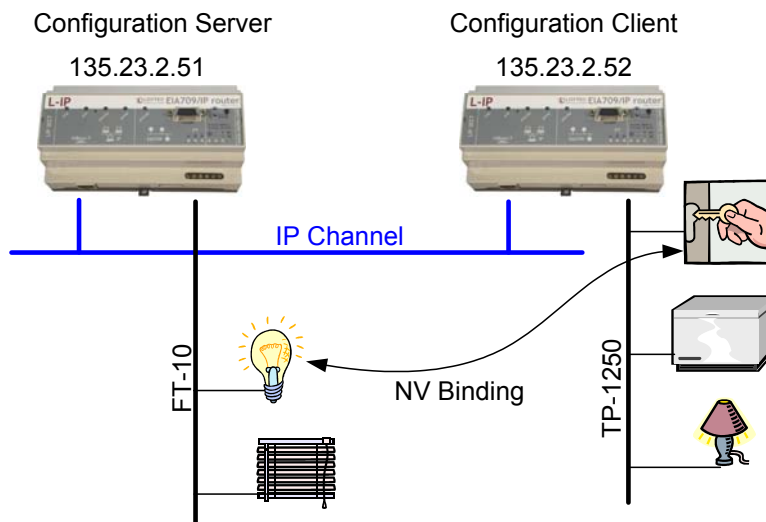


Figure 59: IP channel that consists of 2 IP devices. The left L-IP with IP address 135.23.2.51 acts as router and as a configuration server for this IP channel. It manages both IP devices 135.23.2.51 and 135.23.2.52.

6.2.1 CN/IP 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 CN/IP channel it needs to have the following parameters:

- ◆ IP address/netmask/gateway (either via DHCP or manual entry),
- ◆ NAT address if used behind a firewall (detected automatically with Auto-NAT),
- ◆ MD5 secret if authentication is required,

Please consult Sections 4.6 and 4.7 on how to setup a CN/IP device.

6.2.2 CN/IP Configuration Server

Each logical CN/IP channel needs one configuration server. The configuration server can be enabled in the L-IP in the EIA-852 server configuration menu in Section 4.8. This configuration server can manage one logical CN/IP channel and up to 256 devices on this CN/IP channel. In order to setup the configuration server one must specify the following parameters:

- ◆ IP address/netmask/gateway (either via DHCP or manual entry),

- ◆ NAT address if used behind a firewall,
- ◆ MD5 secret if authentication is required,
- ◆ Channel name,
- ◆ SNTP server (if used on the Internet),
- ◆ List of CN/IP devices.

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

6.3 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 60. In firmware versions prior to 3.0 only one L-IP can be used behind the NAT router. This mode of operation is referred to as “Standard” channel mode. It is fully compliant with EIA-852.

Firmware versions from 3.0 and up support more than one L-IP 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 7.5 on compatibility with the i.LON 600.

6.3.1 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 4.6). 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 60). 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.

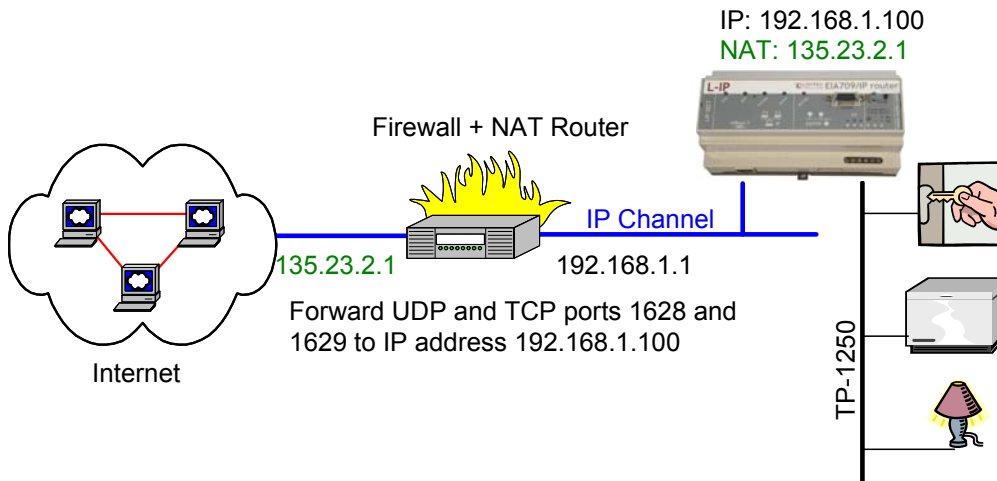


Figure 60: Operating an L-IP behind a NAT router and firewall.

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.

6.3.2 Multiple L-IPs behind a NAT: Extended NAT Mode

When using more than one L-IP behind a single NAT router the recommended method from firmware version 3.0 and up is to use the extended NAT mode. This mode requires that all devices support this feature. Currently these are L-IP 3.0, i.LON 600, and the NIC852 PC software 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 6.3.3 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 that each port points to one of the L-IPs. In the L-IP change the client port in the EIA-852 device configuration menu. Figure 61 shows an example configuration for three L-IPs 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 61 the L-IP with private address 192.168.1.100 also acts as a configuration server.

If the CS is activated on an 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 an L-IP with a CS). To diagnose possible problems in the NAT configuration with port forwarding use the enhanced communications test (see Section 4.10.6).

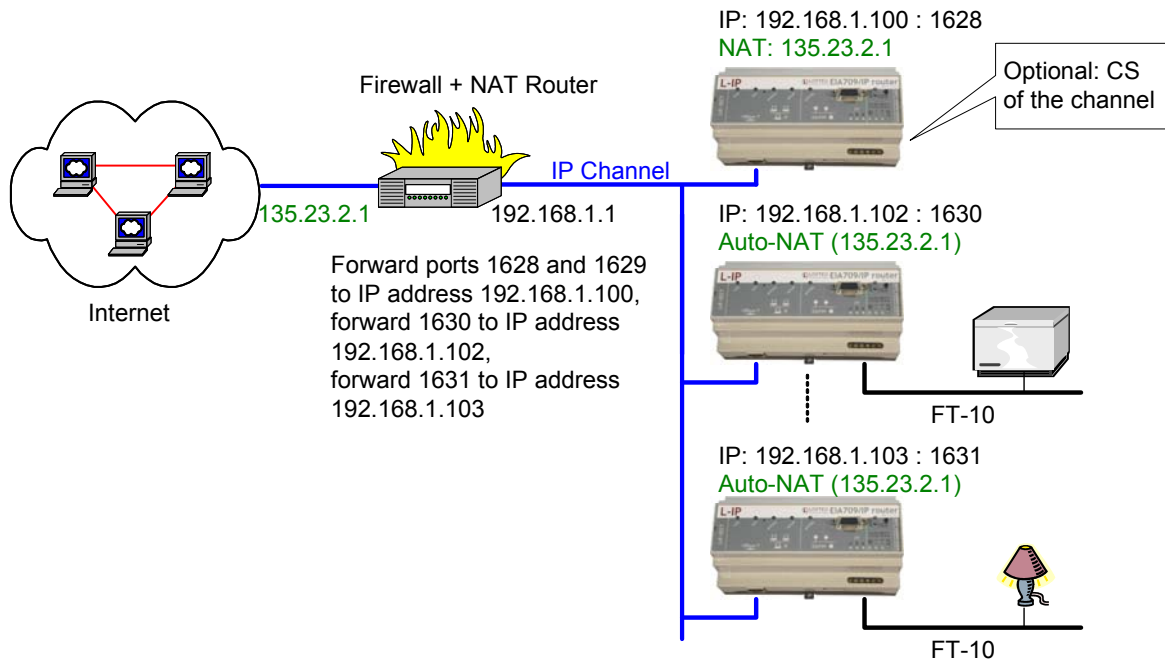


Figure 61 Multiple L-IP devices behind a NAT: Extended NAT Mode.

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.

On the console UI add the devices to the channel in the configuration server menu 7. Choose 'a' to add a device. Enter the private address of the device in the IP address field. Enter the public address of the NAT router in the NAT address field. Modify the port as needed. For example, to add the L-IP with port 1631 in Figure 61 enter the values as shown in Figure 62.

Add CNIP member
=====

```
[1] IP Address      : 192.168.1.103
[2] Port           : 1631
[3] NAT Address    : 135.23.2.1
[4] Device name    : lip-103
```

Figure 62: Adding a member with extended NAT Mode on the console UI.

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 L-IPs in Figure 61 through the Web UI is depicted in Figure 63. To remove a device from a NAT router but not delete it, select it and choose "Remove from NAT" as the action.

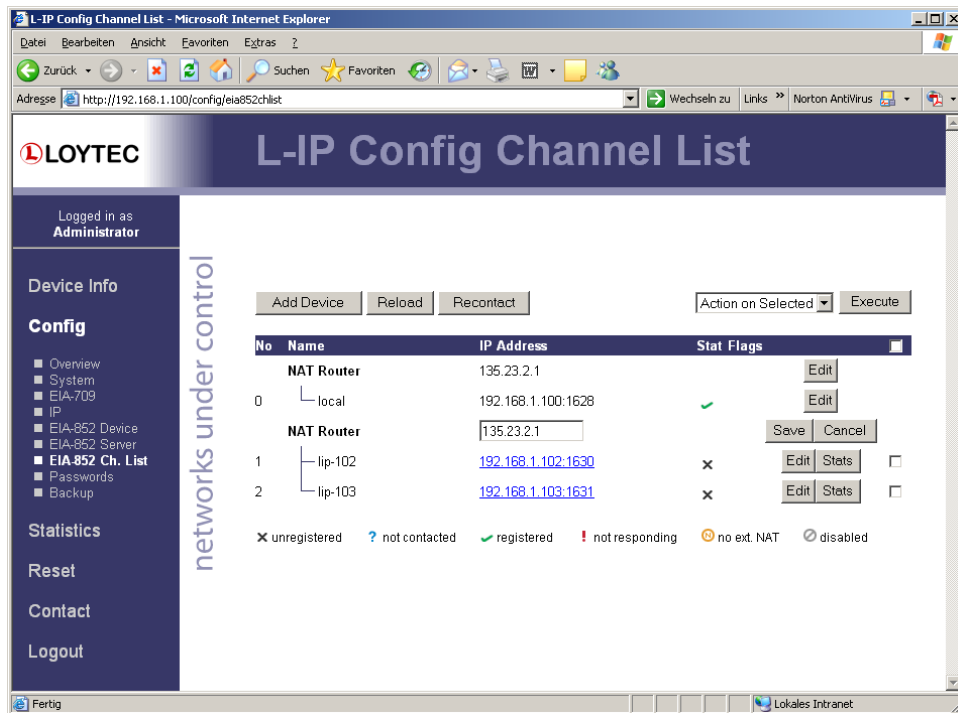


Figure 63: Adding a member with extended NAT Mode on the Web UI.

6.3.3 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 64.

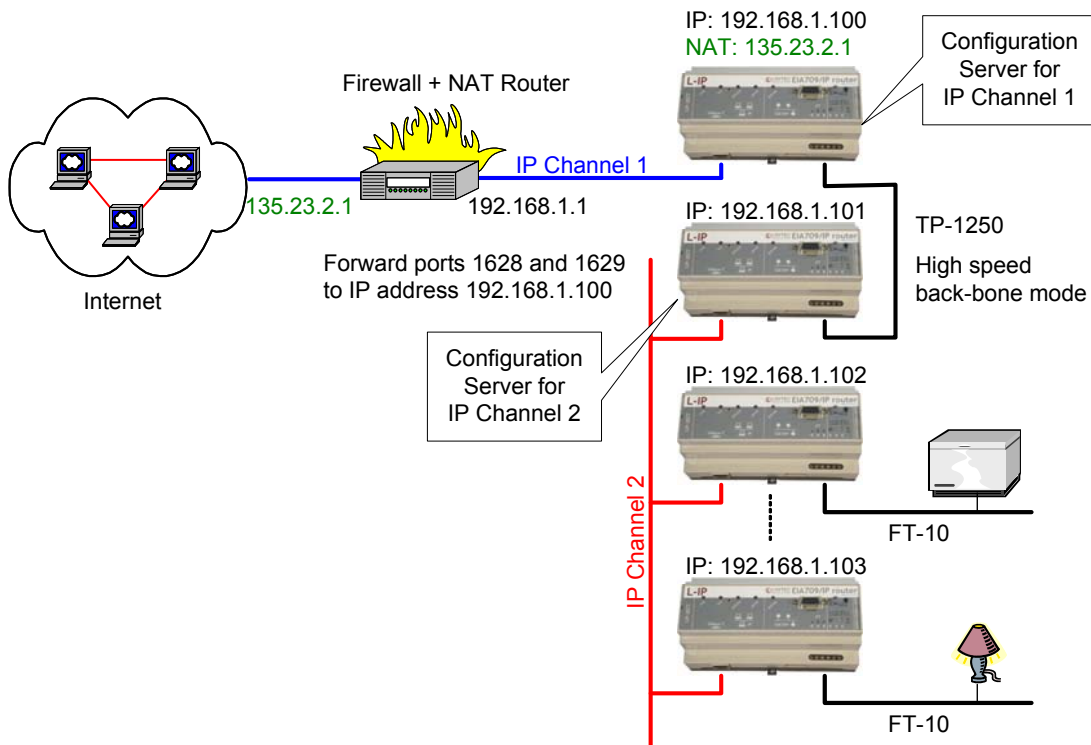


Figure 64: Application that uses multiple L-IP devices behind a NAT router firewall.

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 64 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.

6.4 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.

6.5 Multi-Cast Configuration

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

From firmware version 3.0 and up 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 EIA-852 device statistics in the statistics menu (Section 5.4). The entry "Channel Routing Mode" reads SL (send list) if packets are routed to the multi-cast group. It reads CR (channel routing) if the normal unicast method is employed. Also the entry "Multi-cast packets sent" in the EIA852 device statistics menu (Section 5.4) counts the number of multicast packets transmitted to the group. If this item remains zero, no multi-cast is used by the L-IP.

7 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 EIA-709 router.

Before the L-IP can start routing EIA-709 packets over IP channels, the L-IP must be added to a CN/IP channel. Please refer to Section 7.4 on how to add the L-IP to a CN/IP channel.

7.1 L-IP Acts as a Standard EIA-709 Configured Router

Installing and operating the L-IP is like a standard EIA-709 router when used in the factory default state.

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

After adding the device to a CN/IP 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/english/download/lip.htm>.

The multi-port L-IP contains multiple standard EIA-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 65 shows an example for the multi-port L-IP (LIP-33ECTB).

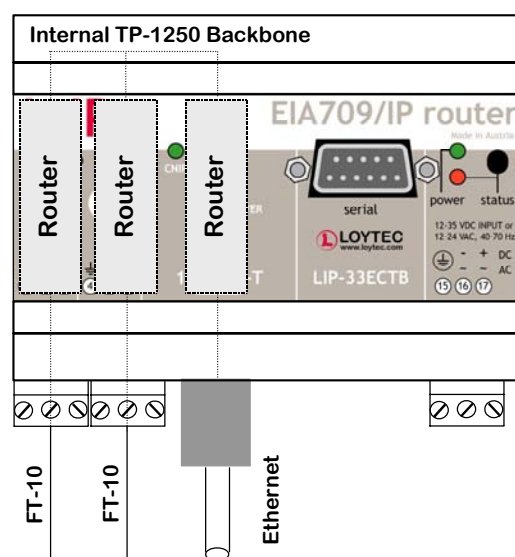


Figure 65: Internal structure of the multi-port L-IP in EIA-709 router mode.

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.

7.2 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 3.6 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 a CN/IP 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 EIA-709 Router network management commands. However, it accepts all other standard network management commands (e.g. to set the channel parameters on every port).

7.3 Creating and Managing a CN/IP Channel

An EIA-709 device that is directly connected to an IP channel (Intranet, Internet) must be managed by a so-called configuration server. A configuration server keeps a list of all devices on a logical CN/IP channel and distributes the routing information between those devices. If a device wants to join a CN/IP 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. Please refer to the following sections on how to setup the device and the configuration server.

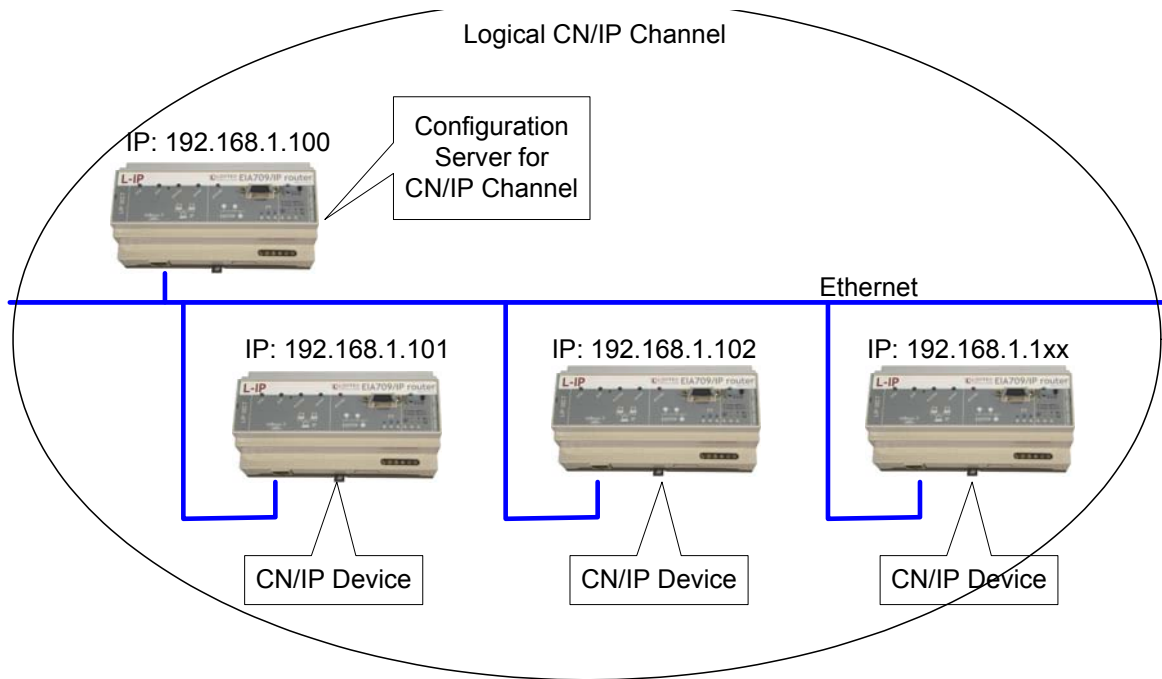


Figure 66: The configuration server manages the devices on a CN/IP channel.

7.4 Setting up an L-IP Device

Every device that connects to a CN/IP channel must have proper IP settings (see Section 4.6) before it can contact a configuration server. Proper IP settings are set through the console interface or the web interface.

There are 2 different scenarios how a device can join a CN/IP 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.

7.4.1 Configuration Server Contacts L-IP Device

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

- ◆ IP address/netmask/gateway (either via DHCP or manual entry), see Section 4.6
- ◆ Auto-NAT or manual NAT address if used behind a firewall/NAT router, see Section 4.6
- ◆ MD5 secret if authentication is required, see Section 4.7

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

Note! If the built-in configuration server is used the configuration server always contacts the device as described in this Section.

7.4.2 L-IP Device Contacts Configuration Server

In this scenario the L-IP 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 4.6
- ◆ Auto-NAT or manual NAT address if used behind a firewall/NAT router, see Section 4.6
- ◆ MD5 secret if authentication is required, see Section 4.7
- ◆ Configuration server IP address and port number, see Section 4.7.1

Note! If the built-in configuration server is used the configuration server always contacts the device as described in Section 7.4.1.

If the “Auto member” feature is enabled in the configuration server, the CN/IP device can add itself to the CN/IP channel without explicitly adding the device at the configuration server. Note, that enabling auto member is a potential security hole since all devices can add themselves to the CN/IP channel.

7.5 Using the Built-In Configuration Server

The L-IP has a built-in configuration server that can manage one CN/IP channel and up to 256 devices on this CN/IP channel. The L-IP can act as a device and a configuration server at the same time. In order to activate the configuration server the L-IP must have the following parameters set.

- ◆ IP address/netmask/gateway (either via DHCP or manual entry), see Section 4.6
- ◆ NAT address if used behind a firewall/NAT router, see Section 4.6
- ◆ MD5 secret if authentication is required, see Section 4.7
- ◆ Enable the configuration server, see Section 0 (server LED lights up green)
- ◆ A list of CN/IP channel members, see Section 4.8.11

For security purposes the configuration server contacts each CN/IP device on the CN/IP channel. Therefore one must enter a list of all channel members in the EIA-852 Server Configuration Menu. This ensures that no unwanted device can join the CN/IP channel. A properly configured CN/IP channel list can look like Figure 67.

```
List of channel members
=====
```

No	Name	IP Address	Status	Flags
000	local	128.168.1.253:1628	registered	

NAT Router		128.168.1.250		
+ 001	lip-n1	10.0.2.2:1628	registered	
+ 002	lip-n2	10.0.2.3:1631	registered	

003	pc37	128.168.1.37:1628	not responding	

Press <RETURN> to continue

Figure 67: Properly configured CN/IP channel with 4 channel members.

Note that also i.LON 1000/600, VNI and LOYTEC NIC852 based network nodes (e.g. LonMaker or NL-220 applications) can join the CN/IP channel managed by the L-IP.

Note that the built-in configuration server should be used if L-IP devices are communicating across firewalls/NAT routers.

For adding multiple devices behind a NAT router the L-IP configuration server supports the extended NAT mode (see Section 6.3.2). The L-IP CS 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 L-IP CS, because the i.LON 600 does not switch to that mode automatically.

7.6 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 EIA-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 6.3.2) 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.

7.7 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/english/download/lip.htm>.

Detailed instructions on how to use the L-IP together with LNS based network management tools can be found in Section 12.2.

7.8 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 EIA-709 networks. Therefore the EIA-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.

First add the IP address of the PC to the configuration server's list of devices (see Section 7.4.1). Then select the LonWorks/IP Channels utility program from your Control Panel.

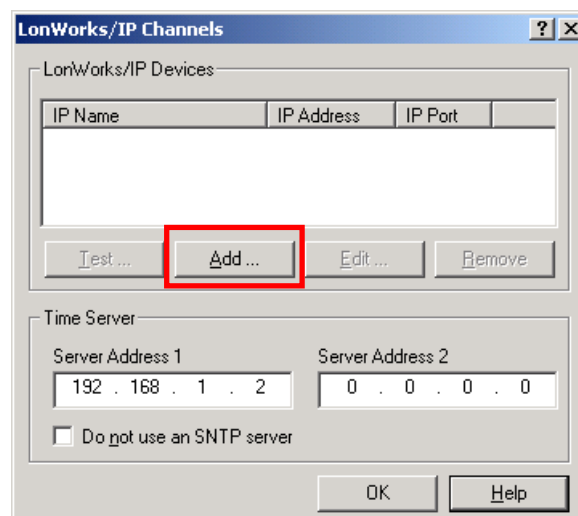


Figure 68: Add a new LNS IP interface to your PC.

Click on *Add*

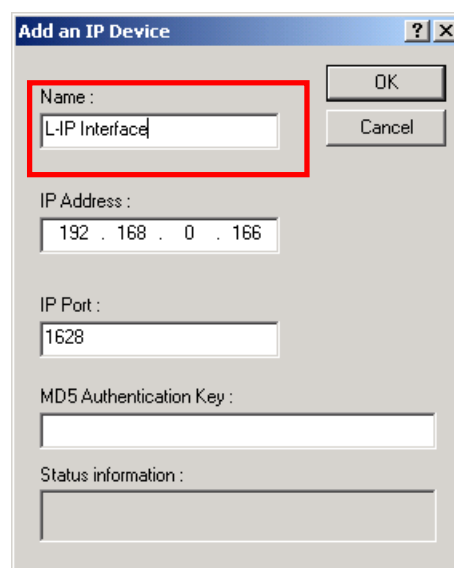


Figure 69: Give the new interface a name.

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*. You should now see a window like Figure 70. Set the timeserver fields to 0.0.0.0 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.

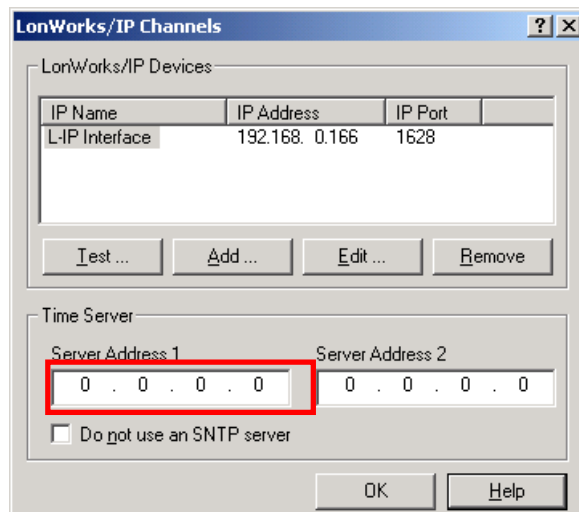


Figure 70: Disable the SNTP server if you have a local NTP client installed on your PC.

If you already have an NTP client installed on your PC, which synchronizes your PC clock to an NTP timer server, you must select “Do not use an SNTP server” otherwise this NTP client will compete with the NTP client already installed on your PC.

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

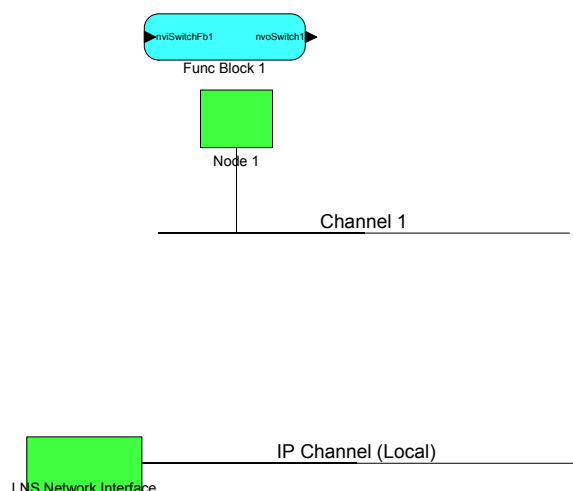


Figure 71: Move the LNS Network Interface to the newly created IP Channel.

If the L-IP is used as an EIA-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 71 by selecting the LNS Network Interface and choosing “Change Channel” from the context menu.

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 72.

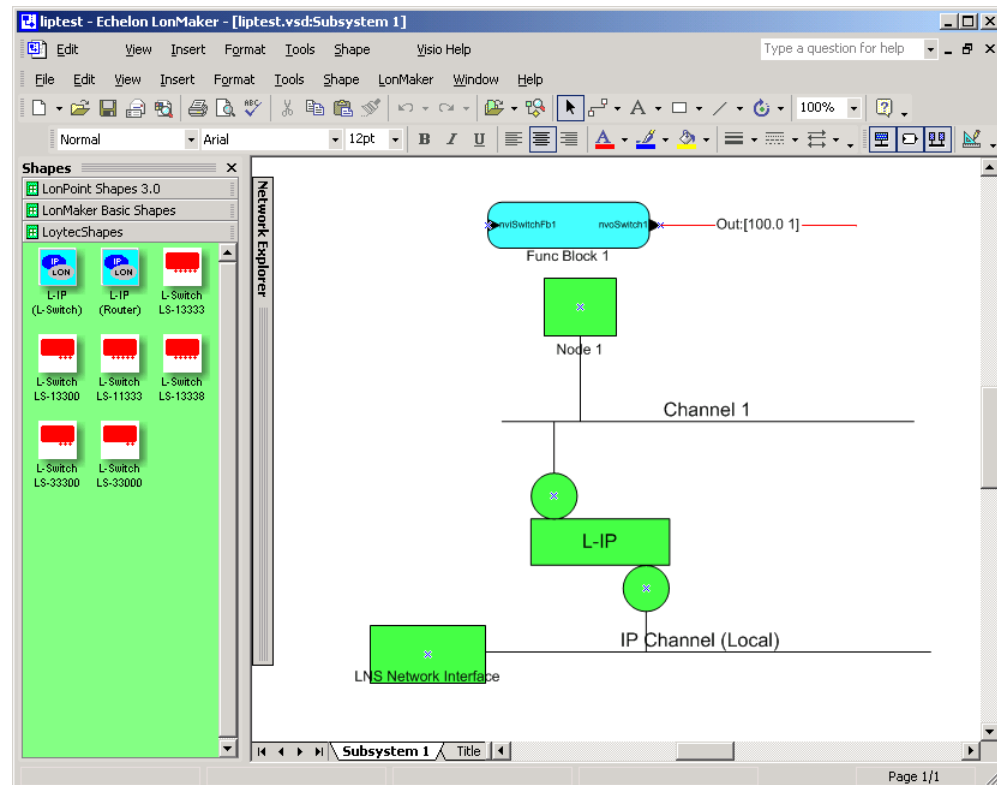


Figure 72: Drag the L-IP (Router) shape onto the drawing area and commission the device.

7.9 Remote LPA Operation

Starting with firmware version 2.0 the L-IP supports remote LPA access. This means that a protocol analyzer connected to the Ethernet network can connect to the L-IP and record all packets on the EIA-709 channel (FT-10 or TP-1250). Our LPA-IP supports this sophisticated feature. The principle functionality is shown in Figure 73.

The LPA-IP runs on a Windows PC that is connected to the Ethernet network. In a L-IP 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 CN/IP channel. Note that this functionality is only possible with L-IP Internet routers.

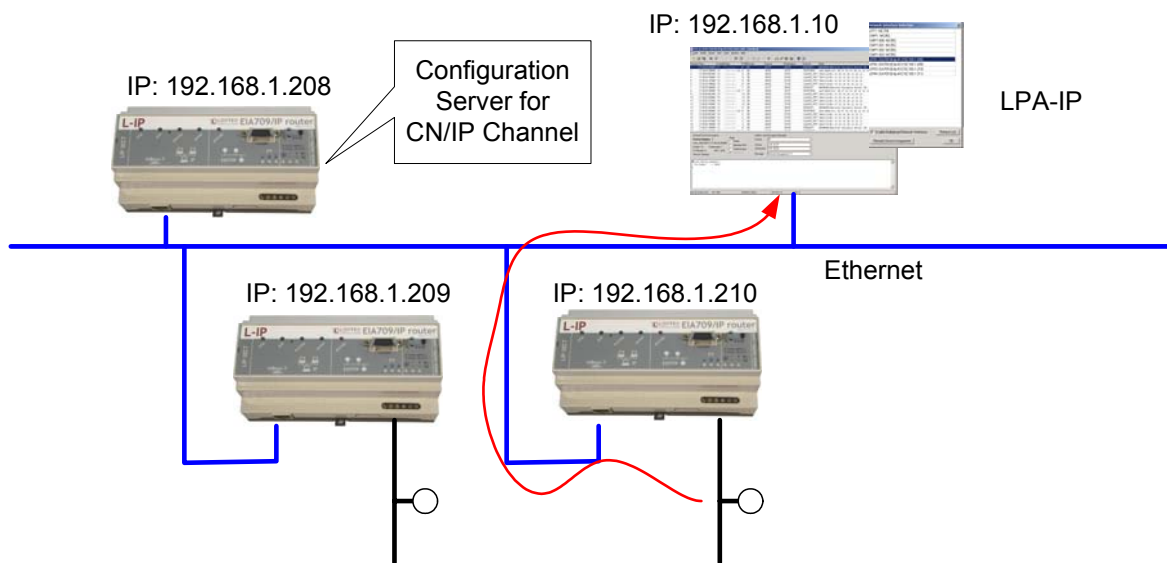


Figure 73: Remote LPA principle.

7.10 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 client device whereas the Channel Delay is a channel property of LNS and can be set in LonMaker or other network management tools.

Table 16 summarizes the timing values that must be set when operating the L-IP under WAN conditions.

Timing Parameter	Value
Channel Timeout	Average ping delay + Aggregation Timeout
Escrowing (Packet Reorder Timer)	The smaller value of: $0.25 \times \text{Channel Timeout}$ or 64ms
Aggregation Timeout (Packet Bunching)	Typ. 16 ms
Channel Delay in LonMaker	Average ping delay +10% + $2 \times \text{Aggregation Timeout}$

Table 16: Advanced CN/IP timing parameters.

Please use a PC to determine the average ping delay between the different L-IPs in the network. If multiple L-IPs are communicating with each other always use the largest measured average ping delay for the input value for the calculations in Table 16.

Escrowing should be disabled in a LAN (0 ms). The Channel Delay in LonMaker should be set to $2 \times \text{Aggregation Timeout}$ 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.

7.10.1 Channel Timeout

The Channel Timeout is a property of the CN/IP channel. If a packet travels across this CN/IP channel for longer than what is specified in Channel Timeout in ms the packet is discarded.

The L-IPs always needs to synchronize with a 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. Set Channel Timeout to 200 ms and Channel Delay to 20 ms in a LAN environment.

Please refer to Section 4.8.6 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 L-IP will drift apart and communication between the PC and the L-IP will terminate.

7.10.2 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 EIA-709 nodes. Please consult the documentation for your network management tool about the Channel Delay details.

7.10.3 Escrowing Timer (Packet Reorder Timer)

The Escrowing Timer or Packet Reorder Timer is a CN/IP 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 CN/IP devices if a packet is lost or destroyed.

If enabled or disabled, out-of-sequence packets are never sent to the EIA-709 channel. Please refer to Section 4.7.6 on how to enable or disable escrowing.

7.10.4 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 CN/IP networks like the Internet with possibly long packet delays one must specify a SNTP server to synchronize the local clocks of the L-IP devices. The local clocks must be synchronized to a common notion of time in order to make CN/IP protocol features like escrowing (Channel Timeout) work properly.

The SNTP timeserver can be specified on the CN/IP channel level in the configuration server, which distributes the timeserver address to all CN/IP devices on the CN/IP channel.

A primary and a secondary SNTP server can be defined, please refer to Section 4.7.5 and Section 4.8.5 on how to enable the SNTP server.

7.11 Advanced Topics

7.11.1 Aggregation

Aggregation (or packet bunching) is a technique that collects multiple EIA-709 packets into a single larger CN/IP packet. Aggregation improves overall system performance since one CN/IP packets now carries multiple EIA-709 packets und with the same number of CN/IP transactions more EIA-709 packets can be exchanged between L-IP devices thus reducing protocol overhead. The Aggregation Timeout defines the time period in ms in which the transmitting device collects the EIA-709 packets before it transmits the CN/IP packet over the CN/IP channel. Please refer to Section 4.7.7 on how to enable aggregation. Note, that aggregation adds a delay to the transactions but dramatically improves the throughput of your CN/IP channel. Use aggregation if you have a high channel load but can tolerate some additional propagation delay given by the aggregation time value.

7.11.2 MD5 Authentication

MD5 authentication is a method to verify 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 CN/IP channel. Please refer to Section 4.7.8 and Section 4.8.9 for details.

7.11.3 DHCP

When using DHCP with firmware versions 1.0 and 1.1 the DHCP server must be active and the L-IP Ethernet cable must be connected when the L-IP powers up otherwise the L-IP will not receive a valid IP address. Furthermore the DHCP Server must provide the IP settings with an infinite lease time otherwise the L-IP will reject those IP settings from the DHCP server.

With firmware version 2.0 and higher the only restrictions for the use of DHCP is that 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.

7.11.4 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 L-IP would need to be updated. The Auto-NAT feature in L-IP firmware versions 2.2 and up permanently monitors the current NAT address. When the L-IP detects a change in the NAT address it re-registers with the L-IP CS using this new address. This feature requires an L-IP configuration server and “Roaming Members” enabled on that CS.

A consequence of this monitoring process is that the L-IP 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, then 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 L-IP Redundant

8.1 Redundancy and Fault Detection in EIA709.1 Networks

8.1.1 Reasons for Communication Failures

Figure 74 shows typical reasons for communication failures in EIA-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).

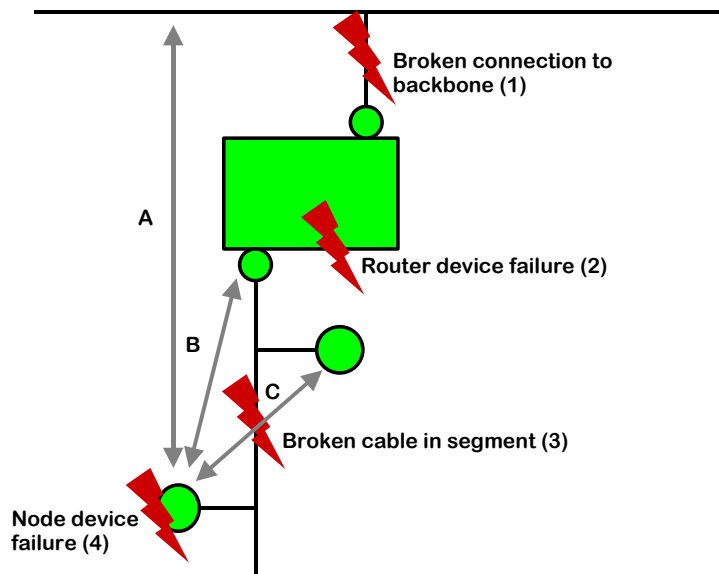


Figure 74: Typical reasons communication failures in EIA709 networks

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).

8.1.2 Conventional Strategies for Redundancy

Although EIA-709.1 allows to introduce redundancy by allowing for a pair of conventional EIA-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 EIA-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 extent “1. Broken connection on the backbone”².

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

8.2 L-IP Redundant Operating Modes

8.2.1 Bus Loop Monitoring

To achieve redundancy against “3. Broken cable in the segment” (see Section 8.1.1) the L-IP allows to build a ring structure by connecting both ends of the bus cable to the L-IP Redundant (see Figure 75).

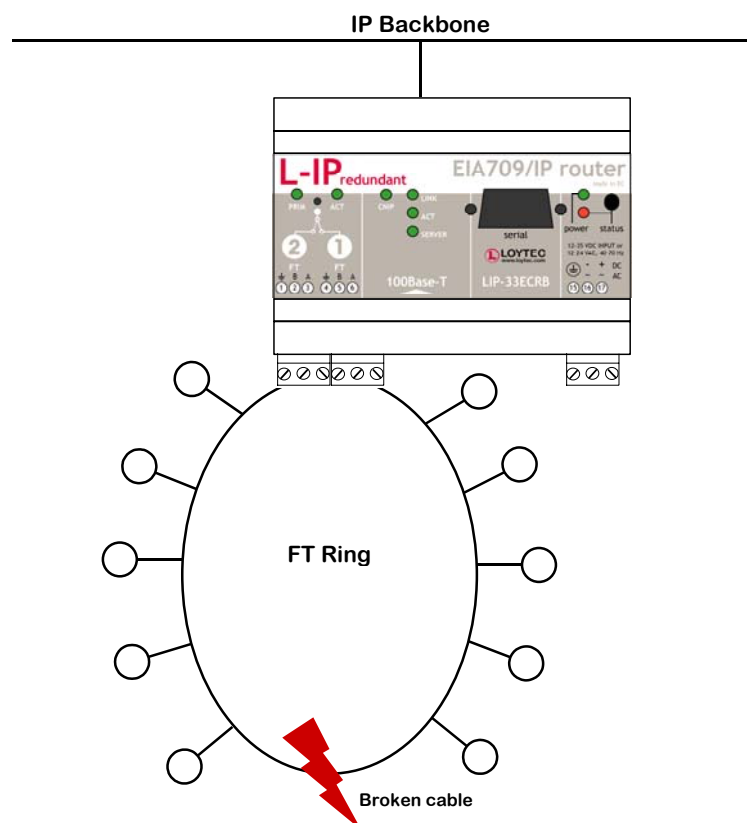


Figure 75: L-IP Redundant with Bus Loop Monitoring

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 loop port 1 to loop port 2 and vice versa. Further an alarm is issued (see Sections 8.5.5 and

² Assuming a redundant backbone.

8.6.3). 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 8.5.7) or the web interface (see Section 8.6.5).

The current bus loop monitoring state can be determined via network variables (see Section 8.7), in the L-IP Redundant plug-in (see Section 8.5.3), and in the web interface (see Section 8.6.1).

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 8.5.4 and 8.6.1).*

8.2.2 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 76). 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”.

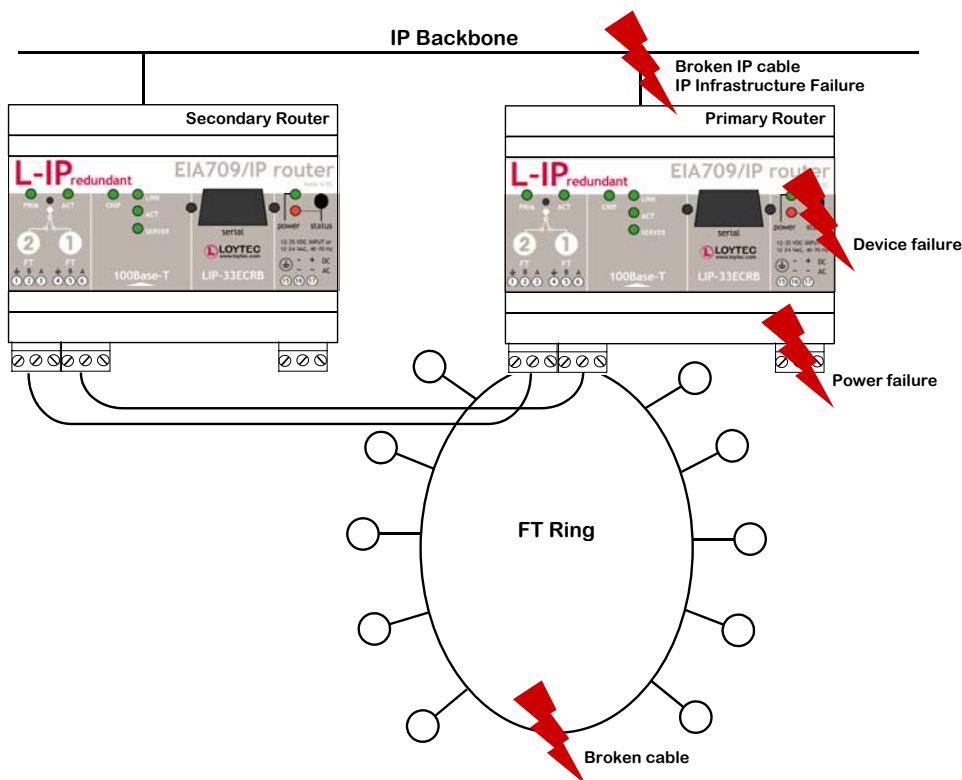


Figure 76: Router Redundancy with two paired L-IP Redundant routers

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 EIA-709 and on the EIA-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 8.2.1).

To enable router redundancy both routers must be commissioned and added to the same EIA-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 8.4.3.2 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 8.5.7) or the web interface (see Section 8.6.5).

The current router state can be determined via network variables (see Section 8.7), in the L-IP Redundant plug-in (see Section 8.5.3), and in the web interface (see Section 8.6.1).

8.2.3 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 8.7), in the L-IP Redundant plug-in (see Section 8.5.4), and in the web interface (see Section 8.6.1).

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 8.5.6) or the web interface (see Section 8.6.4). 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 8.7), in the L-IP Redundant plug-in (see Section 8.5.3), and in the web interface (see Section 8.6.1). In addition the web interface shows detailed statistic information for each node (e.g. number of CRC errors).

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

If bus loop monitoring is enabled (see Section 8.2.1) 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.

8.3 The L-IP Redundant in a Network

As shown in Figure 77 the L-IP Redundant internally consists of a standard EIA-709 router and an diagnostic node. The router routes packets between the EIA-709 and the EIA-852 channels, while the diagnostic node performs monitoring tasks (e.g. node monitoring) and offers network variables to show the results of these diagnostics.

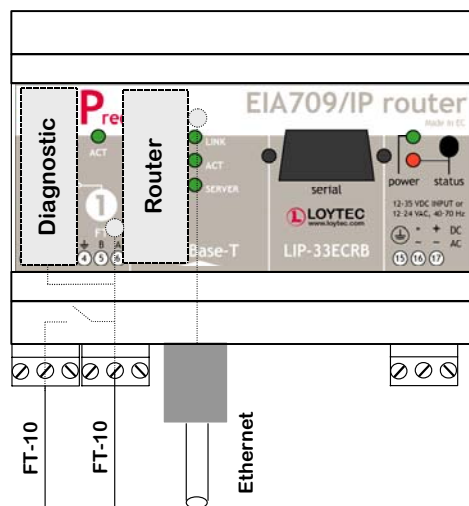


Figure 77: Internal structure of the L-IP Redundant

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 EIA-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 8.4.1).

8.4 Installation

8.4.1 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 8.2.3), 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 or Windows 2000.

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.



Figure 78: Be sure to be logged in as Administrator on Windows 2000/XP

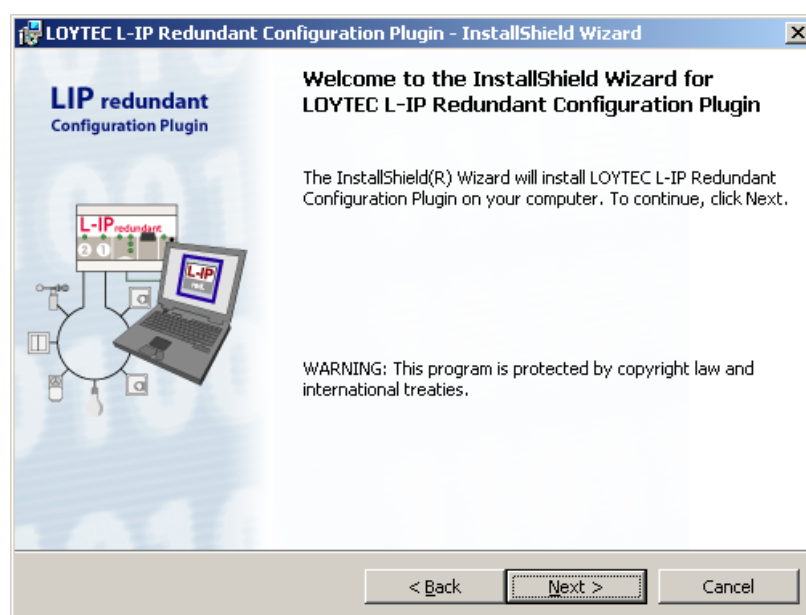


Figure 79: L-IP Redundant Plug-In welcome screen

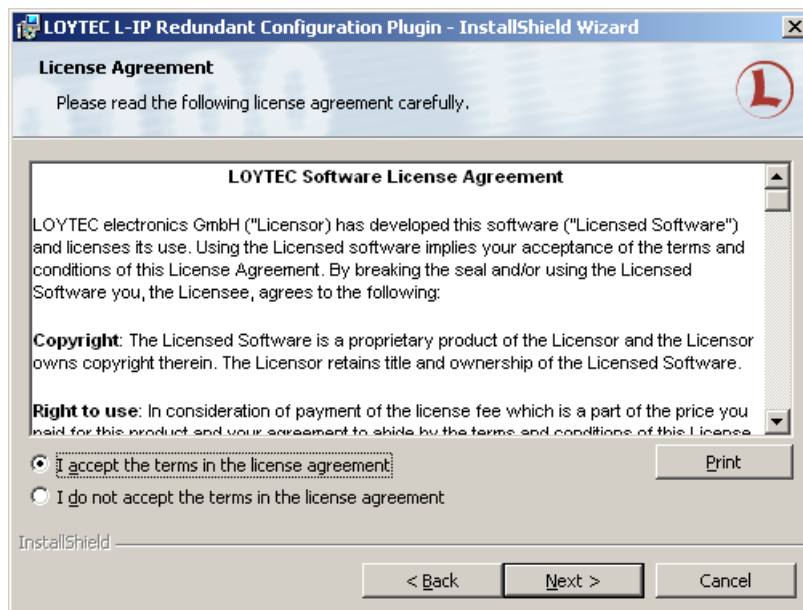


Figure 80: You have to agree to the Software License Agreement

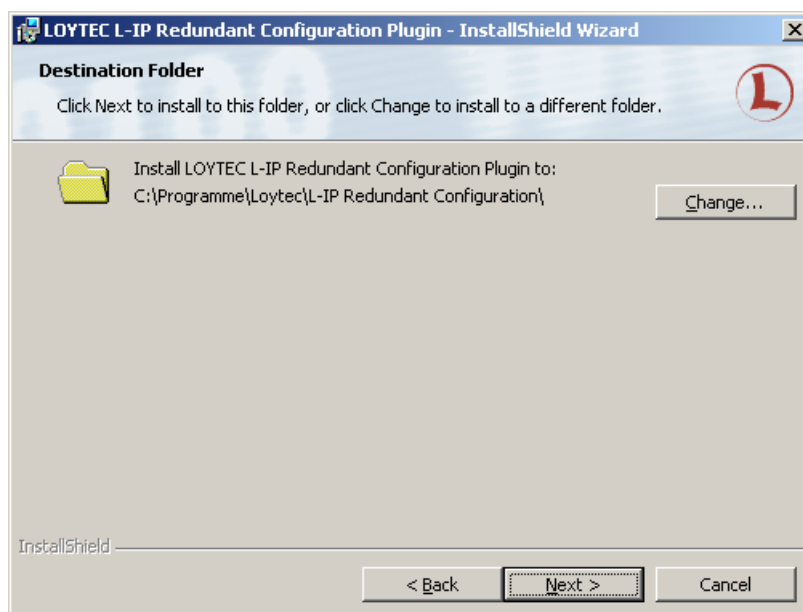


Figure 81: Choose the destination directory

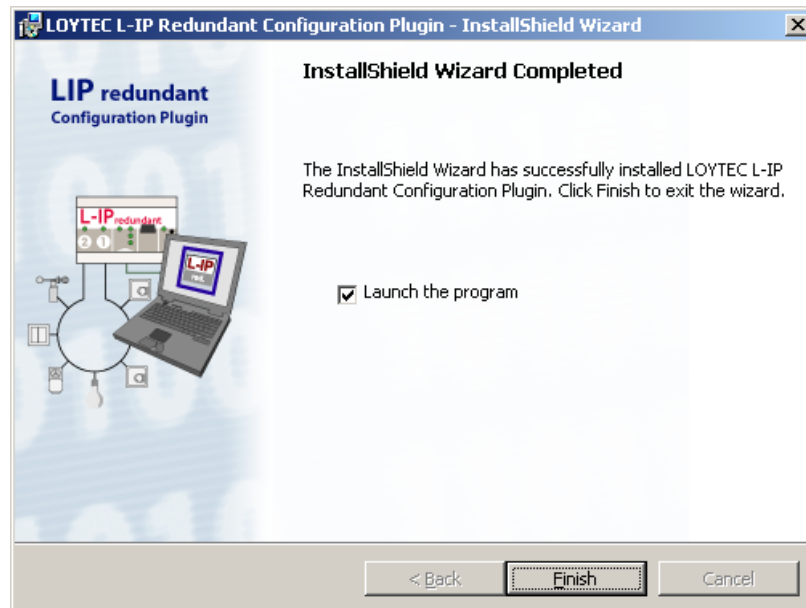


Figure 82: The Plug-In has been successfully installed

8.4.2 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.

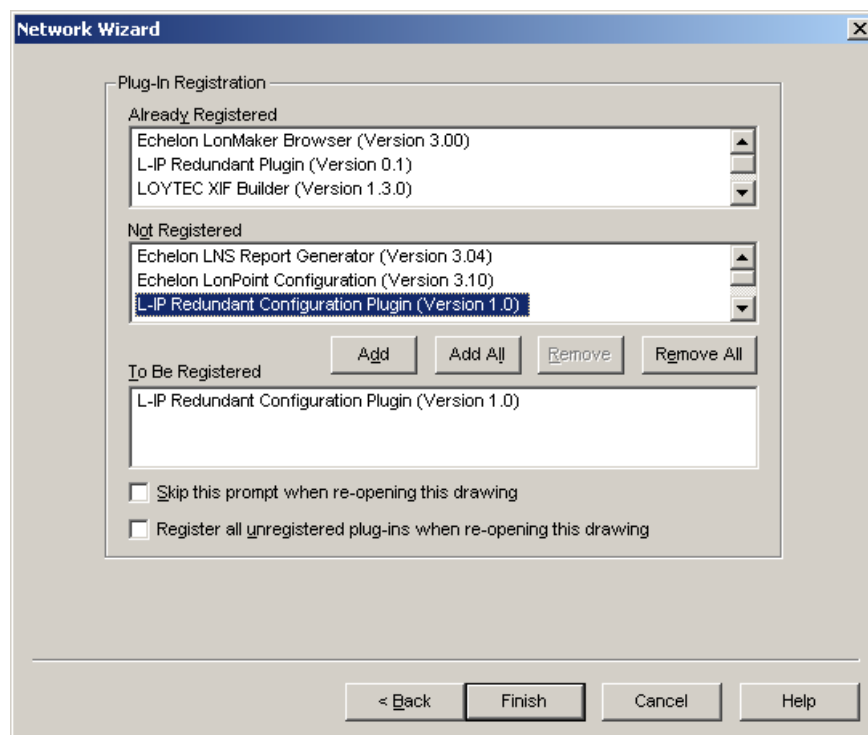


Figure 83: Select the Plug-in to be registered and click Add

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 83). 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”.

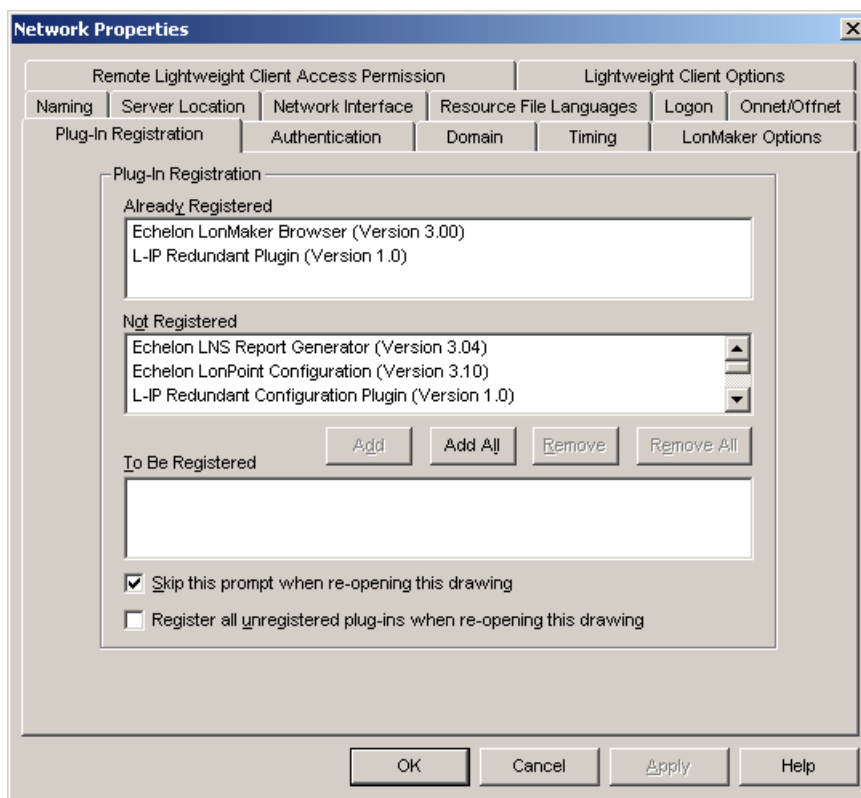


Figure 84: Double check that the L-IP Redundant Configuration Plug-In is properly registered

8.4.3 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..

8.4.3.1 L-IP Redundant Standalone

For operating the L-IP Redundant in standalone mode (see Figure 75), 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 8.4.1).

If using LonMaker for Windows the resulting drawing should look like shown in Figure 85.

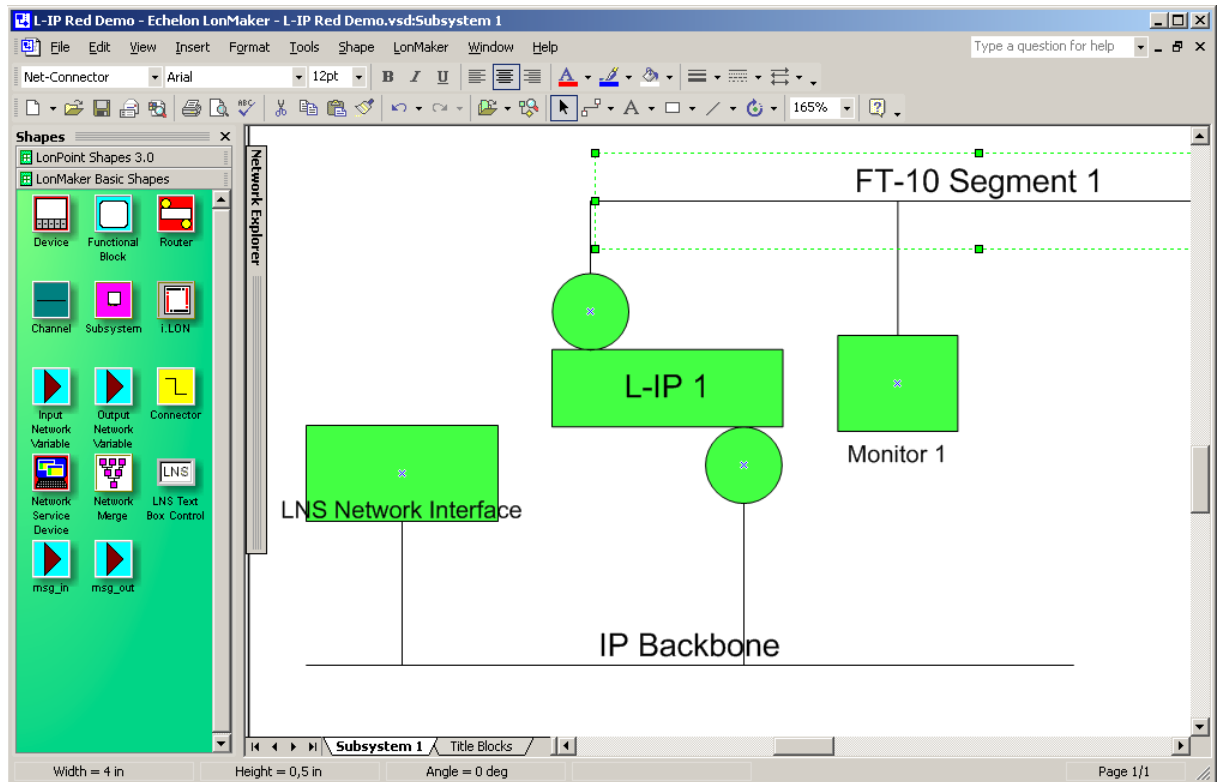


Figure 85: A single L-IP Redundant device configured for standalone operation

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

8.4.3.2 L-IP Redundant with Router Redundancy

For operating the L-IP Redundant in twin router mode (router redundancy, see Figure 76), 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 8.4.1).
- ◆ 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 86.

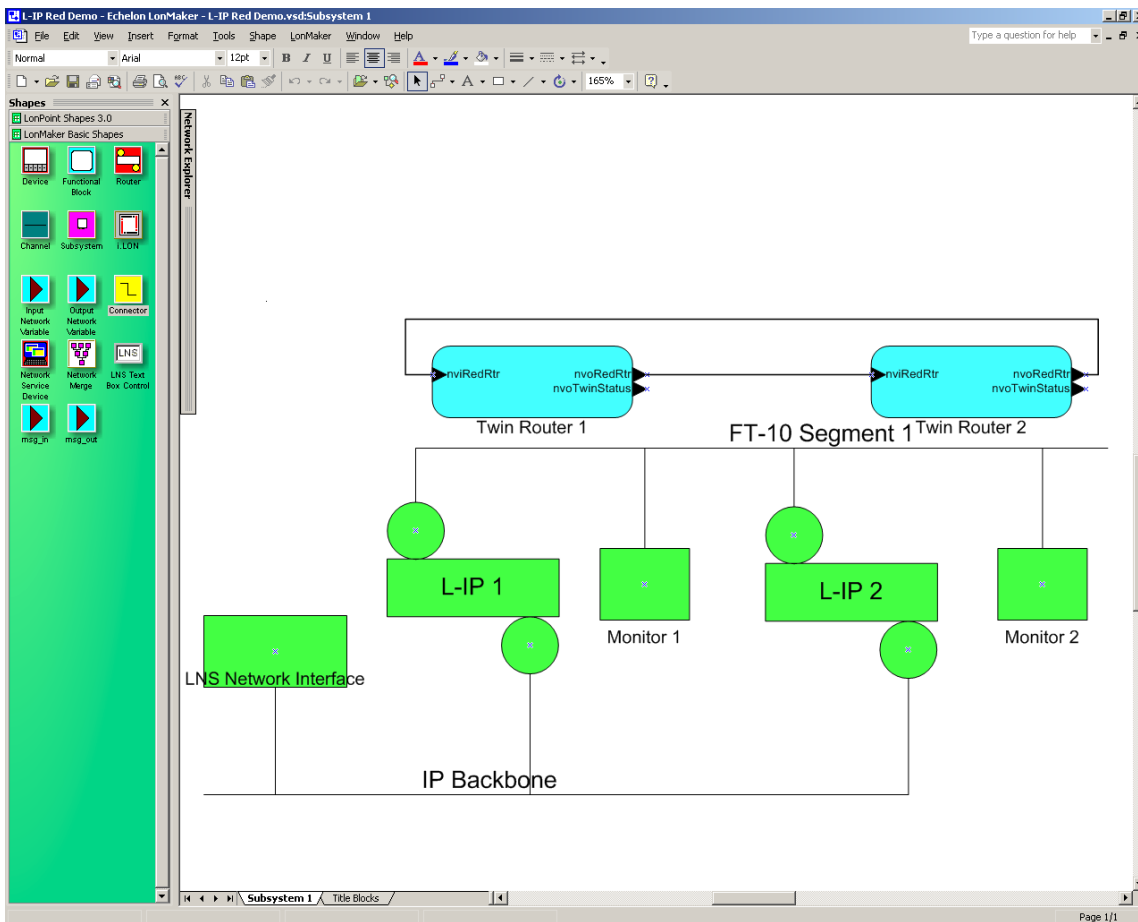


Figure 86: A pair of L-IP Redundant devices configured for twin router operation

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 8.2.1) 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 8.5) or the web interface (see Section 8.6) to enter a node list for node monitoring or to change the parameters for bus loop monitoring and twin router monitoring.

8.5 L-IP Redundant Plug-In

8.5.1 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 2 operating modes of your configuration tool.

8.5.1.1 On-line mode

This is the preferred method to use the configuration utility and allows to use 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.

8.5.1.2 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).

8.5.1.3 Standalone mode

The L-IP Redundant Plug-In can also be executed as a standalone program. This operation mode offers least functionality. It allows to create and edit a node list or load, alter and save a configuration file.

8.5.2 Overview

Figure 87 shows the L-IP Redundant Configuration Plug-In. The window is separated in three main areas:

- ◆ The view selection allows to select 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 to select different actions depending on the currently selected view. The standard commands “load”, “save” and “new” are always possible. “Save” allows to store 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.

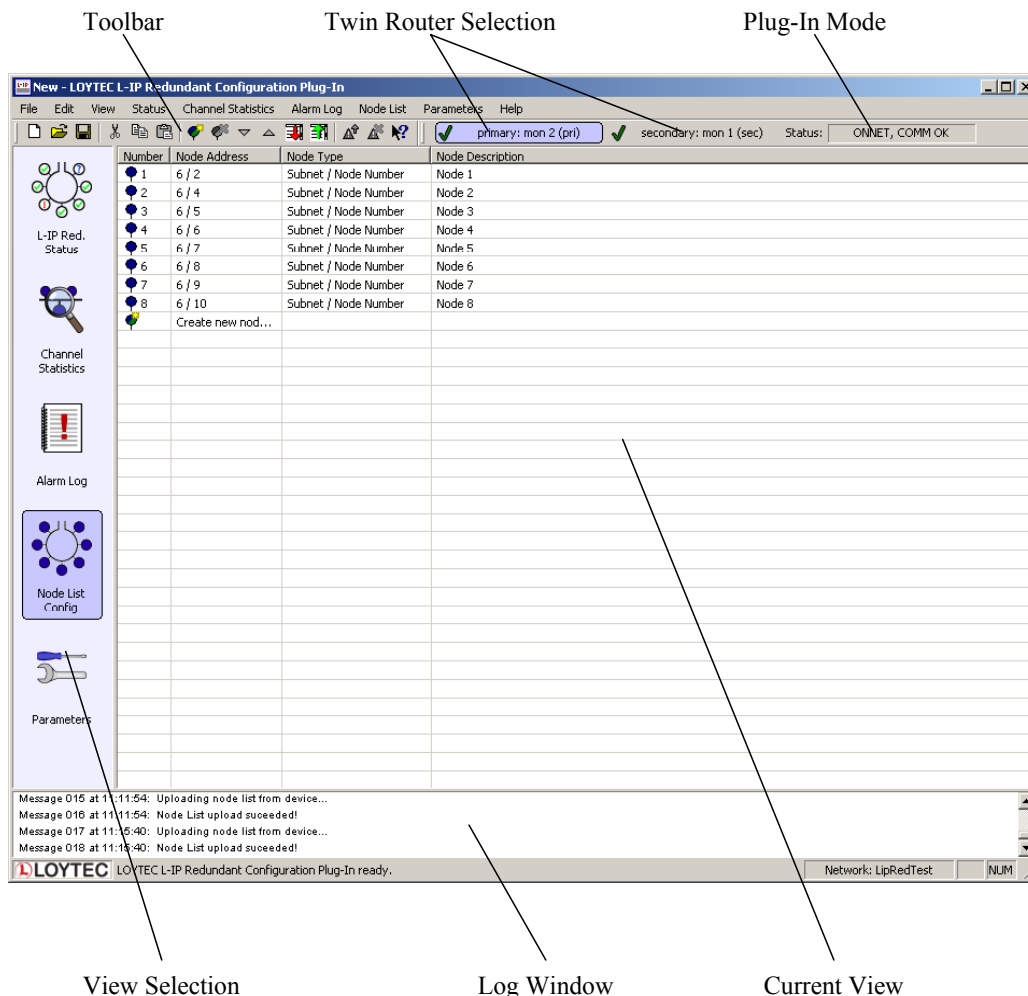


Figure 87: The L-IP Redundant Configuration Plug-In

The “Plug-In Mode” shows the operation mode of the plug-in (see 8.5.1) and whether the device is accessible over the network.

8.5.3 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 88).

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.

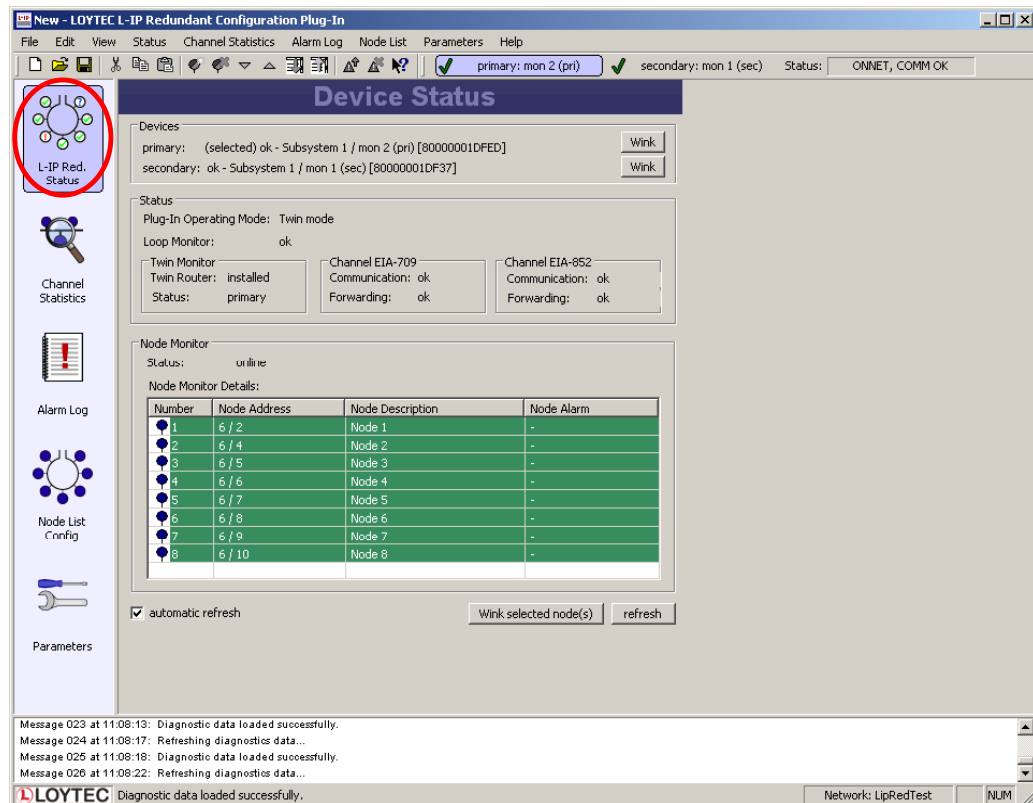


Figure 88: The Device Status View

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 3.4.9). 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.
- ◆ EIA-709/EIA-852 Communication: Shows whether its twin router is reachable via the EIA-709 and EIA-852 segment respectively.

- ◆ EIA-709/EIA-852 Forwarding: Shows whether the device forwards significantly lower amount of packets to its EIA-709 and EIA-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 EIA-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.

8.5.4 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 89).

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.

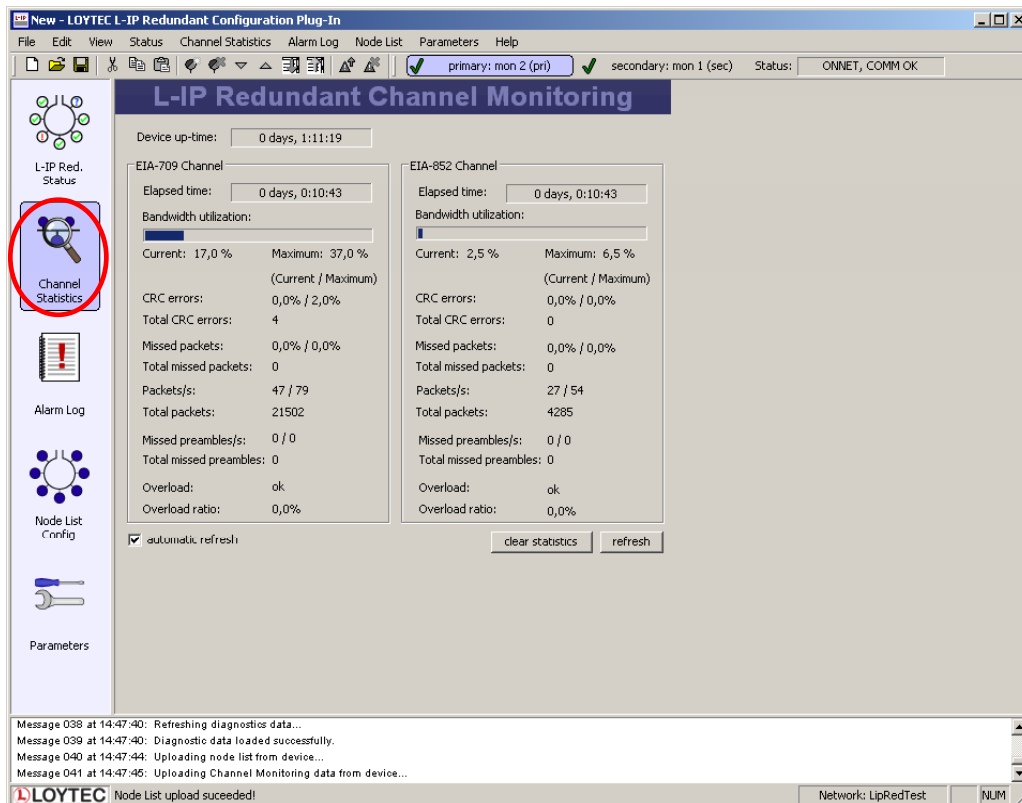


Figure 89: The Channel Statistics View

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 (EIA-709/EIA-852):

Elapsed time

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

8.5.5 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 90).

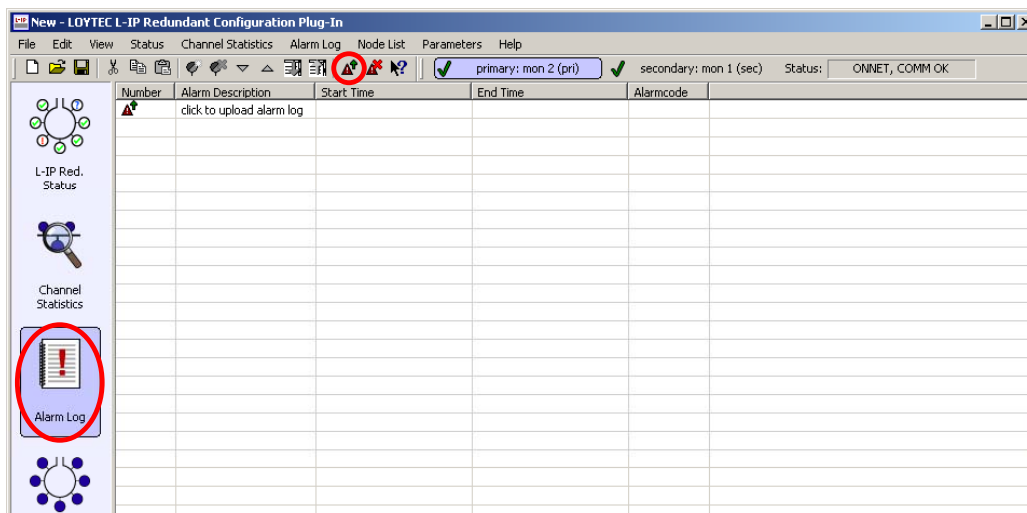


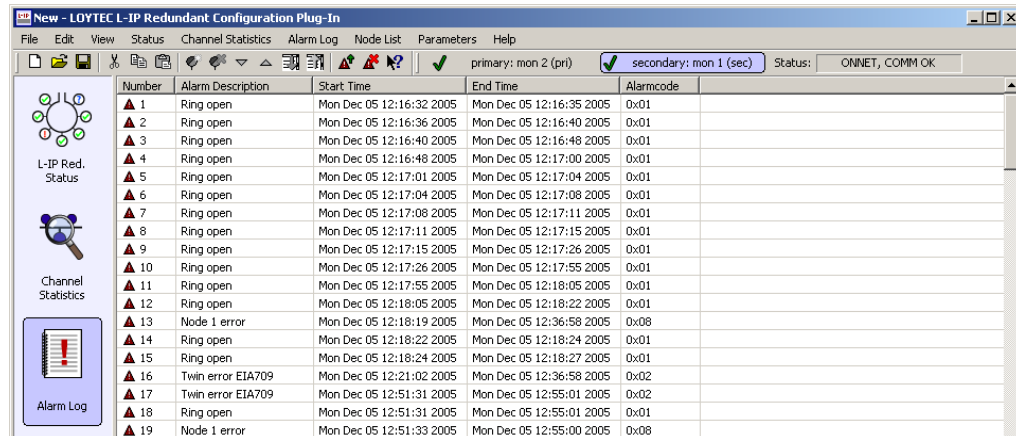
Figure 90: The Alarm Log View

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 90). Similar the alarm log can be cleared.

Figure 91 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 8.2.1).

- ◆ "Twin error EIA709": Twin router is not reachable any more via the EIA-709 side (see Section 8.2.2).
- ◆ "Twin error IP": Twin router is not reachable any more via the EIA-852 side (see Section 8.2.2).
- ◆ "Fwd warning EIA709": Packets forwarded from the EIA-709 to the EIA-852 side on the selected device is significantly lower than on the remote twin router (see Section 8.2.2).
- ◆ "Fwd warning IP": Packets forwarded from the EIA-852 to the EIA-709 side on the selected device is significantly lower than on the remote twin router (see Section 8.2.2).
- ◆ "Fwd error EIA709": The selected device does not forward any packets from the EIA-709 to the EIA-852 side, while the remote twin router does.
- ◆ "Fwd error IP": The selected device does not forward any packets from the EIA-852 to the EIA-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 91: An alarm log

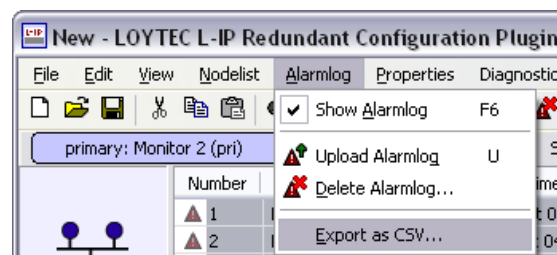


Figure 92: Exporting an alarm log to a CSV-file

The alarm log can be transferred to another application using Copy & Paste or by export to a CSV-file (see Figure 92).

8.5.6 Node List Config

The node list is used for node monitoring (see Section 8.2.3). 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.

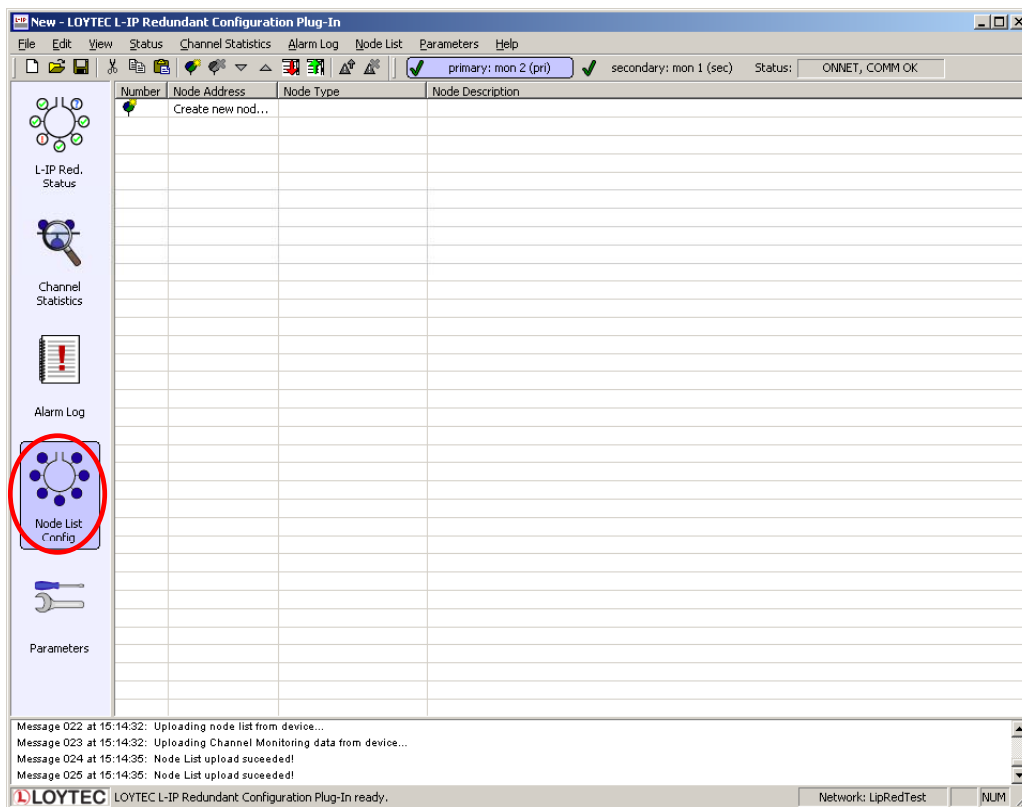


Figure 93: The Node List Config View

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 93).

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.

8.5.6.1 Manually add and edit nodes

You can double click on “Create new node...” to open the new node dialog box (see Figure 94).

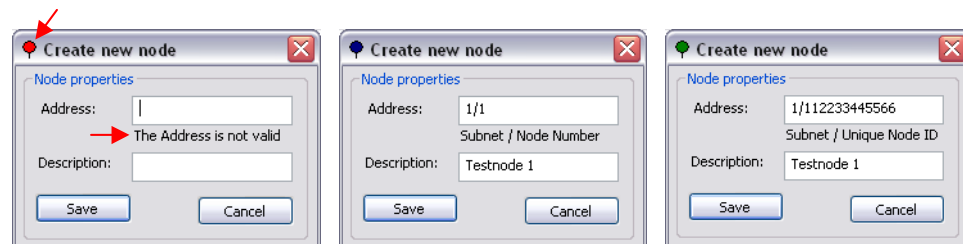


Figure 94: Adding a new node

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.

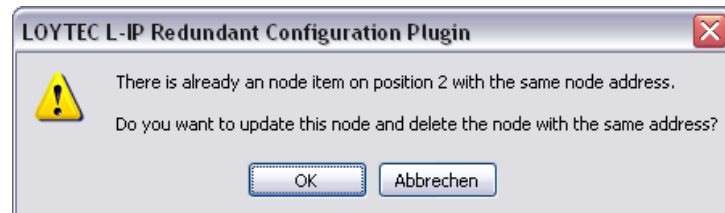


Figure 95: Tried to save entry which is identical to an already existing one

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 95). If you press OK here, entry number 2 will be deleted and entry number 1 updated.

8.5.6.2 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 96).

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.

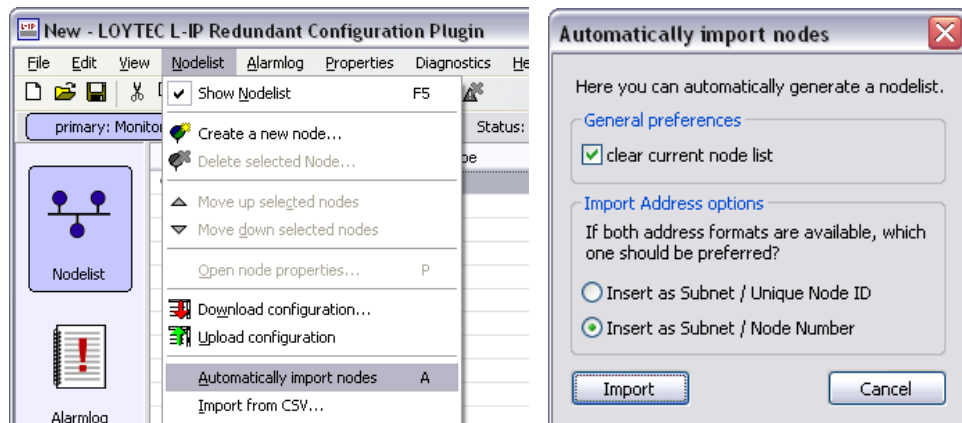


Figure 96: Import node list from LNS database

8.5.6.3 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 97). To select multiple items press the CTRL-key while selecting.

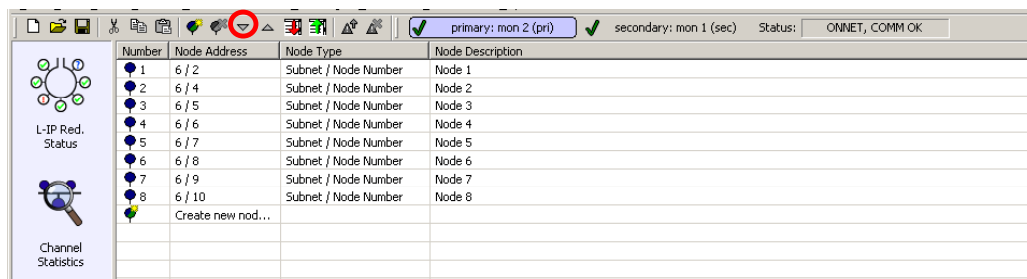


Figure 97: Moving multiple entries in the node list

8.5.6.4 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 98).

Further, the node list can be exported and imported to/from a CSV-file. This allows to use a spreadsheet application (e.g. Microsoft Excel) to create and edit the node list (see Figure 99).

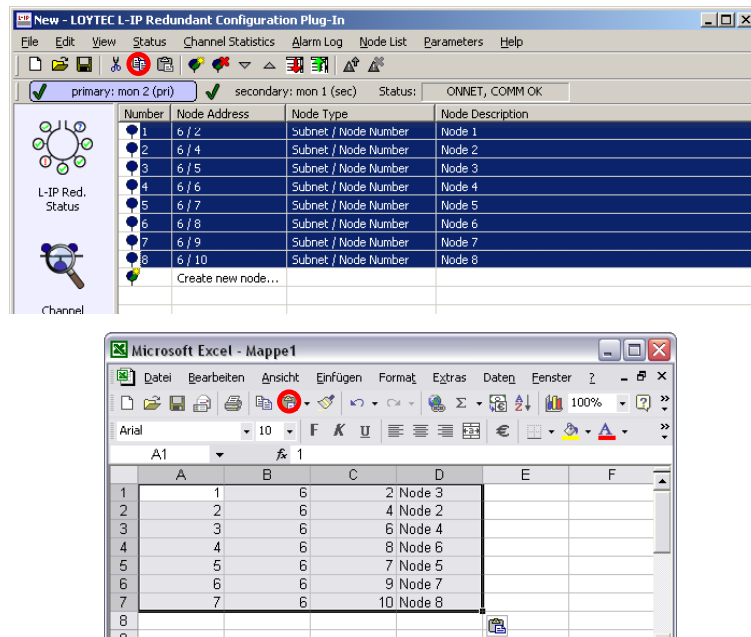


Figure 98: Transfer the node list between applications with Copy & Paste

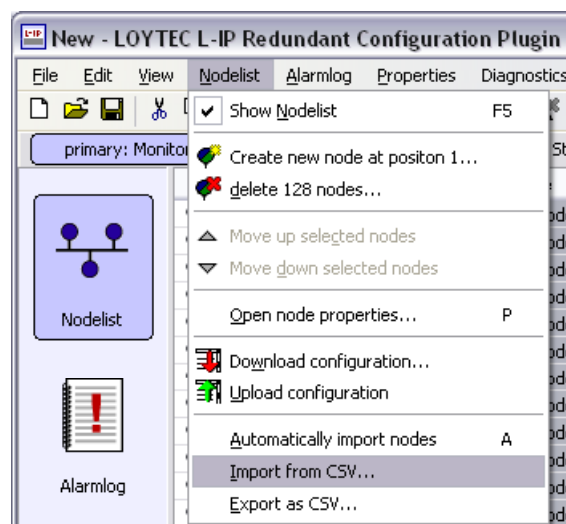


Figure 99: Importing a CSV-file

8.5.6.5 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 100).

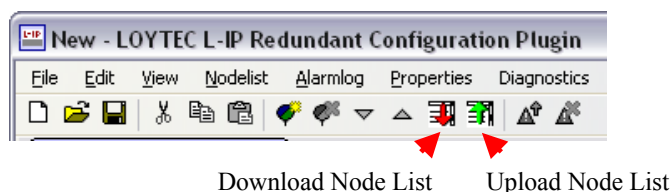


Figure 100: Up- and Downloading the Node List

If the router redundancy is used, a dialog will ask whether to copy the same node list to the twin router (see Figure 101) after the download to the selected device has finished. It is strongly recommended to answer this dialog with “Yes”.

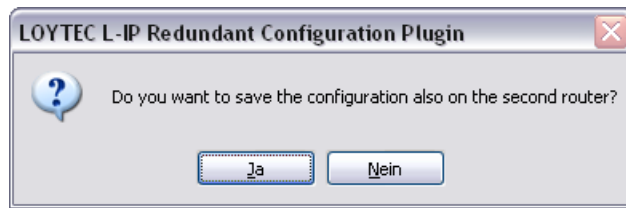


Figure 101: Download the Node List to both routers?

8.5.7 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 102).

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 8.7.1). 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 8.2.1).

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 8.2.2). 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.

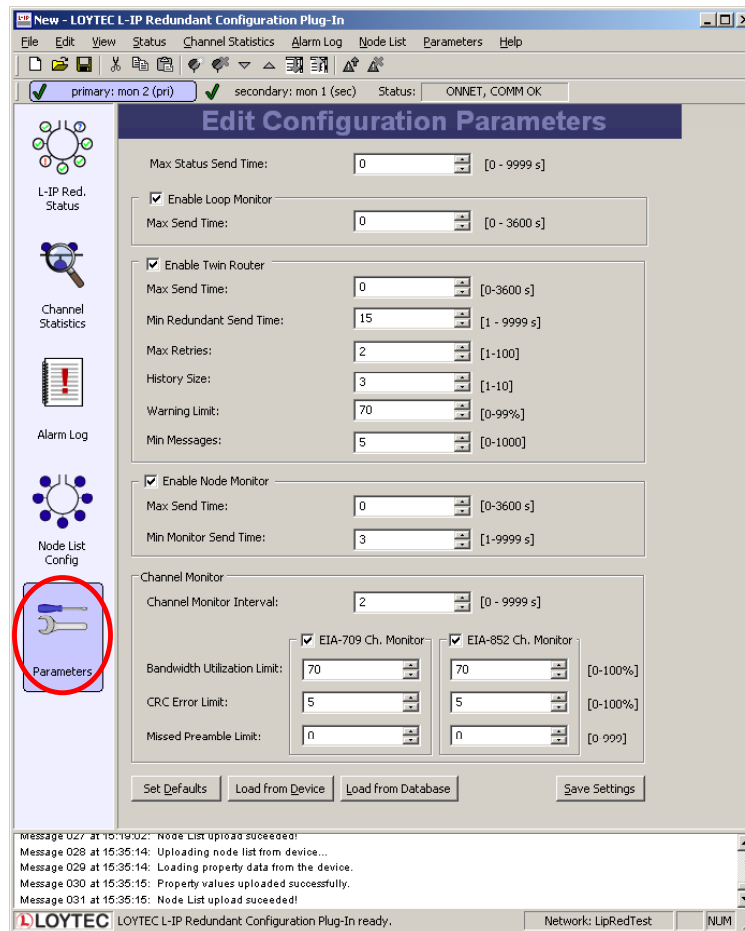


Figure 102: The Parameters View

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:

$$TwinRouterFailureDetectionTime \leq MinRedundantSendTime \times (MaxRetries + 1)$$

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 8.7.4 or alarm log, Section 8.6.3): If the number of packets forwarded by the local

router is less than $\langle Warning Limit \rangle$ % 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 8.7.4 or alarm log, Section 8.6.3): 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 $\langle Min Messages \rangle$ 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 8.2.3).

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 *nvoRingBReceived* 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.

EIA-709 Ch. Monitor/EIA-852 Ch. Monitor

Deselecting these check boxes will disable the corresponding channel monitor object (see Section 8.2.3).

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.

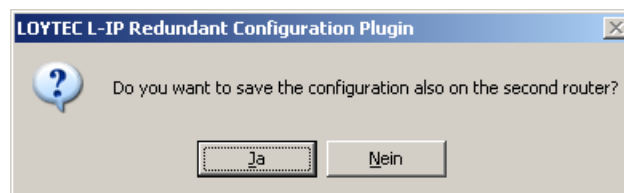


Figure 103: Download configuration to second router?

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 103). 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”.

8.6 Web Interface

On the L-IP Redundant an additional item “Redundant” is found in the main menu of the web interface (see Figure 104). This menu item offers the following submenus:

8.6.1 Status

Figure 104 shows the status page. This page offers similar information as the status view of the L-IP Redundant Plug-In (see Section 8.5.3).

Major differences compared to the plug-in interface are:

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

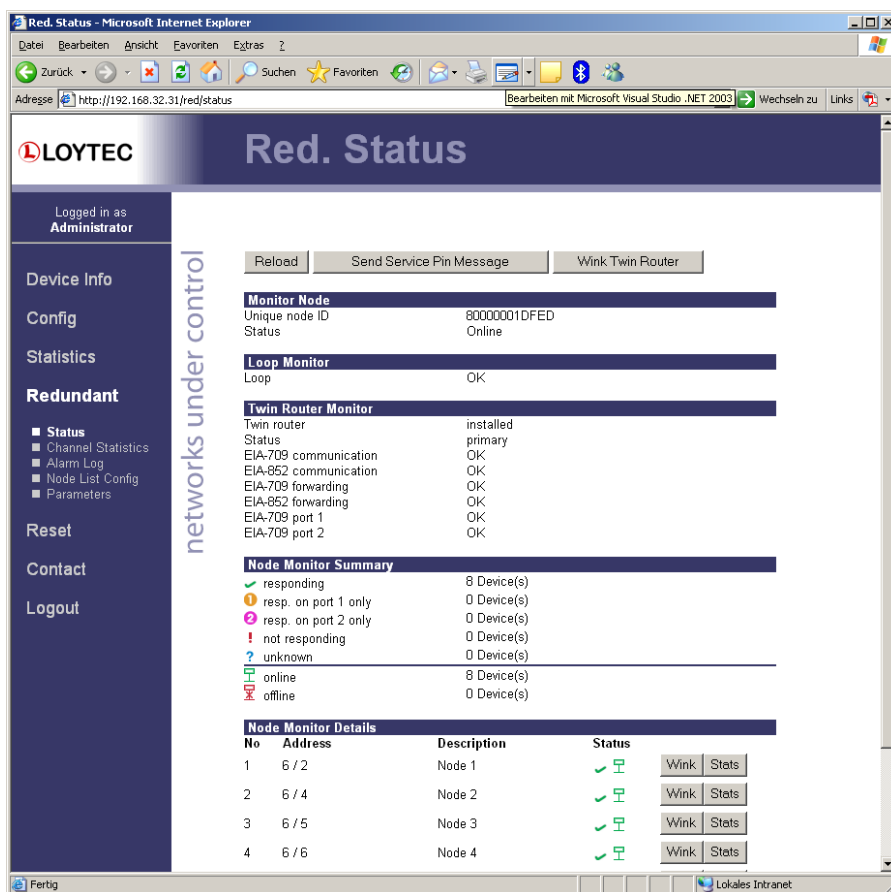


Figure 104: The L-IP Redundant Web Interface – Status Page

- ◆ For each node in the “Node Monitor Details” table, which is responding over the network, a “Stats” button is present. This button allows to view the node statistics of the remote node (see Figure 105).

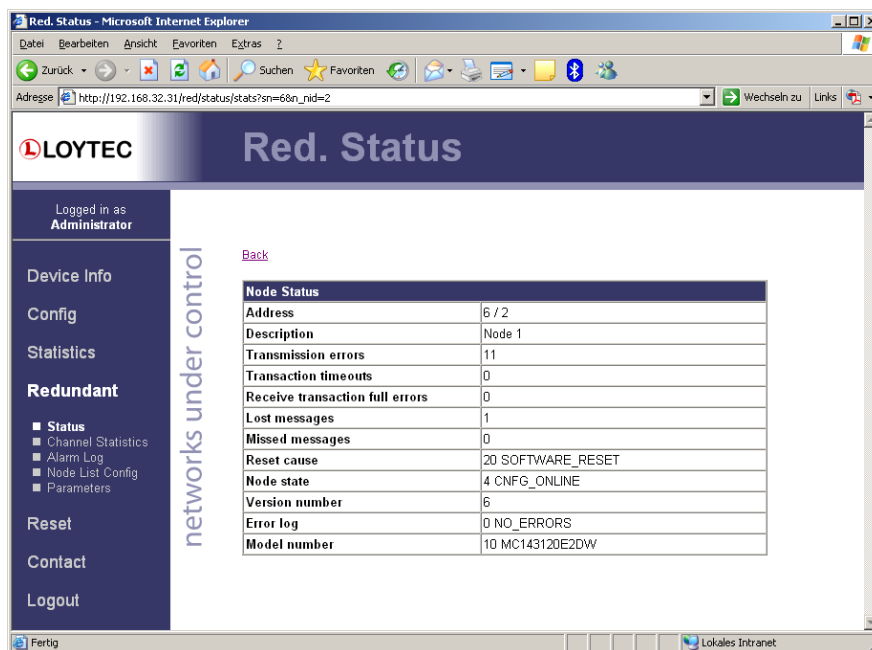


Figure 105: The L-IP Redundant Web Interface – Device Statistics Page

8.6.2 Channel Statistics

Figure 106 shows the channel statistics page. This page offers similar information as the channel statistics view of the L-IP Redundant Plug-In (see Section 8.5.4).

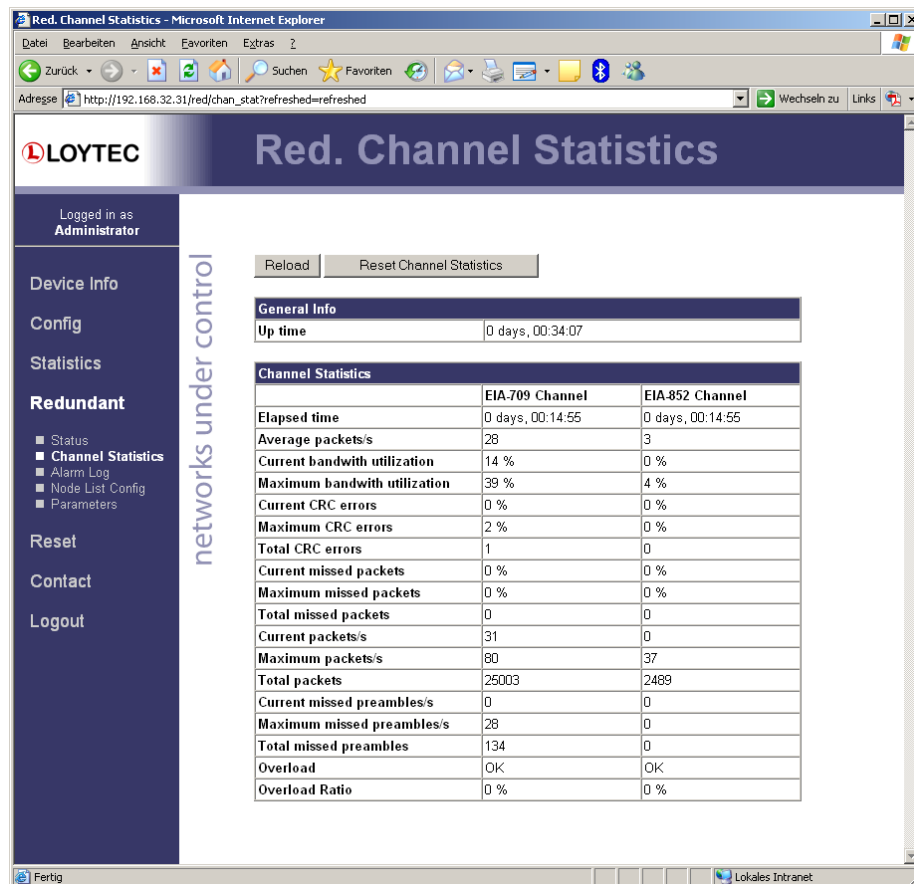


Figure 106: The L-IP Redundant Web Interface – Channel Statistics Page

8.6.3 Alarm Log

Figure 107 shows the alarm log page. This page offers similar information as the alarm log view of the L-IP Redundant Plug-In (see Section 8.5.5).

Major differences compared to the plug-in interface are:

- ◆ A “Download” button allows to download the alarm log as CSV-file.

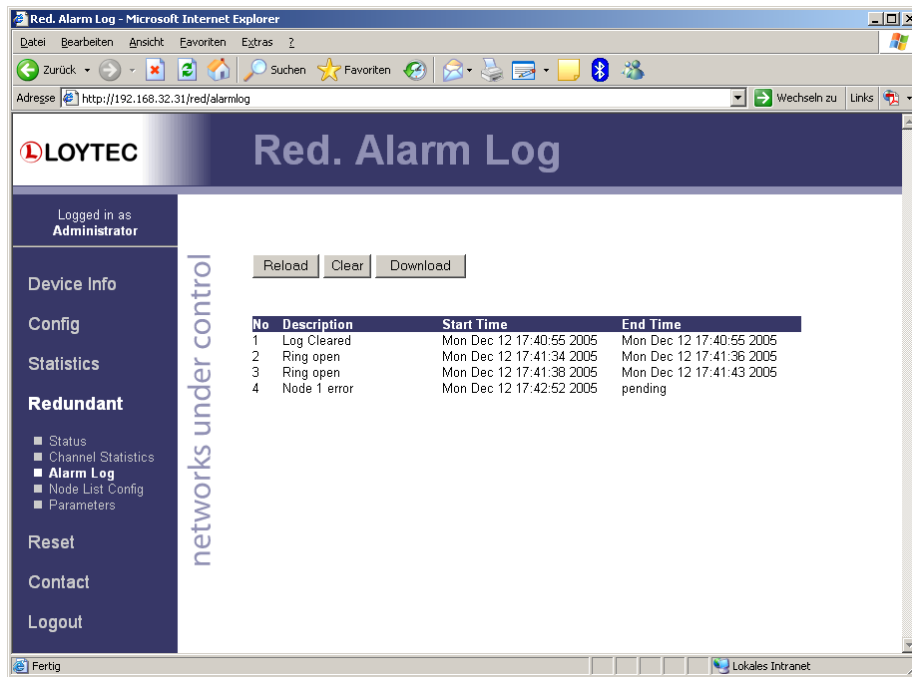


Figure 107: The L-IP Redundant Web Interface – Alarm Log Page

8.6.4 Node List Configuration

Figure 108 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 8.5.6).

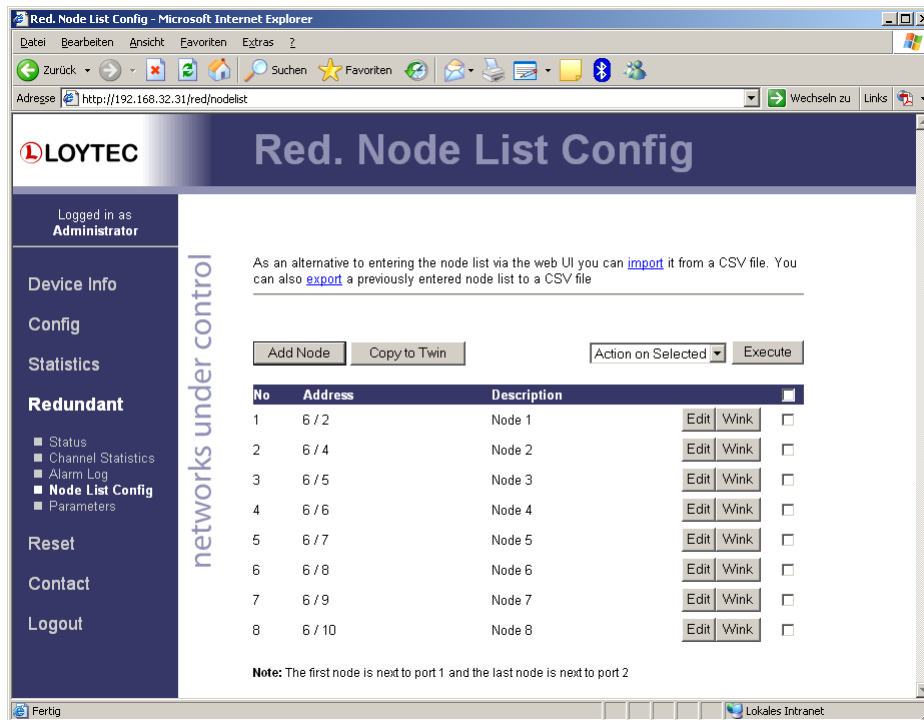


Figure 108: The L-IP Redundant Web Interface – Node List Config Page

Major differences compared to the plug-in interface are:

- ◆ Clicking on the link “import” allows to import/upload a node list from a CSV-file
- ◆ Clicking on the link “export” allows to export/download the node list as 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 to choose 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 5.3.2).

8.6.5 Parameters

Figure 109 shows the parameters page. This page offers similar information as the parameters view of the L-IP Redundant Plug-In (see Section 8.5.7).

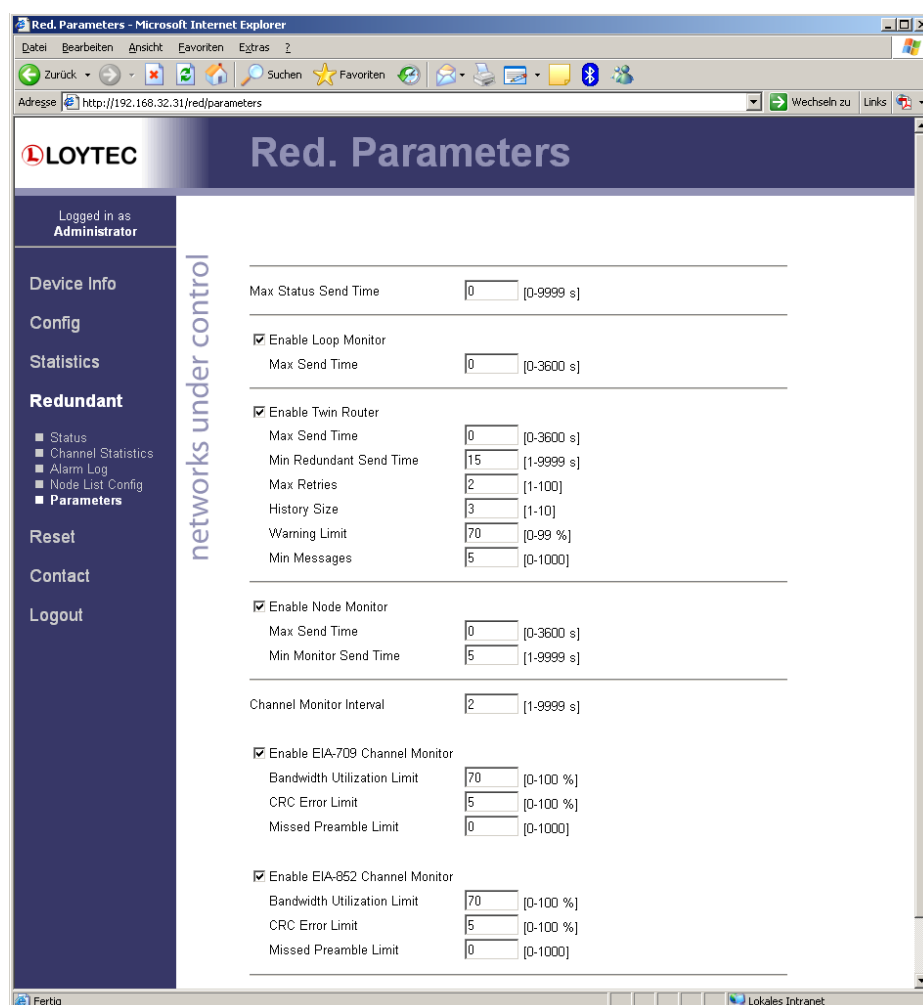


Figure 109: The L-IP Redundant Web Interface – Parameters Page

Major differences compared to the plug-in interface are:

- ◆ If router redundancy is used, the button “Save & Copy to Twin” allows to save 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.

8.7 Network Interface

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

8.7.1 Node Object

The Node Object functional block is shown in Figure 110. In addition to the mandatory functions defined in the LonMark Node Object functional profile the following optional and user defined functions are implemented:

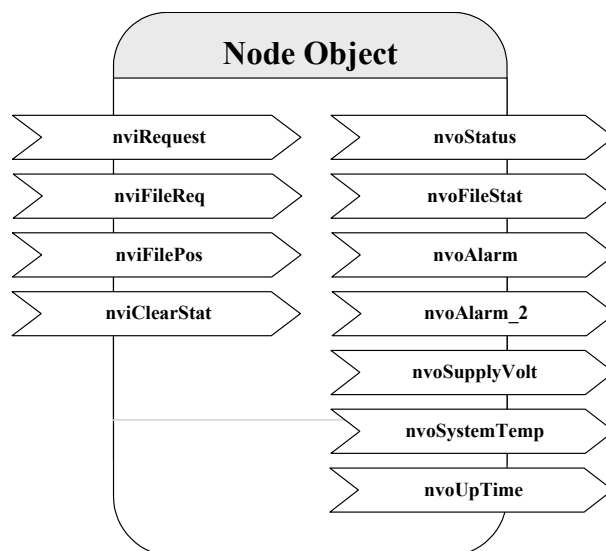


Figure 110: Node Object

- ◆ 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 8.7.5) 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.

8.7.2 Bus Loop Monitor Object

Figure 111 shows the Bus Loop Monitor Object functional block. This functional block is responsible for the bus loop monitoring (see Section 8.2.1). It has the following network variables:

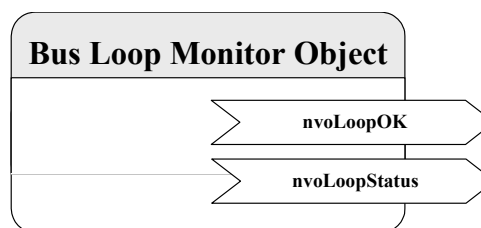


Figure 111: Bus Loop Monitor Object

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, INVALID}: 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.

8.7.3 Device Monitor Object

Figure 112 shows the Device Monitor Object functional block. This functional block is responsible for the device monitoring (see Section 8.2.3). 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.

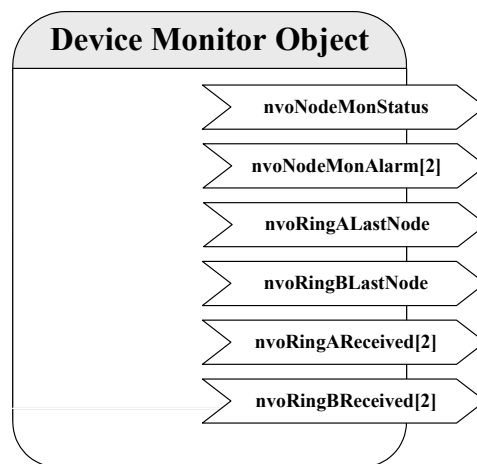


Figure 112: Device Monitor Object

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 to detect 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: index of last node reachable from this port.
- 0xFFFF: loop interrupted directly at loop port 1 (*nvoRingALastNode*) or loop port 2 (*nvoRingBLastNode*) respectively.

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 17.

RingAReceived	RingBReceived	Significance
0	0	<ul style="list-style-type: none"> ◆ 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 17: Significance of *nvoRingXReceived* bit combinations

8.7.4 Twin Router Object

Figure 113 shows the Twin Router Object functional block. This functional block is responsible for the router redundancy (see Section 8.2.2). It has the following network variables:

UNVT_red_rtr nviRedRtr

UNVT_red_rtr nvoRedRtr

As already mentioned in Section 8.4.3.2 these two network variables are used to establish the connection between paired L-IP Redundant devices.

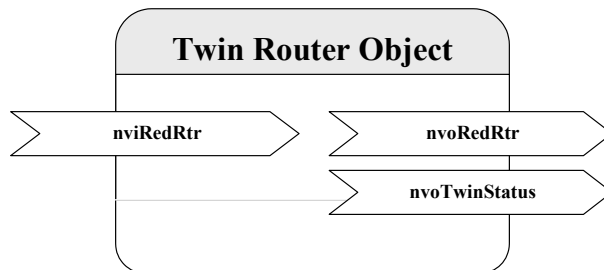


Figure 113: Twin Router Object

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 EIA852 monitoring (*bit9*) and the forwarding warnings and errors (*bit10-bit13*) are not applicable.
- ◆ *bit8*: 1 if the twin router is not reachable via the EIA-709 segment (local segment), 0 otherwise.
- ◆ *bit9*: 1 if the twin router is not reachable via the EIA-852 channel (IP backbone), 0 otherwise.
- ◆ *bit10*: 1 if the packets forwarded from the EIA-709 to the EIA-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 EIA-852 to the EIA-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 EIA-709 to the EIA-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 EIA-852 to the EIA-709 side, while the remote twin router does. 0 if the router is working properly.

8.7.5 Channel Monitor Objects

Figure 114 shows the Channel Monitor Object functional block. This functional block is responsible for network monitoring (see Section 8.2.3). There is one object for each channel the L-IP Redundant is attached to: The channel monitor object with index 0 corresponds to the EIA-709 side of the L-IP Redundant, while the object with index 1 corresponds to the EIA-852/IP side of the L-IP Redundant. Each object has the following network variables:

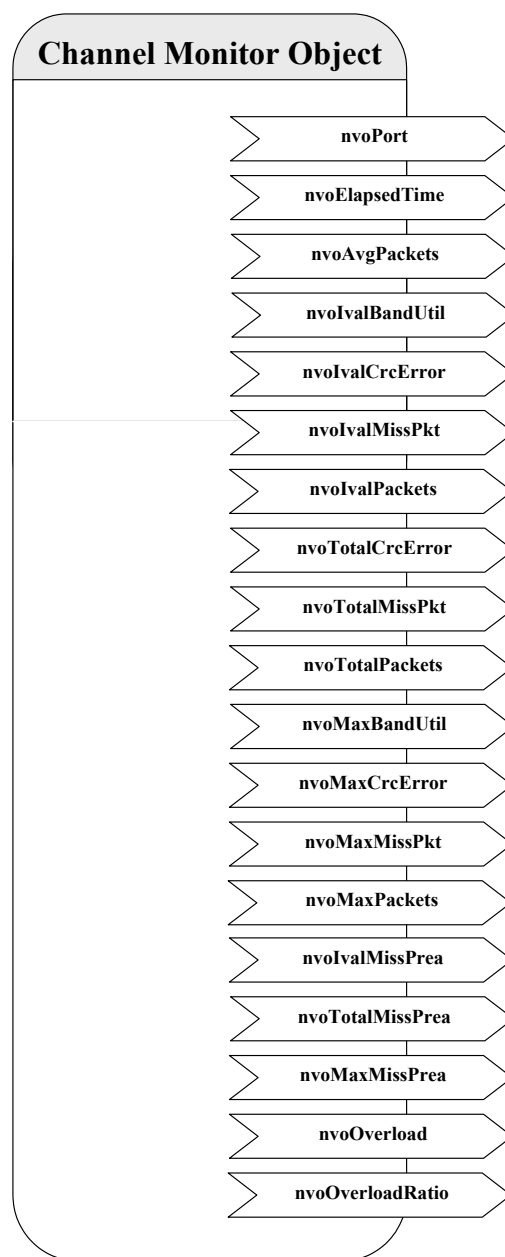


Figure 114: Channel Monitor Object

SNVT_count nvoPort

Index of port associated with this Channel Monitor Object instance. Port 1 corresponds to the EIA-709 side of the L-IP Redundant, while port 2 corresponds to the EIA-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 8.6), the network variable *nvoClearStat* (see Section 8.7.1) 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 EIA-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 EIA-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 were reset.

9 Network Media

9.1 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 with a termination network as shown in Figure 115.

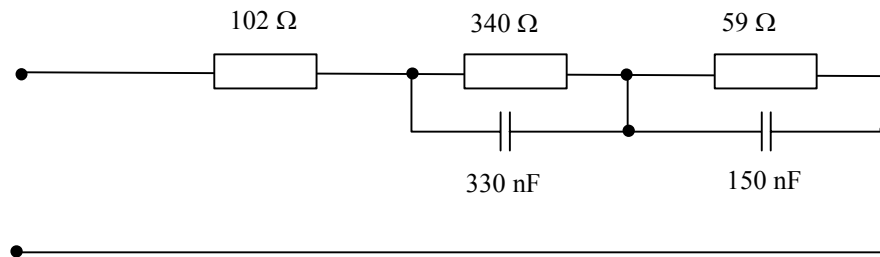


Figure 115: TP-1250 Termination Network

If backbone mode (see Section 0) is disabled, the L-IP TP-1250 ports are fully compatible to the parameters specified by LonMark for this channel (TP/XF-1250). If 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.

9.2 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.

When using the Free Topology Segment feature of the FT-10, only one termination (Figure 116) is required and can be placed anywhere on the free topology segment.

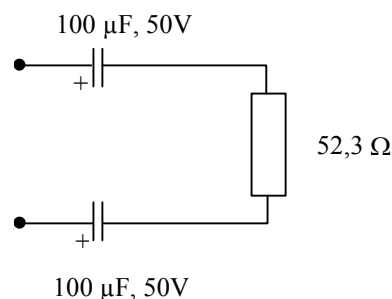


Figure 116: FT-10 Free Topology Termination

In a double terminated bus topology, two terminations are required (Figure 117). These terminations need to be placed at each end of the bus.

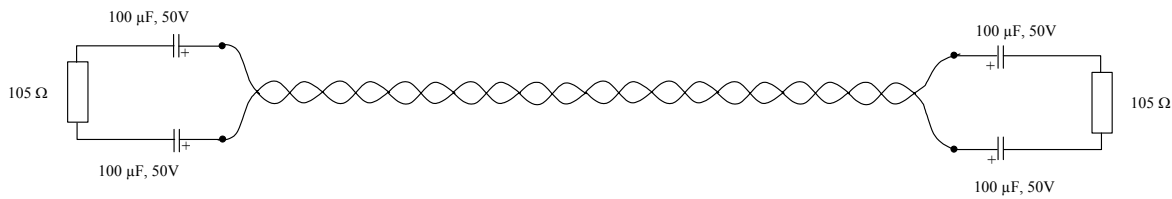


Figure 117: Termination in an FT-10 Bus Topology

9.3 RS-485 Bit-Rate Auto-Detection

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 118 shows the DIP-switch settings to disable bit-rate auto-detection, assuming all other DIP switches remain in the factory default position.

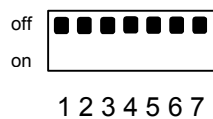


Figure 118: DIP-switch 3 disables bit-rate auto-detection

Alternatively the bit-rate auto-detection can be enabled/disabled via the console menu (see Section 4.5). 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.

RS-485 requires a network segment with bus topology. The maximum stub length between the bus line and the node is 0,3 m. Figure 119 shows the termination required for an RS-485 network.

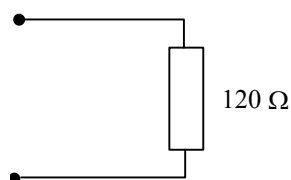


Figure 119: RS-485 Termination

In an RS-485 network terminations need to be placed at each end of the bus (see Figure 120).

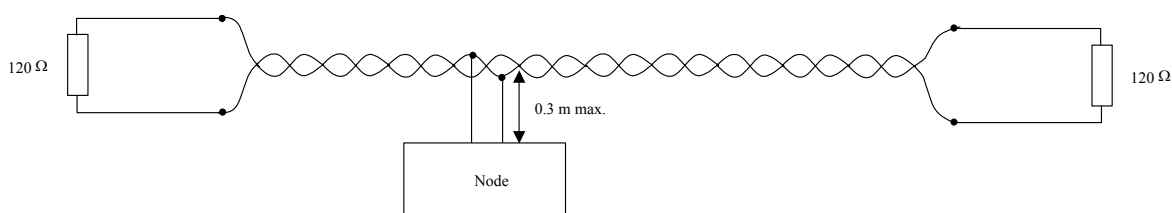


Figure 120: Termination in an RS-485 Bus Topology

9.4 TP-1250 Collision-Less Backbone

The TP-1250 port on the LIP-1ECT can be configured to use a special operating mode in which several L-Switch or L-IP devices can be connected via a TP-1250 collision-less backbone (see Figure 121). This operating mode of the TP-1250 port has two advantages compared to the standard operating mode:

1. Maximizes the effective data throughput on the channel.
2. Multiple L-Switch or L-IP devices connected via this backbone behave like one big L-Switch or L-IP (very low propagation delay).

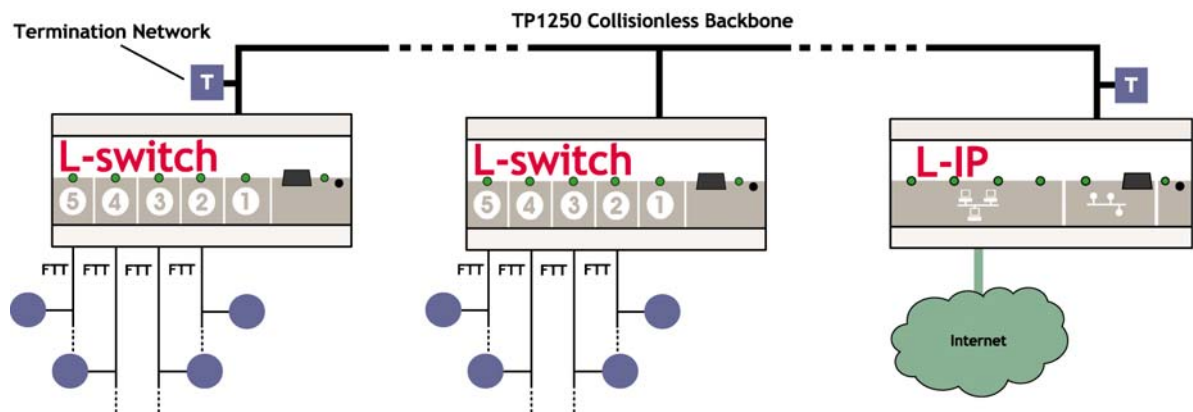


Figure 121: L-Switch and L-IP devices connected via a TP-1250 collision-less backbone

However, this special backbone mode of the L-IP requires the user to set a **unique** ID on each L-Switch and L-IP. This ID needs to be set different for every L-Switch or L-IP. Any number between 0 and 7 can be chosen. Hence, the maximum number of L-Switch/L-IP devices on one backbone is limited to 8 if the collision-less backbone mode is used. Otherwise, if the TP-1250 port is used as a regular LonMark compatible TP-1250 port, none of the above applies.

On the L-IP the backbone-mode must be enabled in the EIA-709 Configuration Menu (see Section 4.5.1) by choosing “Backbone mode” for the TP-1250 port. When backbone mode is selected, a backbone ID must be configured as well, by configuring the TP-1250 port again and selecting “Change backbone ID”. See Section 12.3 for an in-depth discussion of the L-IP backbone mode.

Important: *When using the special collision-less L-IP backbone mode, Neuron Chip based nodes must not be connected to the backbone! This does not apply if the TP-1250 port is used as a regular LonMark compatible TP-1250 port.*

Note: *If more than 8 L-Switch/L-IP devices have to be connected to the collision-less backbone, one L-Switch with two TP-1250 ports (LS-11333C) can be used to connect two TP-1250 collision-less backbone channels. The limit of 8 devices per channel does not apply if the TP-1250 port is used as a regular LonMark compatible TP-1250 port.*

10 L-IP Firmware Update

The L-IP firmware supports remote upgrade over the EIA-709 network, the Ethernet 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:

1. Fall-back image
2. L-IP application image

The fall-back image is write protected in flash memory and provides all means to communicate to the L-IP platform over the EIA-709 and the Ethernet 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 state where the maintenance software can at least talk to the L-IP device and can download a new L-IP application image.

When the L-IP boots up with the fall-back image, the EIA-709 port LED and the STATUS LED are flashing red. In this state it does not forward any messages.

Note: All configuration settings and all forwarding tables will be lost, when the firmware is updated. The EIA-852 and IP settings remain intact.

Note: A firmware update will enable the web interface even if it was disabled via the console interface. Please deactivate the web interface in the console menu if you do not want the web interface being active after a firmware update.

10.1 Firmware Update via the Network

Firmware downloads can be performed on the EIA-709 and the Ethernet network port. However, since the L-IP is not based on a Neuron Chip a new firmware image cannot be downloaded with a standard tool. Rather, a designated tool, the LSD Tool (see Section 12.1), must be used. See the LSD Tool documentation for details on how to download a new L-IP firmware via the network.

10.2 Firmware Update via the Console

To download the firmware via the console the L-IP must be connected to the RS-232 port of a PC via its console interface as described in Section 4.1. You will need the LOYTEC serial upgrade tool (LSU Tool), which can be downloaded from our homepage at www.loytec.com.

Please make sure that the L-IP console shows the main menu otherwise navigate to the main menu or simply reset the L-IP.

Double click on the *.dlc file that comes with the new firmware package. This should start the LSU Tool and load the firmware image referenced in the dlc file. Please note that the dlc

file and the dl file must be stored in the same folder. The start window of the LSU tool is shown in Figure 122.

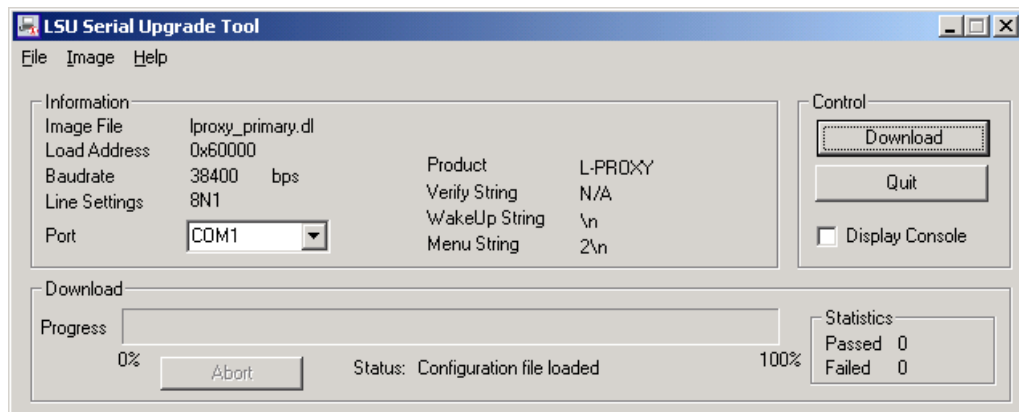


Figure 122: LSU Serial Upgrade Tool in idle mode.

If the L-IP is not connected to COM1 you can change the port to COM1, COM2, COM3, or COM4. Make sure that the product shown under “Product” matches the device you are upgrading. Note that Figure 122 and Figure 123 do not necessarily show the proper product.

Press “Download” to start the download. A progress bar as shown in Figure 123 can be seen.

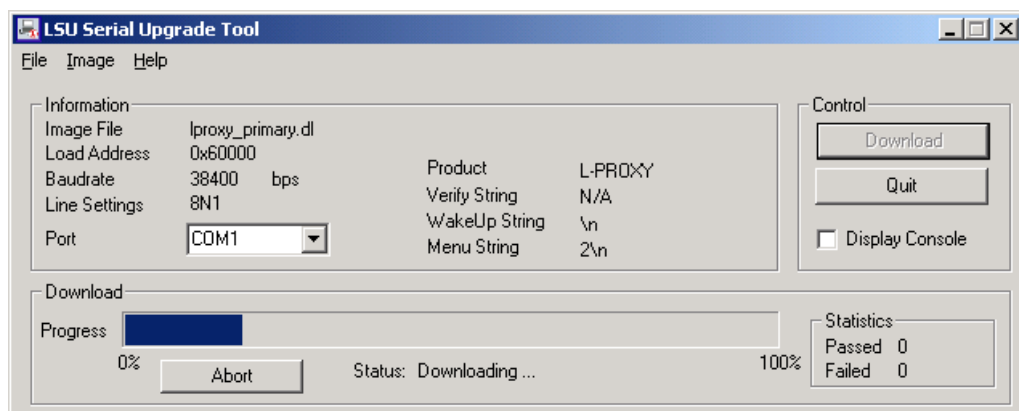


Figure 123: Progress bar during firmware download.

If the upgrade is successful the following window appears (Figure 124).

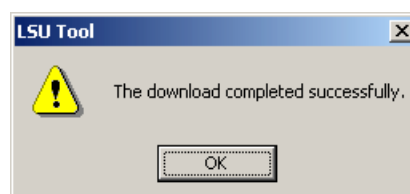


Figure 124: Successful firmware upgrade.

Double check that the new firmware is executed by selecting 1 and pressing Enter in the console window. This will bring up the device information, which shows the current firmware version.

11 Troubleshooting

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

Problem

LonMaker reports an error when commissioning the L-IP as shown in Figure 125.

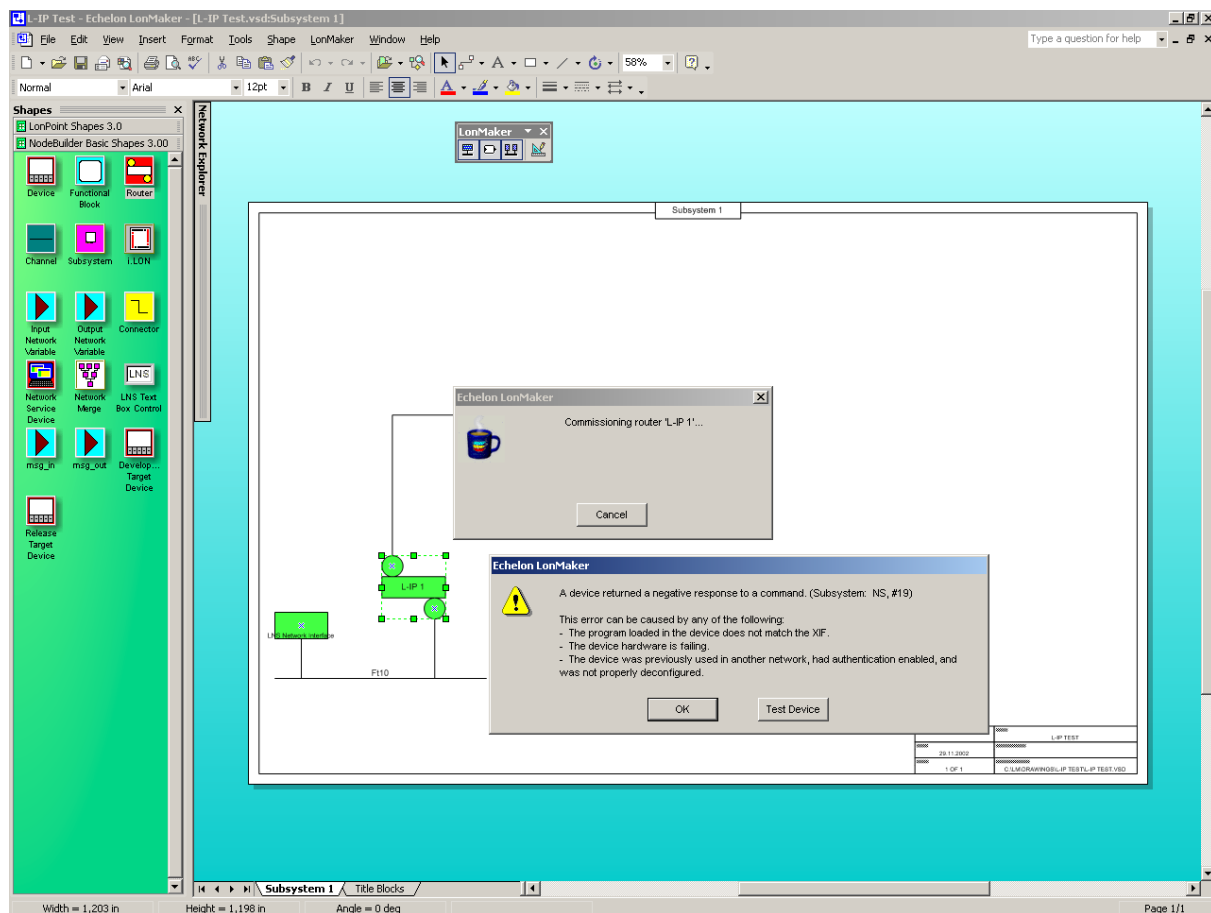


Figure 125: LonMaker fails to commission the L-IP router.

Explanation

The L-IP is not configured as a EIA-709 configured router.

Solution

Please make sure to set the DIP-switches according to Figure 55 as EIA-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 11.8).

11.2 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 16 and that at least one SNTP server is specified for the CN/IP channel. If the L-IP is operated behind a firewall make sure that the firewall doesn't block SNTP requests at port 123.

11.3 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.

11.4 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 (see Section 0) 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.

11.5 EIA-709 Activity LED is flashing red

Problem

The EIA-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 3.4.9): 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 Nodetool) to find the source of the problem.

11.6 The EIA-709 activity LED and the status LED are flashing red

Problem

The EIA-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 8.2.1). 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 11.8).

11.7 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.

11.8 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
Stolzenthalergasse 24/3
A-1080 Vienna
Austria / Europe

email : support@loytec.com
web : <http://www.loytec.com>
tel : +43/1/40208050
fax : +43/1/402080599

12 Application Notes

12.1 The LSD Tool

Please refer to application note “AN002E LSD Tool” for further information about the LOYTEC system diagnostics tool for the L-IP.

12.2 Using the L-IP with LNS based Installation Tools

Please refer to application note “AN003E LIP and LNS” for further information on how to use the L-IP with LonMaker and other network management tools.

12.3 L-IP Backbone Mode vs. a Standard TP-1250 Backbone

Please refer to application note “AN004E Backbone Mode” for further information on how to best utilize the high-speed backbone mode of the L-IP.

12.4 Using the L-Switch with an L-IP Backbone

Please refer to application note “AN005E L-Switch with L-IP Backbone” for further information on how to best utilize the L-Switch together with L-IPs.

13 Firmware Versions

Table 18 shows the most important features available only in certain firmware versions.

Firmware Version/ Features	1.0 Final 1	1.1 Final 1	1.2 Final 2	2.0.0	2.1.0	2.2.0	3.0.0	4.3.0	4.4.0	4.5.0
EIA-709 configured router	√	√	√	√	√	√	√	√	√	√
Smart switch mode	√	√	√	√	√	√	√	√	√	√
Statistics	-	√	√	√	√	√	√	√	√	√
Set RTC	-	√	√	√	√	√	√	√	√	√
IP connection keep alive	-	√	√	√	√	√	√	√	√	√
IP statistics	-	√	√	√	√	√	√	√	√	√
LSD Tool support	-	-	-	√	√	√	√	√	√	√
Bit-rate auto-detection for RS-485	-	-	√	√	√	√	√	√	√	√
DHCP, BOOTP support	-	-	-	√	√	√	√	√	√	√
Configuration via Web browser	-	-	-	√	√	√	√	√	√	√
Remote LPA support	-	-	-	√	√	√	√	√	√	√
Auto member support	-	-	-	√	√	√	√	√	√	√
Roaming member support	-	-	-	√	√	√	√	√	√	√
Backup/Restore configuration	-	-	-	√	√	√	√	√	√	√
Support for route command for web browser setup	-	-	-	-	√	√	√	√	√	√
Automatic NAT router discovery	-	-	-	-	-	√	√	√	√	√
Enable/Disable devices in CS	-	-	-	-	-	√	√	√	√	√
Multiple L-IPs behind one NAT (ext. NAT mode)	-	-	-	-	-	-	√	√	√	√
Multi-cast support	-	-	-	-	-	-	√	√	√	√
Support for 256 members	-	-	-	-	-	-	√	√	√	√
Support for Multi-Port L-IP	-	-	-	-	-	-	-	√	√	√
Support for L-IP Redundant	-	-	-	-	-	-	-	-	√	√
Support for LIP-3333ECTB	-	-	-	-	-	-	-	-	-	√

Table 18: Available features depending on firmware version.

14 Specifications

14.1 LIP-xECT

Operating Voltage.....	9-35 VDC or 12-24 VAC $\pm 10\%$
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 +85°C
Humidity (non condensing) operating	10 to 90% RH @ 50°C
Humidity (non condensing) storage.....	90% RH @ 50°C
Enclosure	Installation enclosure 9 TE, DIN 43 880
Environmental Protection	IP 40 (enclosure); IP 20 (screw terminals)
Installation	DIN rail mounting (EN 50 022) or wall mounting

14.2 LIP-xECTB, LIP-xxECTB, and LIP-xxECRB

Operating Voltage.....	12-35 VDC or 12-24 VAC $\pm 10\%$
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 +85°C
Humidity (non condensing) operating	10 to 90% RH @ 50°C
Humidity (non condensing) storage.....	90% RH @ 50°C
Enclosure	Installation enclosure 6 TE, DIN 43 880
Environmental Protection	IP 40 (enclosure); IP 20 (screw terminals)
Installation	DIN rail mounting (EN 50 022) or wall mounting

14.3 LIP-xxxxECTB

Operating Voltage.....	12-35 VDC or 12-24 VAC $\pm 10\%$
Power Consumption.....	typ. 3 W
In rush current.....	up to 1100 mA @ 24 VAC
Operating Temperature (ambient)	0°C to + 50°C
Storage Temperature.....	-10°C to +85°C
Humidity (non condensing) operating	10 to 90% RH @ 50°C
Humidity (non condensing) storage.....	90% RH @ 50°C
Enclosure	Installation enclosure 9 TE, DIN 43 880
Environmental Protection	IP 40 (enclosure); IP 20 (screw terminals)
Installation	DIN rail mounting (EN 50 022) or wall mounting

15 Revision History

Date	Version	Author	Description
7-11-02	1.0	DL	Initial revision V1.0
01-17-03	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
05-09-03	2.0	DL	Add Section 2.3 IP Configuration for Client Device via Web-Interface
05-09-03	2.0	DL	Add Section 4.4.3 Option 8 - Webserver
05-09-03	2.0	DL	Add Section 4.4.4 Option 9 - Change Web server Password
05-09-03	2.0	DL	Changed menu in Section 4.5 EIA-709 Configuration Menu
05-09-03	2.0	DL	Rewrite Section 4.5.1 and Section 4.5.2.
05-09-03	2.0	DL	Add Section 4.7.10 Option 9 - Location string
05-09-03	2.0	DL	Add Section 4.8.7 Option 7 - Auto members support
05-09-03	2.0	DL	Add Section 4.8.8 Option 8 - Roaming members support
05-09-03	2.0	DL	Add Section 4.8.15 Option s - Show device statistics
05-09-03	2.0	DL	Add Section 4.8.17 Option r - Recontact devices & list channel members
05-09-03	2.0	DL	Add new device states to Table 14
05-09-03	2.0	DL	Add flags to Figure 35: List all CN/IP channel members.
05-09-03	2.0	DL	Add Chapter 5 Web Interface
05-13-03	2.0	DL	Add Section 4.4.2.3 Option 3 - Set router configuration according to DIP switch
05-13-03	2.0	DL	Add Section 7.9 Remote LPA Operation
05-13-03	2.0	DL	Rewrite Section 7.11.3 DHCP
05-29-03	2.0	DL	Release version 2.0
08-14-03	2.1	DL	Added note about PC NTP client to Section 7.10.1
08-14-03	2.1	DL	Add Section 11.7 IP-852 traffic may flood the entire switched IP network
08-28-03	2.1	JB	Corrected information on controlling RS-485 bit-rate auto-detection with DIP switch, see Section 3.6
08-29-03	2.1	DL	Add route command starting with firmware version 2.1 in Section 2.3 and Section 5.1.
09-15-03	2.1	DL	Add Section 4.10.6 Option 6 - Enhanced Communications Test
09-15-03	2.1	DL	Add Enhanced Communications Test to Section 5.4
09-15-03	2.1	DL	Release version 2.1
04-14-04	2.2	JB	Updated for L-IP 2.2
04-15-04	2.2	JB	Release version 2.2
21-09-04	3.0	STS	Release version 3.0. Added extended NAT, multi-cast, Auto-NAT, new enhanced communications test, new channel list in Web, i.LON 600. Corrected terminals 25, 26.
19-04-05	4.3	STS	Updated manual for multi-port L-IP.
22-09-05	4.4	JB	Updated manual for L-IP Redundant
27-06-06	4.5	JB	Updated manual for LIP-xxxxECTB